

**Yealink Meeting Server  
Administrator Guide V23.0.0.12**

# Contents

<b>About This Guide.....</b>	<b>8</b>
Targeted Audiences.....	8
Related Documents.....	8
Basic Concepts.....	8
Icon Introduction.....	9
Summary of Changes.....	9
Changes for Release 23, Guide Version 23.0.0.11.....	9
Changes for Release 22, Guide Version 22.0.0.10.....	10
Changes for Release 21, Guide Version 21.0.0.5.....	10
<b>Introduction of Yealink Meeting Server.....</b>	<b>10</b>
Specifications.....	11
Distributed Architecture.....	13
Benefits of YMS Distributed Architecture.....	13
Components of YMS Distributed Architecture.....	13
Handling the Signaling and the Media.....	14
Browser Requirement.....	15
Port Requirements of the Router.....	15
<b>Port Requirements of the Internal Service</b> .....	15
Port Requirements for the External Service.....	15
Port Requirements for the External Service.....	16
Resource Consumption.....	17
<b>Installing and Deploying YMS.....</b>	<b>18</b>
The Process of Installing and Deploying YMS.....	18
Good to Know about the Hardware.....	19
Basic Requirements of the Hardware.....	19
Calculating Method for the Concurrent Capacity.....	19
Recommended Hardware.....	20
Network Requirements.....	21
Checking the Version of CentOS.....	21
Viewing the Version of CentOS.....	21
Upgrading CentOS Online.....	21
Installing CentOS by Using a USB Flash Drive.....	22
Configuring the Node IP.....	22
Upgrading YMS 1.X to YMS 2.X.....	22
Making a Backup on YMS 1.4.....	22
Uninstalling YMS 1.4.....	24
Installing YMS 2.X.....	25
Migrating the Data on YMS.....	25
Installing YMS 2.X.....	26
Installing Stand-Alone YMS.....	26
Installing Cluster YMS.....	27
Expanding the Stand-Alone YMS.....	29
Upgrading YMS 2.X.....	30
Upgrading YMS 2.X via the Command.....	30
Upgrading YMS 2.X via the Web Interface.....	31

Uninstalling YMS 2.X.....	31
<b>Getting Started.....</b>	<b>32</b>
Logging into YMS.....	32
Setting the Setup Wizard.....	33
System Settings.....	34
Setting the Primary Domain Name.....	34
Editing the Login Password.....	34
Configuring SNTP.....	35
Configuring the SMTP Mailbox.....	36
Setting the Node.....	37
Service Settings.....	54
Setting the Registration Service.....	54
Setting the Traversal Service.....	55
Setting the Interactive Media Service.....	56
Activating a License.....	56
Importing the Device Certificate to the Server.....	56
Activating a License Online.....	57
Activating a License Offline.....	57
Disassociating the License.....	58
Creating Accounts.....	58
Creating Meeting Rooms.....	60
Managing Conferences.....	62
The Checklist for the Configurations and the Common Features.....	62
<b>System Setting.....</b>	<b>63</b>
Basic Operations.....	63
Introduction of the Home Page.....	64
Changing the Display Language for the Website.....	65
Editing the Registered Email.....	65
Setting the Session Timeout.....	65
Enabling Forced Https Authentication.....	66
Adding a Sub Admin Account.....	66
Customizing the Theme.....	68
Setting the Password Policy.....	74
Logging out of YMS.....	74
Setting the Web Service Address.....	74
Setting the Log Service Address.....	75
Setting the Time Zone.....	75
Importing the Trusted CA Certificate.....	76
Importing the HTTPS Certificate.....	77
Importing the TLS Certificate.....	78
Configuring the Port.....	78
Setting the Data Space.....	79
Allocating the Number Resource.....	79
Setting the IP Property.....	81
Setting the Intelligent Security Strategy.....	81
Adding a Security Group.....	83
Deleting the Abnormal IP.....	83
Applying for the Accesskey.....	84
Adding the User-Agent Blacklist.....	84
Adding the User-Agent Compatible List.....	85
Configuring the Email Template.....	85
Setting SIP Trunk IVR.....	86

Setting the Audio IVR.....	87
Setting IVR language.....	88
<b>Managing Services.....</b>	<b>88</b>
Configuring the Redirection Service.....	88
Broadcasting Interactive Conference.....	89
Configure the Broadcast Media Service.....	89
Enabling Broadcasting Interactive for Scheduled Conferences.....	90
Enabling Broadcasting Interactive for VMR.....	90
Yealink Recording Service.....	91
Enabling the Recording Service.....	92
Managing the Recording Settings.....	92
Enabling the Recording Privileges for User Accounts.....	96
Enabling the Recording Privileges for VMRs.....	97
Managing the Recording Files.....	98
Viewing the Recording Log.....	100
Configuring the Media Bypass Service.....	101
Yealink Live Service.....	101
Enabling Live Service.....	102
Configuring YMS System RTMP Live.....	103
Setting the RTMP Live for VMRs.....	103
Collaboration Service.....	104
Setting the Collaboration Service.....	105
Managing Collaboration Files.....	105
Configuring the Third-Party Registration Service.....	106
Configuring the GK Service.....	107
Setting the GK Service.....	107
Enable GK Registration for Accounts.....	109
H.323 Gateway.....	109
Setting H.323 Gateway.....	109
H.323 Gateway Example.....	111
H.323 Gateway Example (Taking H.323 Gateway as an Endpoint).....	112
Setting the IP Call.....	113
Setting the IP Call Service.....	113
IP Call Example.....	115
Call Routing.....	116
Process of Call Routing.....	117
Regular Expressions.....	118
Adding a Call Routing Rule.....	120
Setting the Call Routing Rule for Rejecting.....	121
Add a Number Filter.....	122
<b>Managing Accounts.....</b>	<b>123</b>
User Account, Room System Account and Other Accounts.....	123
Managing Accounts by Group (Optional).....	123
Parameters of User Account and Room System Account.....	124
Add a User Account.....	126
Importing a Batch of Accounts.....	128
LDAP.....	129
Configuring the LDAP.....	129
Adding an LDAP Account.....	132
Synchronizing LDAP Accounts.....	133



<b>Managing Meeting Rooms.....</b>	<b>133</b>
Entity Meeting Room and the Virtual Meeting Room.....	134
Managing Meeting Rooms by Groups (Optional).....	134
Adding Entity Meeting Rooms.....	135
Adding a VMR.....	136
Discussion Mode and Training Mode.....	137
Sending Emails to VMR Participants.....	139
<b>Managing Conferences.....</b>	<b>139</b>
Call Settings.....	139
Setting the Video and Content Resolution.....	140
Setting the Call Bandwidth.....	141
Configuring the Max Video Parties per Conference.....	141
Configuring the Max Audio-Only Parties per Conference.....	142
Setting the Time for Joining Conference Beforehand.....	142
Enabling Auto Dialing.....	142
Enabling Audio Redialing.....	143
Enabling Mute Participants upon Entry.....	143
Setting the Audio Prompt When Participants Join or Leave Conferences.....	144
Displaying the Native Video.....	145
Setting the Last Participant Backstop Timeout.....	145
Setting the Auto End Conference Without Moderator.....	145
Enabling Content Only.....	145
Setting the Join with APP Awakened by Browser.....	146
Enabling Receiving Ringtone Receipt.....	146
Enabling External/Internal Network Access WebRTC Authentication.....	147
Enabling the Roll Call.....	147
Setting the App Push Address.....	148
Setting the QoS.....	148
Setting the Default Layout.....	148
Displaying the Participant Name.....	150
Display Participant Status.....	150
Displaying the Participant Quantity.....	151
Displaying the Audio-Only Participant.....	151
Controlling Conferences.....	151
Monitoring the Conference.....	152
Going to the Conference Monitoring Page.....	152
Selecting an Audio Output Device.....	152
Adjusting the Output Volume.....	153
Changing the Display Language.....	153
Configure the Video Images in Equal N×N.....	153
Setting the Video Carousel.....	154
Displaying a Participant in a Full Screen/Exiting the Full Screen.....	154
Scaling the Video Image.....	154
Hiding/Showing the Conference Video.....	155
Switching Between the Video Window and the Content Window.....	155
Displaying the Conference Monitoring Page in a Full Screen/Exiting the Full Screen.....	155
Deleting Conferences.....	156
Viewing the Usage of Meeting Rooms.....	156
<b>Managing Conference Statistics.....</b>	<b>156</b>
Viewing the MCU Resource.....	157

Viewing the Conference Statistics.....	157
Viewing the Call History.....	158
<b>Managing Devices.....</b>	<b>158</b>
Prerequisites for the Devices Automatically Connected to YMS.....	158
Device Status.....	159
Managing Devices by Groups (Optional).....	159
Pushing the Configuration.....	160
Pushing Firmware.....	161
Diagnosing Devices.....	163
Managing T49 Devices.....	163
<b>Integrating YMS with Other Servers.....</b>	<b>165</b>
Communicating with the PSTN.....	165
Setting the PSTN Gateway Service.....	165
PSTN Example.....	166
Communicating with Skype for Business Server.....	167
Communicating with the Local SfB Server.....	168
Communicating with Microsoft Office 365.....	171
Communicating with Other Enterprise SfB Servers.....	174
Setting the SFB Gateway.....	179
Setting the SfB Gateway Media Service.....	183
Communicating with Another YMS or Third-Party PBX (Peer Trunk).....	183
Setting the Peer Trunk Service.....	183
Peer Trunk Example.....	185
Communicating with Another YMS or Third-Party PBX (Registration Trunk).....	186
Configuring the REG Trunk Service.....	186
Registration Trunk Example.....	188
Setting Alibaba Cloud RTMP Live.....	189
Configuring the RTMP Media Service.....	190
Configuring the RTMP Live.....	190
Setting the RTMP Live for VMRs.....	191
Enabling Conference Recording (Third-Party Recording Server).....	192
<b>System Maintenance.....</b>	<b>193</b>
Making Backups and Restoring the Server.....	193
Setting the Auto Backup.....	193
Creating a Backup Manually.....	194
Downloading a Backup.....	194
Restoring the Backup.....	195
Rebooting the System.....	196
Resetting to the Factory.....	196
Viewing Operation Logs.....	197
Exporting System Logs.....	197
Using Tools.....	198
Pinging the Network.....	198
Capturing Packets.....	198
<b>Troubleshooting.....</b>	<b>199</b>
Users Do Not Receive Emails.....	199
Failing to Connect to SMTP.....	200
Users Fail to register an Account.....	200

Failing to Activate a License Online.....	201
Failing to Activate a License Offline.....	201
Loading the Organizational Structure Slowly.....	202
The Configuration of Access WebRTC Authentication Is Invalid.....	202

# About This Guide

---

The enterprise administrator can read this guide to operate and maintain YMS.

- [Targeted Audiences](#)
- [Related Documents](#)
- [Basic Concepts](#)
- [Icon Introduction](#)
- [Summary of Changes](#)

## Targeted Audiences

---

This guide is mainly intended for the following audiences.

- The distributors
- The system administrator

## Related Documents

---

You can download these documents from the **Video Collaboration** product line on [Yealink Official website](#).

- Yealink Meeting Server User Guide: it introduces how to use YMS after you log in as a user.
- Yealink Meeting Server Web App User Guide for PC: it introduces how to use the browser on PC to join conferences.
- Yealink Meeting Server Web App User Guide for Mobile: it introduces how to use the browser on the mobile phone to join conferences.
- YouTube Streaming Guide: it introduces how to stream the conference to YouTube by RTMP so the YouTube user can watch the webcast of the conference.
- Yealink Meeting Server and Skype for Business Deployment Guide: it introduces how to deploy YMS and Skype for Business server so YMS users can communicate with SfB users.
- Yealink SIP Trunk Deployment Guide: it introduces how to deploy SIP trunk in both CUCM/3CX/FreePBX and YMS so the users of CUCM/3CX/FreePBX can communicate with YMS users.
- Yealink Federation Management Platform Guide: it introduces how to install and use Yealink federation management platform. Besides, it presents how YMS synchronizes the data with the federation management platform and manages the data.

## Basic Concepts

---

This section introduces the basic concepts which you may encounter in this document.

**Enterprise directory:** it refers to the directory which includes user accounts, room system accounts, and third-party devices.

**Yealink VC devices:** it refers to the devices that you can register them with YMS accounts and then use the features provided by YMS, including PVT950/PVT980, VC880/VC800/VC500/VC200/VC400/VC120/VC200 video conferencing system, SIP VP-T49G IP phone, VP59 IP phone, and VC Desktop & VC Mobile.

**The interactive party:** it refers to the participant who sends the audio or video in the broadcasting interactive conference.

**The broadcasting party:** it refers to the participant who only receives but does not send the audio or video in the broadcasting interactive conference.

**Content:** it refers to the documents, the pictures or the videos shared by the moderator and the lecturer.








**Node:** A single YMS is one node, in either the cluster version or the stand-alone version.

## Icon Introduction

---

The icons on YMS are described as below.

**Table 1: Icon Introduction**

Icon	Description
	Recurrence conference
	RTMP live
	General meeting room
	User account
	Room system account
	Other account
	Video meeting room

## Summary of Changes

---

- [Changes for Release 23, Guide Version 23.0.0.11](#)
- [Changes for Release 22, Guide Version 22.0.0.10](#)
- [Changes for Release 21, Guide Version 21.0.0.5](#)

### Changes for Release 23, Guide Version 23.0.0.11

The following sections are new for this version:

- [Making Backups for Recording Files](#)
- [Adding Watermark for Recording Files](#)
- [Managing Devices](#)
- [Setting the Audio Prompt When Participants Join or Leave Conferences](#)
- [Yealink Live Service](#)

Major updates have occurred to the following sections:

- [Specifications](#)
- [Managing Accounts](#)
- [Displaying the Participant Name](#)
- [Parameters of the Recording Template](#)
- [Adding a Sub Admin Account](#)
- [Adding a VMR](#)

- [Configuring the RTMP Live](#)

## Changes for Release 22, Guide Version 22.0.0.10

The following sections are new for this version:

- [Setting the Collaboration Service](#)
- [Managing Collaboration Files](#)
- [Setting the Password Policy](#)
- [Using Tools](#)

Major updates have occurred to the following sections:

- [Setting the Video and Content Resolution](#)
- [Parameters of the Recording Template](#)
- [Managing the Recording Files](#)
- [Deleting Recording Files](#)
- [Managing the Sharing Link](#)
- [Adding a VMR](#)
- [Displaying a Participant in a Full Screen/Exiting the Full Screen](#)

## Changes for Release 21, Guide Version 21.0.0.5

The following sections are new for this version:

- [Loading the Organizational Structure Slowly](#)
- [Displaying the Audio-Only Participant](#)
- [Enabling Receiving Ringtone Receipt](#)
- [Setting the Join with APP Awakened by Browser](#)
- [Monitoring the Conference](#)
- [Enabling the Recording Service](#)
- [Managing the Recording Settings](#)
- [Viewing the Recording Log](#)
- [Resetting to the Factory](#)

Major updates have occurred to the following sections:

- [Adding a Sub Admin Account](#)
- [Adding a VMR](#)
- [Customizing the Theme](#)
- [Introduction of the Home Page](#)
- [Setting the IP Call Service](#)
- [Communicating with the PSTN](#)
- [Setting the Peer Trunk Service](#)
- [Configuring the REG Trunk Service](#)
- [Setting the GK Service](#)

# Introduction of Yealink Meeting Server

---

Yealink Meeting Server (YMS) is a virtualized and distributed multipoint conferencing platform. As a powerful all-in-one meeting server, YMS brings together a host of key features and services: MCU, registrar server, directory server, traversal server, meeting and device management server, SIP Trunk, WebRTC server, GK & H.460 server, Microsoft

SfB (Lync) gateway, recording server, and collaboration server. It provides any number of users with their VMRs to hold high definition conferences, share presentations, collaborate, and chat. Participants can use virtually any type of communication tools to join the conference over audio or video. YMS connects people with crystal-clear audio, HD video, content and web collaboration, bridging locations across any distance or device and providing users with an enjoyable conferencing experience while cutting costs and improving efficiency.

- [Specifications](#)
- [Distributed Architecture](#)
- [Browser Requirement](#)
- [Port Requirements of the Router](#)
- [Resource Consumption](#)

## Specifications

The specifications are as below:

Features	YMS3000	YMS2000	YMS1000
<b>All-in-One</b>	MCU, Registrar Server, Traversal Server, Meeting and Device Management Server, Enterprise Directory Server, SIP Trunk Server (Video & Audio), WebRTC Server, GK& H.460 Server, SfB (Lync) Gateway, Recording Server, Collaboration Server		
<b>Conference Capability</b>	144 parties of 720P30 72 parties of 1080P30 36 parties of 1080P60	80 parties of 720P30 40 parties of 1080P30 20 parties of 1080P60	40 parties of 720P30 20 parties of 1080P30 10 parties of 1080P60
<b>Broadcasting Interactive Conference</b>	Up to 1,500 parties from External Server		
<b>Additional Audio Calls</b>	40		
<b>Communication Protocols</b>	ITU-T H.323/H.239, IETF SIP/BFCP, RTMP, RDP, RTSP		
<b>Resolution</b>	4K, 1080P, 720P, 360P, 4CIF, CIF		
<b>Video Codecs</b>	H.265, H.264 High Profile, H.264, H.263+, H.263, VP8		
<b>Audio Codecs</b>	Yealink ARES, Opus, G.722.1C, G.722.1, G.722, G.711(μ/A), G.729, G.729A, G.729AB, G.728, AAC-LC		
<b>Distributed Architecture</b>	Server Cluster Management & Multi-host Hot Standby		
<b>Server Federation</b>	Server Federation Management & Multi-server Cascading		
<b>Expansion</b>	MCU Stack Technology, Cascading Video Conference		
<b>Flexible Layouts</b>	Equal NxN (N=2, 3, 4, 5, 6, 7), onePlusN (N=0, 4, 7, 9, 12, 16, 20), twoPlusN (N=8), Overlay and Selected Speaker		
<b>Recording</b>	Supports 5-way full HD(1080P30) recording with dual stream	Recording, VOD(Video on Demand) and Management	

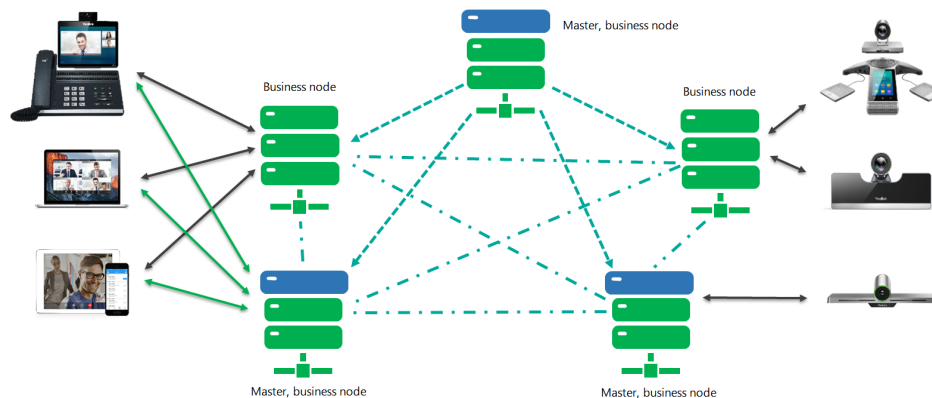
Features	YMS3000	YMS2000	YMS1000
<b>Other Functions</b>	RTMP Live, Audio IVR, Display Native Video and Content, Display audio parties, Chat in Conference		
<b>Bandwidth Dynamic Adaptive Adjustment</b>	Anti 30% video and 70% audio packet loss, QoS		
<b>Security Protocols</b>	TLS, SRTP, HTTPS, SSH, H.235, AES-256bit		
<b>Firewall Traversal</b>	Ability to deploy conferencing nodes in a public DMZ: deploy privately-addressed conferencing nodes behind NAT firewalls; allow external parties to connect directly via a public address.		
<b>Multiple Conferencing Methods</b>	P2P Call, Meet Now, Ad Hoc, Scheduled Conferencing, VMR		
<b>Multiple Conference Modes</b>	Training Mode, Discussion Mode and Lecturer View		
<b>Integration with Yealink VC Endpoints</b>	Sync Conference Information, Conference Reminder, One-touch Conference Access, Apply for Speaking		
<b>Conference Control</b>	Invite/Remove, Lock/Unlock/End Conference, Conference Lobby, Conference Monitoring, Mute/Unmute Video & Audio, Block/Unblock Audio, Change Roles, Sharing Permission, Rename, Roll Call, Call Statistics, Conference Banner/Subtitle/Agenda, FECC		
<b>Personal Layout</b>	Voice Activated Speaker, Video Carousel, Customized Layout and Application Parties		
<b>User Account</b>	Organizational Structure and up to 100,000 accounts		
<b>Enterprise Directory</b>	Synchronize directory to the device		
<b>LDAP</b>	Synchronize directory from Microsoft AD Server		
<b>Third-party Device Registration</b>	SIP/H.323		
<b>Traversal Features</b>	ICE/TURN/STUN/NAT/H.460		
<b>Web Management</b>	Friendly Web UI and Setup wizard		
<b>Customization</b>	Web & Logo, Email Template, Audio IVR and SIP Trunk IVR		
<b>System Status Monitoring</b>	Web-based real-time dashboard & data update on capacity and system information		
<b>Resource Statistics Management</b>	Graphic display and statistics & analysis of conferences, MCU resources and CDR		
<b>System Maintenance Management</b>	Remote Upgrade, Backup/Restore, Reboot/Factory Reset and Syslog, Network Ping, Packet Capture, SNMP		
<b>System Security Management</b>	Blacklist, Whitelist and Intelligent Security Strategy		
<b>Device Remote Management</b>	Automatic Upgrade, Reboot, Factory Reset, Packets Capture, Export Logs and Export Configuration File		



## Distributed Architecture

From version 2.X or later, YMS distributed architecture provides the following features:

- **Load balance:** ability to realize the load balance among the service nodes in the cluster. The same conferences will select the same MCU server with priority to reduce consumption, and different conferences will select the MCU server whose load is the smallest with priority.
- **Redundancy:** with the feature of active-active high availability cluster and hot-standby failover, if one server does not work, the whole service can still work without any interruption. Because when a service node cannot work, other service nodes in the cluster will take over its service automatically within 20 seconds. It is seamless to the conference participants.
- **Scalability:** YMS allows you to scale up your service nodes based on your demand and supports a large number of concurrent videos.



- [Benefits of YMS Distributed Architecture](#)
- [Components of YMS Distributed Architecture](#)
- [Handling the Signaling and the Media](#)

## Benefits of YMS Distributed Architecture

- Centralized management of the nodes.
- Ability to add nodes at any time from any location without service outage.
- Ability to deploy dedicated edge servers for providing external services.
- Independent services; ability to deploy the MCU service and the traversal service in the edge node.
- Ability to expand your nodes and to upgrade your server seamlessly. Ability to select MCU addresses dynamically (the same conference will select the same MCU server) to use the MCU resource optimally.
- Ability to hold a broadcasting interactive conference, which contains at least 1000 participants in the conference and allows you to toggle between the broadcasting parties and the interactive parties.
- Allow you to customize the call routing.
- Ability to be compatible with the H.323 endpoints with the built-in H.323 gateway and GK server.

## Components of YMS Distributed Architecture

YMS consists of the master node and the business node. The master node is required and can be a business node if the hardware performance and the network meet the requirements. The business node is not required, and you can scale it up according to the hardware performance and the network demand.

**Master node:** it mainly provides the Web service, for example, the data center, the discovery service, and the business data. Due to the service attributes, you cannot configure these services via the web interface. You need to configure the master node when the first time you deploy it and you can only run the related command line to expand.

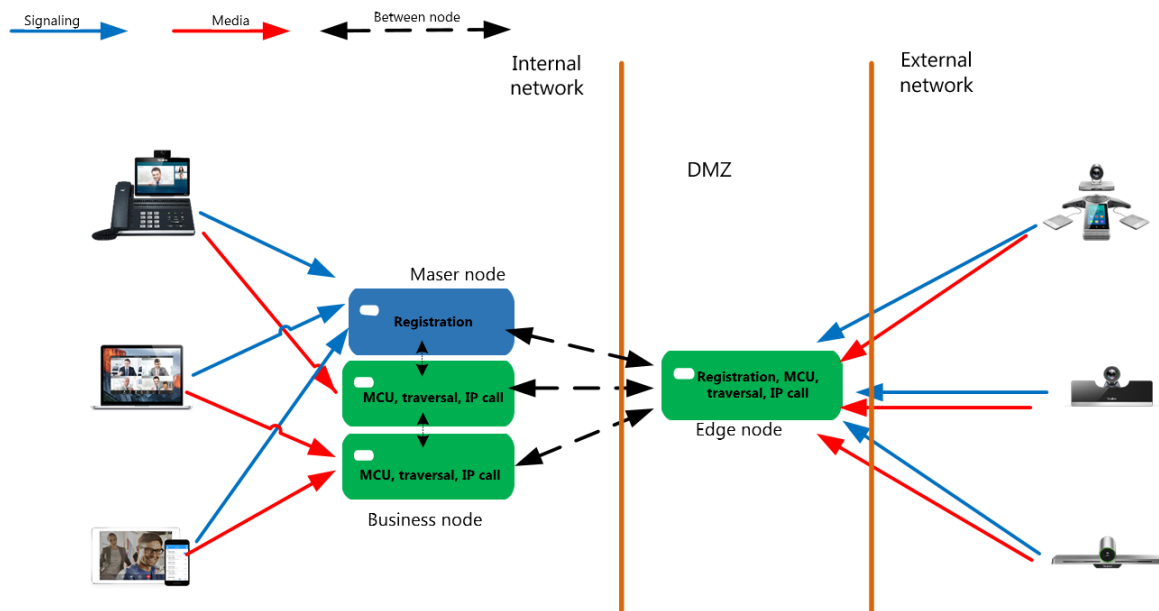
**Business node:** those nodes mainly provide services, for example, SIP service, H.323 service, and MCU service. You can configure and add business nodes via the web interface. You can also enable and disable these services via the web interface. Especially for the MCU service that calls for higher hardware performance, you can add nodes.

You can deploy one or three master nodes. For one master node, when it does not work, the services are unavailable. For three master nodes, when one server fails, the other two servers can still provide services. There is no limit to the business node, and you can deploy as many as you need. For more information about the deployment, refer to [Installing Cluster YMS](#).

## Handling the Signaling and the Media

The media and the signaling for each call in YMS may take different paths, mainly depending on the function and capacity of the node. Take the cluster deployment of 1+3 as an example to introduce the rule of handling the media and the signaling.

- The incoming calls will be assigned to the corresponding nodes according to DNS, and the signaling will be sent to these nodes.
- YMS selects the MCU media service dynamically. The same conference will select the same MCU with priority, and different conferences will select the MCU with the lowest load.
- The signaling flow from the endpoints in the internal network will be sent to the master node and then the master node will assign the media service dynamically.
- The interaction process of the signaling flow between the endpoints in the internal and the external network: the endpoints in the internal network->the master node->the edge node->the endpoints in the external network.
- The interaction process of the media flow between the endpoints in the internal and the external network: the master node->the business node (dynamic assignment)->the edge node->the endpoints in the external network.



## Browser Requirement

YMS supports the following browsers.

**Table 2: Browser Requirement**

Browser Requirement	Version
Firefox	50 or later
Google Chrome	50 or later
360	8.1 or later
Internet Explorer	10 or later

## Port Requirements of the Router

If you restrict the following ports, please open them. If you deploy YMS in the internal network, you need to map the following ports to the public network on the router, to solve the interconnection problem between the private and public networks.

- [Port Requirements of the Internal Service](#)
- [Port Requirements for the External Service](#)
- [Port Requirements for the External Service](#)

## Port Requirements of the Internal Service

**Port requirements for the internal service:** make sure that the following ports in every node of the cluster can communicate with each other.

Port	Protocol	Description
8000-10000	UDP+TCP	The port for the internal service.
27017	UDP+TCP	The port for accessing the database.
22	TCP	Install or upgrade the server via ssh.

## Port Requirements for the External Service

**Table 3: Port requirements for the external service (Some of the following ports are configurable. You can edit the default port based on the actual demand.)**

Module	Port	Protocol	Description
Web port	443	TCP	HTTPS port
	444	TCP	The port that can be accessed by Yealink devices via HTTPS
	80	TCP	HTTP port
Rsyslog log service port	514	UDP/TCP	YMS uses this port for collating the device logs

Module	Port	Protocol	Description
H.323 port	1719	UDP	RAS listening port of the GK.
	1722	TCP	H.225 listening port of the GK
	20000-23999	TCP	GK Q.931/H.245
	20000-29999	UDP	Media proxy port of GK
	1720	TCP	H.225 listening port of the Gateway
	27000-29999	TCP	Gateway Q.931/H.245
Turnserver port	3478	UDP/TCP	The listening port of the traversal service
	3479	UDP/TCP	Backup listening port
	9688	TCP	As long as the IP address exists, this port should be mapped, because it might influence the traversal service
	40000-49999	UDP/TCP	Relay port

## Port Requirements for the External Service

**Table 4: Port requirements for the external service (Some of the following ports are configurable. You can edit the default port based on the actual demand.)**

Module	Port	Protocol	Description
SIP port	5061	UDP/TCP/ TLS	Redirection service and registration service
	5060	UDP/TCP	IP call service
	5062	TLS	
	5063	UDP/TCP	Third-Party registration service
	5065	UDP/TCP	PSTN gateway service
	5066	UDP/TCP	Peer trunk service
	5065	UDP/TCP	REG trunk service
	5067	UDP/TCP/ TLS	Skype for Business service
MCU service port	50000-54999	UDP	Interactive media service
	63000-63999	UDP	Collaboration service
	55000-59999	UDP	Broadcast media service
	60000-60899	UDP	RTMP media service
	61000-62999	UDP	SfB gateway media service
	64000-64999	UDP	Media bypass service
IVR port	10000-10999	UDP	IVR
BFCP/FECC port	11000-12999	UDP	BFCP/FECC

Module	Port	Protocol	Description
The stack-signaling port of the conference	13000-13199	UDP	Conference stack
The stack-media port of the conference	13200-13399	UDP	Conference stack
Recording service port	65000-65499	UDP	Recording service
RTMP live service port	60900-60999	UDP	RTMP live service

## Resource Consumption

The type of call (HD, SD, or others) affects the amount of resource required by the server to handle the call. The table below lists the resource consumption in different call situations.

**Table 5: Resource consumption**

No.	Situation	HD 720p call	Full HD 1080p call
1	In a broadcasting interactive conference, when 23 broadcasting parties join the conference	1	2
2	Enable Alibaba Cloud RTMP live	2 (One HD 720p call and one SD 360p call)	3 (One full HD 1080p call, one HD 720p call, and one SD 360p call)
3	Enable Yealink RTMP live	2 (One HD 720p call and one SD 360p call)	3 (One full HD 1080p call, one HD 720p call, and one SD 360p call)
4	Streaming by RTMP	1	2
5	Enable recording	1	2
6	Establish a call via the peer trunk (you need to configure the peer trunk first and then establish a call with the third-party MCU)	Bypass disabled: 3; Bypass enabled: 1	Bypass disabled: 6; Bypass enabled: 2
7	Establish a call via the registration trunk (you need to configure the registration trunk first and then establish a call with the third-party MCU)	Bypass disabled: 3; Bypass enabled: 1	Bypass disabled: 6; Bypass enabled: 2
8	Establish a SfB call	3 (Bypass not supported)	6 (Bypass not supported)
9	YMS users join a SfB conference	3 (Bypass not supported)	6 (Bypass not supported)
10	Lync users join a YMS conference	3 (Bypass not supported)	6 (Bypass not supported)
11	Invite users to join the conference via IP call (IVR/URL/IP)	Bypass disabled: 3; Bypass enabled: 1	Bypass disabled: 6; Bypass enabled: 2
12	H.323 users join a YMS conference	Bypass disabled: 3; Bypass enabled: 1	Bypass disabled: 6; Bypass enabled: 2
13	H.323 users call SIP users or SIP users call H.323 users	Bypass disabled: 3; Bypass enabled: 1	Bypass disabled: 6; Bypass enabled: 2

## Installing and Deploying YMS

---

- [The Process of Installing and Deploying YMS](#)
- [Good to Know about the Hardware](#)
- [Checking the Version of CentOS](#)
- [Configuring the Node IP](#)
- [Upgrading YMS 1.X to YMS 2.X](#)
- [Installing YMS 2.X](#)
- [Upgrading YMS 2.X](#)
- [Uninstalling YMS 2.X](#)

## The Process of Installing and Deploying YMS

---

The following introduces the process of installing, deploying, and configuring YMS 2.X.

	Upgrading YMS 1.X to YMS 2.X	Deploying ex-factory YMS 2.X	Installing and deploying YMS 2.X on a VM	Installing and deploying YMS 2.X on a third-party server	Installing and deploying cluster YMS 2.X	Reference
Good to Know about the Hardware	√		√	√	√	<a href="#">Good to Know about the Hardware</a>
Making a Backup on YMS 1.4	√					<a href="#">Making a Backup on YMS 1.4</a>
Uninstalling YMS 1.X	√					<a href="#">Uninstalling YMS 1.4</a>
Checking the Version of CentOS	√		√	√	√	<a href="#">Checking the Version of CentOS</a>
Configure the Node IP	√	√	√	√	√	<a href="#">Configuring the Node IP</a>
Installing YMS 2.X	√		√	√	√	<a href="#">Installing YMS 2.X</a>
Migrating the data on YMS	√					<a href="#">Migrating the Data on YMS</a>
Activating a License	√	√	√	√	√	<a href="#">Activating a License</a>
The network of YMS 2.X and the basic configuration	√	√	√	√	√	<a href="#">Getting Started</a>

The Checklist for the Configurations and the Common Features	√	√	√	√	√	<i>The Checklist for the Configurations and the Common Features</i>
--	---	---	---	---	---	---

## Good to Know about the Hardware

---

- [Basic Requirements of the Hardware](#)
- [Calculating Method for the Concurrent Capacity](#)
- [Recommended Hardware](#)
- [Network Requirements](#)

### Basic Requirements of the Hardware

Before installing YMS, your hardware should meet the following requirements.

**Table 6: Basic Requirements of the Hardware**

Item	Requirements
CPU	E5-2600 V4 or later, with the clock speed more than 2.3GHz
RAM	<ul style="list-style-type: none"> <li>• 16G</li> <li>• The memory frequency should be at least 2133MHz</li> <li>• 2GB RAM for one core</li> <li>• Support multi-channel memory architecture</li> </ul>
Network	1 Gbps NIC or switches
Disk	<p>At least 500G for every master node</p> <ul style="list-style-type: none"> <li>• /home/mcudata: 300GB, depends on the size of the business</li> <li>• /usr/local/apollo: 150GB, depends on the size of the business</li> <li>• /Var/log/apollo: 50GB, depends on the size of the business</li> </ul> <p>At least 200G for every business node</p> <ul style="list-style-type: none"> <li>• /Home/mcudata: 50G, depends on the size of the business</li> <li>• /Usr/local/apollo: 100GB, depends on the size of the business</li> <li>• /Var/log/apollo: 50G, depends on the size of the business</li> </ul>

### Calculating Method for the Concurrent Capacity

- **For the physical machine, you can refer to the following:**

Concurrent capacity of 720p = total number of cores \* clock speed \* 1.2

Concurrent capacity of 1080p = total number of cores \* clock speed \* 0.6

- **For the virtual machine, you can refer to the following:**

Concurrent capacity of 720p = total number of Vcores \* clock speed \* 0.6

Concurrent capacity of 1080p = total number of Vcores \* clock speed \* 0.3

## Recommended Hardware

- If you install YMS in VMware, you can refer to the following recommendations.

CPU Model	Clock Speed	Total Number of Vcores	RAM	Concurrent Capacity (the video + the shared content + SRTP)	
				(720p30fps+1080p30fps+SRTP)	(1080p30fps+1080p30fps+SRTP)
Xeon(R) Platinum 8163 CPU	2.5GHZ	12	24G	18	9
Intel(R) Xeon(R) CPU E5-2666 v3	2.9GHZ	10	20G	17	8
Intel(R) Xeon(R) Gold 6149 CPU	3.1GHZ	10	20G	18	6
Xeon(R) Platinum 8163 CPU	2.5GHZ	24	48G	36	18
Intel(R) Xeon(R) CPU E5-2666 v3	2.9GHZ	20	40G	34	17
Intel(R) Xeon(R) Gold 6149 CPU	3.1GHZ	20	40G	37	18
Intel(R) Xeon(R) CPU E5-2666 v3	2.9GHZ	32	64G	55	27
Intel(R) Xeon(R) Gold 6149 CPU	3.1GHZ	32	64G	59	29
Intel(R) Xeon(R) CPU E5-2666 v3	2.9GHZ	40	80G	69	34
Intel(R) Xeon(R) Gold 6149 CPU	3.1GHZ	40	80G	74	37
Intel(R) Xeon(R) Gold 6149 CPU	3.1GHZ	48	96G	89	44
Intel(R) Xeon(R) CPU E5-2666 v3	2.9GHZ	64	128G	111	55
Intel(R) Xeon(R) Gold 6149 CPU	3.1GHZ	64	128G	119	59
Intel(R) Xeon(R) Gold 6149 CPU	3.1GHZ	32	64G	59	29
Intel(R) Xeon(R) Gold 6149 CPU	3.1GHZ	32	64G	59	29
Intel(R) Xeon(R) CPU E5-2666 v3	2.9GHZ	40	80G	69	34
Intel(R) Xeon(R) Gold 6149 CPU	3.1GHZ	40	80G	74	37



### Note:

- If you install YMS in VMware, you can refer to the following recommendations.
- We recommend 300G Disk for formal deployment. For internal testing of YMS2.0, 100G is acceptable.
- Other services cannot occupy the VCPU resource assigned to this YMS server in any case. Otherwise, the concurrent calls cannot reach the number we provide.
- Recording consumes some hardware resources of the video call. One 720p recording consumes double hardware resources of one 720P call.
- One 1080p recording consumes quadruple hardware resources of one 720P call.
- If you use Intel E5 to install CentOS and then install YMS 2.0, you can refer to the following recommendations.

CPU Model	Clock Speed	Total Number of CPUs	Total Number of Cores	RAM	Concurrent Capacity (the video + the shared content + SRTP)	
					(720p30fps+1080p30fps+SRTP)	(1080p30fps+1080p30fps+SRTP)
E5-2620 v3	2.4GHz	1	6	4*8G ( 2133MHz )	17	8
E5-2620 v3	2.4GHz	2	12	8*8G ( 2133MHz )	34	16
E5-2620 v4	2.1GHz	1	8	4*8G ( 2400MHz )	20	10
E5-2620 v4	2.1GHz	2	16	8*8G ( 2400MHz )	40	20
E5-2660 v3	2.6GHz	1	10	4*8G ( 2133MHz )	31	15
E5-2660 v3	2.6GHz	2	20	8*8G ( 2133MHz )	62	31
E5-2680 v4	2.4GHz	1	14	4*8G ( 2400MHz )	40	20
E5-2680 v4	2.4GHz	2	28	8*8G ( 2400MHz )	80	40
E5-2695 v4	2.1GHz	2	36	8*8G ( 2400MHz )	92	46
E5-2699 V4	2.2GHz	2	44	8*8G ( 2400MHz )	116	58

- If you use Intel Silver & Gold to install CentOS and then install YMS 2.0, you can refer to the following recommendations.

CPU Model	Clock Speed	Total Number of CPUs	Total Number of Cores	RAM	Concurrent Capacity (the video + the shared content + SRTP)	
					(720p30fps+1080p30fps+SRTP)	(1080p30fps+1080p30fps+SRTP)
Intel Xeon Silver 4114	2.2GHz	1	10	6*8G ( 2400MHz )	25	12
Intel Xeon Silver 4114	2.2GHz	2	20	12*8G ( 2400MHz )	50	25
Intel Xeon Silver 4116	2.1GHz	1	12	6*8G ( 2400MHz )	30	15
Intel Xeon Silver 4116	2.1GHz	2	24	12*8G ( 2400MHz )	60	30
Intel Xeon Gold 6132	2.6GHz	1	14	6*8G ( 2666MHz )	40	20
Intel Xeon Gold 6132	2.6GHz	2	28	12*8G ( 2666MHz )	80	40
Intel Xeon Gold 6152	2.1GHz	1	22	6*8G ( 2666MHz )	50	25
Intel Xeon Gold 6152	2.1GHz	2	44	12*8G ( 2666MHz )	100	50



## Network Requirements

**Table 7: Network Requirements**

Item		Requirements
Bandwidth	1080P60fps (1920x1080)	4M
	1080P60fps (1920x1080) the video	6M
	1080P30fps (1920x1080) the shared content	
	1080P30fps (1920x1080)	1.7Mb
	1080P30fps (1920x1080) The video + the shared content	3.4Mb
	720P30fps (1280x720)	700Kb
	720P30fps (1280x720) The video + the shared content	1.5Mb
Delay		The general delay of the video conference should be less than 200ms
Jitter		Less than 50ms
Packet loss		Less than 1%

## Checking the Version of CentOS

If the YMS cannot access the external network, we recommend that you use CentOS 7.5 or later. If it can access the external network, you can use CentOS 7.0 or later.

- [Viewing the Version of CentOS](#)
- [Upgrading CentOS Online](#)
- [Installing CentOS by Using a USB Flash Drive](#)

## Viewing the Version of CentOS

### Procedure

Run the command `cat /etc/redhat-release`.

```
[root@localhost ~]# cat /etc/redhat-release
CentOS Linux release 7.2.1511 (Core)
```

## Upgrading CentOS Online

### Before you begin

The server can access the external network.

## Procedure

1. Run the command `yum clean all` to clear yum.

```
[root@localhost ~]# yum clean all
已加载插件: fastestmirror, langpacks
正在清理软件源: base extras updates
Cleaning up everything
Cleaning up list of fastest mirrors
```

2. Run the command `yum update` to update the yum package.  
The whole upgrading process might take a long time. Please wait.

```
安装 17 软件包 (+137 依赖软件包)
升级 869 软件包
总下载量: 952 M
Is this ok [y/d/N]: y
Downloading packages:
No presto metadata available for base
updates/7/x86_64/prestodelta
Delta RPMs reduced 645 k of updates to 150 k (76% saved)
(1/1023): libvorbis-1.3.3-8.el7_1.3.3-8.el7.1.x86_64.drpm
(2/1023): augeas-libs-1.4.0-2.el7_1.4.0-5.el7_5.1.x86_64.drpm
```

After upgrading, check the current version of CentOS.

## Installing CentOS by Using a USB Flash Drive

### About this task

If the server cannot access the public network, you can re-install the system by using a USB flash drive.

### Procedure

1. Download the mirroring package, which you obtain from Yealink technical support engineers.
2. Create a Boot disk in the USB flash drive. You can find the method on the Internet.
3. Install the CentOS. You can find the method on the Internet.  
After the installation, check the current version of CentOS.

## Configuring the Node IP

---

We recommend you use the static IP address for the server. You can find the method on the Internet.

## Upgrading YMS 1.X to YMS 2.X

---

Directly upgrading YMS 1.X to YMS 2.X is not available. Therefore, you can update it according to this part. Note that you should re-configure the corresponding information of the NIC.



**Note:** For upgrading YMS 2.X to YMS 2.Y, see [Upgrading YMS 2.X](#).

- [Making a Backup on YMS 1.4](#)
- [Uninstalling YMS 1.4](#)
- [Installing YMS 2.X](#)
- [Migrating the Data on YMS](#)

### Making a Backup on YMS 1.4

- [Saving the Data by Screenshot](#)
- [Exporting All Call Statistics](#)
- [Making a Backup for the System Data](#)

## Saving the Data by Screenshot

From Version 2.X, the structure of YMS has changed. Therefore, the data migration is not available. You can save the following configuration by taking screenshots.

Log into YMS 1.X, and do the following:

- Click **System**->**Call Settings**->**Global settings**, and take screenshots of the entire configuration.

**Yealink Meeting Server | YMS DEMO**

**Global settings**

**Video resolution**

Max video resolution : 360P/30FPS

Max content sharing resolution : 720P/5FPS

**Call bandwidth**

Call bandwidth : 512Kbps

Limit the bandwidth of media being received by Yealink Meeting Server from individual participants.

**Layout**

Display participant name :  Equal N+N  onePlusN

Default layout :  Equal N+N  onePlusN

Equal N+N : 4\*4

Max number of videos displayed in equal N+N layout

When the number of videos exceed the maximum, every 30s :

- one video switches per cycle
- all videos switch per cycle

- Click **System**->**Call Settings**->**Call routing**, and take screenshots of the entire configuration.

**Yealink Meeting Server | Yealink Network Technology Co.,Ltd**

**Call routing**

Batch delete

Name	Priority	Destination match	Call target	Out location	Enable	Operation
to_sfb_client	1	^888(d+)*@	SFB	to_sfb	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
to_sfb_mcu	2	^666(d+)*@	SFB	to_sfb	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
to_sfb_client1	3	y@(d+)*@	SFB	to_sfb	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
shouji	4	^\(d{11})\$	PSTN	testtjy	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
to_sfb_client2	6	^8888(d+)*@	SFB	to_sfb	<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
test	10	^0(d+)*\$	PSTN	testtjy	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

All 6 records | 50 rows per page | page 1

- Click **System**->**Gateway Configuration**->**SIP trunk IVR**, and take screenshots of the entire configuration.

**Yealink Meeting Server | YMS DEMO**

**SIP Trunk IVR**

**Receptionist Greeting Prompt Configuration**

Configure greeting prompt :  Default Greeting (Current IVR language: Portuguese)

Personal Greeting

Select file

The uploaded personal greeting must be a .wav file which cannot exceed 10MB.

**Menu Options**

Enable first-level extension dialing

Key	Description	Action	Action Data
0	Extension dialing	Extension dialing	
1	Conference dialing	Conference dialing	
2		---	
3		---	
4		---	
5		---	

## Exporting All Call Statistics

### About this task

Log into YMS 1.X, and do the following:

### Procedure

Click **Statistics > Export**.

The screenshot shows the 'Statistics (2018/10/27 ~ 2018/11/27)' page in the Yealink Meeting Server. The interface includes a sidebar with navigation options like Status, Account, Meeting Room, VMR, Conference Control, and System. The main content area shows summary statistics for conferences and ports, and a table of individual conference records. The 'Export' button is located at the bottom right of the records table.

Subject	Type	ID	Time	Duration	Detail
1 Wilson SU-Yealink's video conference	Meet Now	62610	2018/11/27 02:52:45 - 02:52:52	00:00:07	View
2 Sala1's video conference	Meet Now	54936	2018/11/27 01:05:31 - 01:05:32	00:00:01	View
3 Sala1's video conference	Meet Now	32611	2018/11/27 01:05:04 - 01:05:29	00:00:25	View
4 Wilson SU-Yealink's videoconferencia	Scheduled	86623	2018/11/26 15:44:50 - 16:30:00	00:45:10	View

## Making a Backup for the System Data


### About this task

Log into YMS 1.X, and do the following:
























**Note:** Make sure there are no ongoing conferences before making the backup.

### Procedure

1. Click **System > System Maintenance > Backup/Restore**.
2. Click  on the right side of the created backup to download it to your computer.

The screenshot shows the 'Backup/Restore' page in the Yealink Meeting Server. The page includes a sidebar with navigation options like Security, System Maintenance, Licenses, and System Log. The main content area shows a table of backup files with columns for File name, File size(MB), Build time, and Operation. The 'Download' icon is highlighted with a red box.

File name	File size(MB)	Build time	Operation
AutoBackup_20181127_120000.tar.gz	85.14	2018/11/27 00:00:00	  
AutoBackup_20181126_120000.tar.gz	85.14	2018/11/26 00:00:00	  
AutoBackup_20181125_120000.tar.gz	85.13	2018/11/25 00:00:00	  
Backup_20181109_164627.tar.gz	85.19	2018/11/09 16:46:26	  
Backup_20181108_152854.tar.gz	85.15	2018/11/08 15:28:53	  
Backup_20181102_170837.tar.gz	85.10	2018/11/02 17:08:37	  
Backup_20181017_094557.tar.gz	84.74	2018/10/17 09:45:58	  

## Uninstalling YMS 1.4

- If the server can access the external network

1. Use SecureCRT to go to the command interface of the root account via SSH.

2. Run the following command to download the uninstalling script:

```
Curl -O address # the address of the uninstalling script (You can
contact Yealink technical support engineers to obtain)#
```

3. Run the following command to add an executive privilege to the uninstalling script:

```
chmod u+x apollo_util.sh
```

4. Run the following command to execute the uninstalling script:

```
./apollo_util.sh uninstall 11055011 no
```

5. Wait until the uninstallation is finished.
6. Run the following command to clear the remained process:

```
ps -ef | grep apollo | grep -v grep | awk '{print $2}' | xargs -I{} kill
-9 {}
```

- **If the server cannot access the external network**

1. Manually download the uninstalling script to your PC. You can contact Yealink technical support engineers to obtain the uninstalling script.
2. Use SecureCRT to go to the command interface of the root account via SSH.
3. Run the command `cd /root` to go to the directory (/root).
4. Run the command `rz` and upload the installed uninstalling script on the pop-up window.
5. Run the following command to add an executive privilege to the uninstalling script:

```
chmod u+x apollo_util.sh
```

6. Run the following command to execute the uninstalling script:

```
./apollo_util.sh uninstall 11055011 no
```

7. Wait until the uninstallation is finished.
8. Run the following command to clear the remained process:

```
ps -ef | grep apollo | grep -v grep | awk '{print $2}' | xargs -I{} kill
-9 {}
```

## Installing YMS 2.X

### Procedure

1. Run the command `cd /usr/local` to go to the directory (/usr/local).
2. Run the following command to delete the `apollo_install` folder:

```
rm -rf apollo_install
```

3. [Installing Stand-Alone YMS](#).

## Migrating the Data on YMS

You can contact Yealink technical support engineer to migrate the data.

## Installing YMS 2.X

---

The YMS installation method includes the stand-alone installation and the cluster installation.

The differences between them are as below:

Type	Description
<b>Installing Stand-Alone YMS</b>	A single YMS but with all services.
<b>Installing Cluster YMS</b>	Multiple YMSs, including the following node types: <ul style="list-style-type: none"> <li>• <b>Master node:</b> it provides all the YMS services.</li> <li>• <b>Sub-master node:</b> if you want to realize the disaster recovery for all features, it must contain 2 sub-master nodes.</li> <li>• <b>Business node:</b> you can assign the desired service, mainly the MCU service, to each business node according to the enterprise deployment need.</li> </ul>

- [Installing Stand-Alone YMS](#)
- [Installing Cluster YMS](#)
- [Expanding the Stand-Alone YMS](#)

### Installing Stand-Alone YMS

This part introduces how to install YMS 2.X.

- [Downloading the Installation Package](#)
- [Unzipping the Installation Package](#)
- [Running the Installation Command](#)

#### Downloading the Installation Package

- **The server can access the external network**

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

```
cd /usr/local
```

2. Run the following command to download the installation package (change x.x.x.x to the version you want to download):

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

- **The server cannot access the external network**

1. Manually download the installation package, which you obtain from Yealink technical support engineers.
2. Use SecureCRT to go to the command interface of the root account via SSH.
3. Run the command `cd /usr/local` to go to the directory (/usr/local).
4. Run the command `rz` and upload the Rom package on the pop-up window.

## Unzipping the Installation Package

### Procedure

Run the following command:

```
cd /usr/local                                #go to the directory where the
  installation package is in#
tar xzf YMS_x.x.x.x.tar.gz                  # unzip the installation package
(change x.x.x.x to the version you want to install)#
cd apollo_install                            # go to the installation directory#
tar xzf install.tar.gz                      # unzip the installation script#
```

## Running the Installation Command

### Procedure

1. Run the following command:

```
./install.sh
```

```
已安装:
libtomcrypt.x86_64 0:1.17-26.e17          libtommath.x86_64 0:0.42.0-6.e17
sshpas.x86_64 0:1.06-2.e17

完毕!

Default profile /usr/local/apollo/data/install.conf does not exist.
please make a choice:
!!! timeout 30 seconds, timeout default is [A].
[A]. Deploy allinone with default 127.0.0.1
[B]. Create default profile and then exit to edit it

Please Input your choice:
```

2. Enter A to select the stand-alone installation.

If you do not select within 30 seconds, the system will select the stand-alone installation automatically. The installation will be finished in about 10 minutes. Please wait.

## Installing Cluster YMS

Here are two plans for installing cluster YMS:

Plan A: 1+N ( N can be 1.2.3.4.5.6..... ) , 1 master node and N business nodes. It does not have the disaster recovery feature, but it has multiple business nodes, with good service capability and low coupling.

Plan B: 3+N ( N can be 1.2.3.4.5.6..... ) , 1 master node, 2 sub-master nodes, and N business nodes. It has the disaster recovery feature (multi-machine backup feature).

Note that there is no 2+N plan, that is, 1 master node, 1 sub-master node and N business nodes. The reason is that the sub-master node cannot be installed successfully, which makes it have the same effect as plan A.

### Before you begin:

- The network among all the nodes can be accessed. All the nodes can access the external network.
- YMS is not installed in all the nodes.
- [Downloading the Installation Package](#)
- [Unzipping the Installation Package](#)
- [Run the Installation Command](#)

### Downloading the Installation Package

- The server can access the external network

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

```
cd /usr/local
```

2. Run the following command to download the installation package (change x.x.x.x to the version you want to download):

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

- **The server cannot access the external network**

1. Manually download the installation package, which you obtain from Yealink technical support engineers.
2. Use SecureCRT to go to the command interface of the root account via SSH.
3. Run the command `cd /usr/local` to go to the directory (/usr/local).
4. Run the command `rz` and upload the Rom package on the pop-up window.

## Unzipping the Installation Package

### Procedure

Run the following command:

```
cd /usr/local #go to the directory where the
installation package is in#
tar xzf YMS_x.x.x.x.tar.gz # unzip the installation package
(change x.x.x.x to the version you want to install)#
cd apollo_install # go to the installation directory#
tar xzf install.tar.gz # unzip the installation script#
```

## Run the Installation Command

### Procedure

1. Run the following command:

```
./install.sh
```

```
已安装:
libtomcrypt.x86_64 0:1.17-26.e17      libtommath.x86_64 0:0.42.0-6.e17
sshpas.x86_64 0:1.06-2.e17

完毕!

Default profile /usr/local/apollo/data/install.conf does not exist.
please make a choice:
!!! timeout 30 seconds, timeout default is [A].
[A]. Deploy allinone with default 127.0.0.1
[B]. Create default profile and then exit to edit it

Please input your choice:
```

2. Enter B to select the cluster installation.
3. Run the following command:

```
vi /usr/local/apollo/data/install.conf
```

4. Enter A to edit the configuration file.



```

10.82.24.202 (1)
[global] #Global variable configuration.
ansible_ssh_user = root #The default root authority, used for logging into the backend server.
ansible_ssh_pass = Yealink@2018 #You can set the same backend login password for all nodes for unified specifying in this sentence.
# ansible_ssh_private_key_file= #No need configuration.

[manager-master] #The IP address of the master node.
ip=10.82.24.202
# ansible_ssh_user=root #The backend login password of the root authority of the master node. The password is set in the global
# configuration, so you do not need set the password again here.

[manager-slave-1]
ip=10.82.24.203 #The IP address of the sub-master node.

[manager-slave-2]
ip=10.82.24.204

[business-1]
ip=10.82.24.208 #The IP address of the business node.

[business-2]
# ip=x.x.x.x

[business-3]
# ip=x.x.x.x
-- INSERT --

```

5. Press Esc to exit, and run the following command:

```

:wq #save the configuration file #
./install.sh #install the cluster YMS#

```

The installation starts and it takes about 30 minutes. After the installation is finished, use the IP address of any master node to log into YMS.

## Expanding the Stand-Alone YMS

For the stand-alone YMS, if you want to strengthen its MCU by making it become 1+N (N can be 1, 2, 3, 4, 5, 6.....). That is one master node and N business nodes, and then you can expand your YMS.

### Before you begin

- The network among all the nodes can be accessed. All the nodes can access the external network.
- YMS is not installed in all the nodes.

### Procedure

1. Use SecureCRT to go to the command interface of the root account via SSH.
2. Run the following command.

```
vi /usr/local/apollo/data/install.conf
```

3. Enter A to edit the configuration file.

```

10.86.0.33 - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
10.86.0.33
[global]
# ansible_ssh_user = root
# ansible_ssh_pass = XXXXXX
# ansible_ssh_private_key_file=

[manager-master]
ip=10.86.0.33
ansible_ssh_user=root
ansible_ssh_pass = 123456

[manager-slave-1]
# ip=x.x.x.x

[manager-slave-2]
# ip=x.x.x.x

[business-1]
ip=10.86.0.55
ansible_ssh_user=root
ansible_ssh_pass = Yealink1105

[business-2]
-- INSERT --
就绪          ssh2: AES-256-CTR    21, 31    24行, 80列    VT100          大写 数字

```

4. Press Esc to exit, and run the following command.

```

: wq
cd /usr/local/apollo_install/
./install.sh

```

## Results

After the installation is finished, you can see multiple nodes in the **Node Management** page. You can set them as the MCU business nodes to expand the MCU.

## Upgrading YMS 2.X

When a new version is available, you can upgrade your YMS. You can contact Yealink technical support engineers to get the latest software.

- [Upgrading YMS 2.X via the Command](#)
- [Upgrading YMS 2.X via the Web Interface](#)

### Upgrading YMS 2.X via the Command

#### Procedure

1. Use SecureCRT to go to the command interface of the root account via SSH.
2. Run the following command to go to the directory (/usr/local):

```
cd /usr/local
```

3. Run the following command to delete the apollo\_install folder under the directory (/usr/local):

```
rm -rf apollo_install
```

4. Run the following command to upload the ROM package.

```
rz
```

5. Run the following command to unzip the ROM package:

```
tar xzf YMS_x.x.x.x.tar.gz
```

6. Run the following command to go to the installation directory:

```
cd apollo_install
```

7. Run the following command to unzip the installation script:

```
tar xzf install.tar.gz
```

8. Run the following command to run the deployment script:

```
./install.sh
```

## Upgrading YMS 2.X via the Web Interface

### About this task



**Note:** For YMS version 2.0 or later, you can update them seamlessly via the web page. If you access YMS from the external network, we do not recommend you upgrade YMS2.X via the web interface. [Upgrading YMS 2.X via the Command](#) is recommended.

### Procedure

1. Click **Maintenance > Upgrade**.
2. Click **Update**, select the installation package, and update YMS.

### System Upgrade

Current version :

24.0.0.3

Update

## Uninstalling YMS 2.X

### About this task



**Note:** Generally, you do not need to uninstall YMS 2.X. If you need to uninstall YMS2.X, you should contact Yealink technical support engineers first and then uninstall YMS.

### Procedure

1. Use SecureCRT to go to the command interface of the root account via SSH.
2. Run the command `/usr/local/apollo_install` to go to the directory.

- Run the command `apollo-uninstall` to uninstall the script.  
For the cluster deployment, you need to run the uninstalling command on every node.
- Enter the password, which you obtain from Yealink technical support engineers.

```
[root@localhost apollo_install]# apollo-uninstall
|-----|
|      卸载 YMS      |
|-----|
Please Input Password:
Are you sure you want to uninstall Apollo YMS?([y/n]): y
Do you want to keep the YMS data?([y/n]): n
```

## Getting Started

---

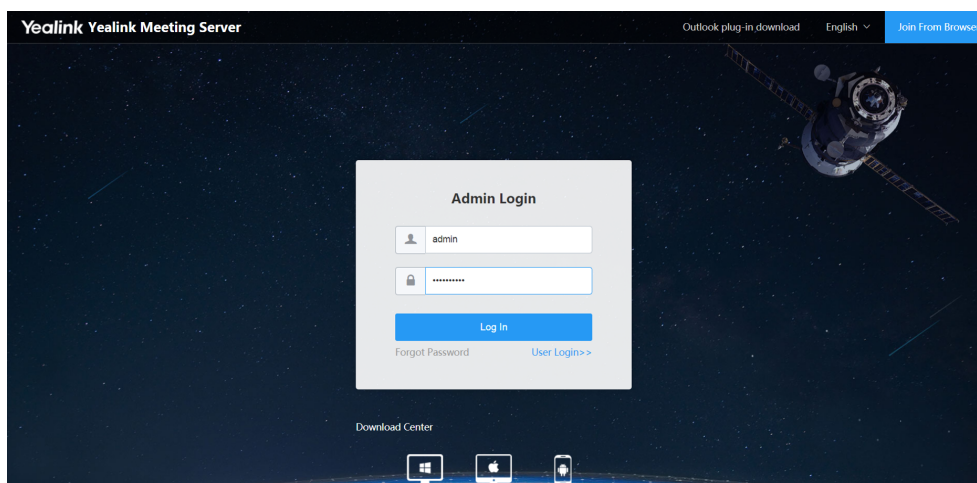
- [Logging into YMS](#)
- [Setting the Setup Wizard](#)
- [System Settings](#)
- [Service Settings](#)
- [Activating a License](#)
- [Creating Accounts](#)
- [Creating Meeting Rooms](#)
- [Managing Conferences](#)
- [The Checklist for the Configurations and the Common Features](#)

## Logging into YMS

---

### Procedure

- Enter the IP address or the domain name of YMS in the address bar to go to the Login page.  
If you log in via HTTPS, the page might prompt that the access is insecure, you can [Importing the HTTPS Certificate](#) to solve this problem.
- Click **Admin Login**, enter the username and the password to log in.  
By default, the username is admin and the password is v12345678. If it is the first time you log into YMS, you are required to change the password.



## Setting the Setup Wizard

To meet the necessary call and conference need, you can configure the server according to the setup wizard.

### About this task

When you log in for the first time, the setup wizard will pop up automatically.

### Procedure

1. If you close the setup wizard, you can click **Setup Wizard** at the top of the page to open it again.

## Setup Wizard



- 1 Primary Domain**  
 Primary domain is used for the authentication of account registration.  
 Please click System Setting > Common Setting > [Network Association](#) to set up.
- 2 Change Password**  
 For information security, please change your admin password as soon as possible.  
 Please click [Admin Account](#) to set up.
- 3 Time/Time Zone**  
 Please setup the correct server time to make sure all applications operate properly. Server acquires date and time from NTP server by default. Date and time can also be configured manually.  
 Please click System Setting > Common Setting > [Time](#) to set up.
- 4 SMTP Mailbox**  
 SMTP Mailbox is used to send system emails, such as conference schedule email, account info email, etc.  
 Please click System Setting > Common Setting > [SMTP Mailbox](#) to set up.
- 5 Node Network**  
 To ensure smooth network, please setup the basic server node information.  
 Please click System Setting > [Node Management](#) to set up.
- 6 Registration Service**  
 Please setup registrar service to make sure system accounts can be registered properly on intranet

For more information, please refer to the Administrator's Guide.

Don't show me these options again.

2. [Setting the Primary Domain Name](#) .
3. [Editing the Login Password](#) .
4. [Configuring Sntp](#) .
5. [Configuring the SMTP Mailbox](#) .
6. [Setting the Node](#) .
7. [Setting the Registration Service](#) .
8. [Setting the Traversal Service](#) .

- 9. [Setting the Interactive Media Service](#) .
- 10. [Activating a License](#) .

## System Settings

---

- [Setting the Primary Domain Name](#)
- [Editing the Login Password](#)
- [Configuring Sntp](#)
- [Configuring the SMTP Mailbox](#)
- [Setting the Node](#)

### Setting the Primary Domain Name

You can configure the domain name for the authentication or the access. When you register an account on a device, the server address you enter in is this domain name.

#### Procedure

1. Click **System Setting > Common Setting > Network Association**.
2. Enter the domain name in the **Primary domain** field, and save it.

The default domain name is <your server IP>.xip.io and xip.io is an open domain name. By default, the domain name is resolved as the IP address before xip.io. For example, 10.10.10.10.xip.io is resolved as 10.10.10.10 via DNS.

<a href="#">Network Association</a>	<a href="#">Time</a>	<a href="#">Data Space</a>	<a href="#">SMTP Mailbox</a>	<a href="#">Number Resource Allocation</a>
* Primary domain :	<input type="text" value="10.83.1.150.xip.io"/>			
Cluster ID :	<input type="text" value="14edad73cd324aad92372d63503521a4"/>			

### Editing the Login Password

For the account security, we recommend that you change your password regularly.

#### Procedure

1. Click the account name in the top-right corner.
2. In the **Password** field, click **Change**.
3. Change the password and save it.

### Change Password ✕

1、 Your password has to be 8 to 20 characters long.  
 2、 Must contain at least one character from three of the following categories: digits、 letters、 special characters ( !@#\$%^&\* ).

\* Current password :

\* New password :  ✕

Password strength : Strong

\* Confirm password :

OK
Cancel

## Configuring SNTP

By default, YMS uses the SNTP server to obtain accurate system time.

### About this task



**Note:** Make sure the system time is correct. Otherwise, the services, for example, the conference service, will be abnormal.

### Procedure

1. Click **System Setting > Common Setting > Time**.
2. Configure the parameters.

Network Association
Time
Data Space
SMTP Mailbox
Number Resource Allocation

**Current server time :** 2019-09-17 09:06:10 UTC+08:00

**Time access :**  SNTP  Date & time configuration

**Server domain :**

+ Add

**i18n.ntp.services.75859**  OFF

**Timezone :** (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi ▼

**Auto adjust conference DST :** Close ▼

**Table 8: Time parameter**

Parameter	Description
<b>Time access</b>	Select the desired method to obtain the system time. <ul style="list-style-type: none"> <li>• <b>SNTP</b></li> <li>• <b>Date &amp; time configuration</b></li> </ul> <b>Default:</b> SNTP.
<b>Server domain</b>	If you select <b>SNTP</b> , configure the SNTP server. <b>Note:</b> the first server address is the primary server by default, and its default value is pool.ntp.org.
<b>Date &amp; time</b>	If you select <b>Date &amp; time configuration</b> , configure the time and date manually.
<b>Auto adjust conference DST</b>	Configure the type of DST. <ul style="list-style-type: none"> <li>• <b>Enabled</b>—YMS uses the corresponding DST automatically according to the time zone you set. When users schedule conferences in countries using the DST, the DST is enabled by default.</li> <li>• <b>Close</b>—DST is disabled.</li> </ul> <b>Default:</b> disabled.

3. Save the configuration and the system reboots.

## Configuring the SMTP Mailbox

You can use the SMTP mailbox to inform users about the related information, for example, the account information.

### Procedure

1. Click **System Setting > Common Setting > SMTP Mailbox**.
2. Configure the parameters.



Network Association	Time	Data Space	<b>SMTP Mailbox</b>	Number Resource Allocation
SMTP server :	<input type="text" value="smtp.yealinkops.com"/>			
Mailbox :	<input type="text" value="yms@yealinkops.com"/>			
Username :	<input type="text" value="yms@yealinkops.com"/>			
Password :	<input type="password" value="*****"/>			
Port :	<input type="text" value="465"/>	(Only 1~65535)		
	<input checked="" type="checkbox"/> This server requires a secure connection			
	<input type="text" value="SSL"/>			

3. Click **Test Mailbox Setting** to test whether the configuration is correct.

If the mailbox connection is successful, the prompt “Operation Successful” is popped up.

## Test Mailbox Setting ×

Test mailbox :

4. Save the configuration.

#### Related information

[Failing to Connect to SMTP](#)

## Setting the Node


For YMS 2.X, you need to set the node first and then configure the service. In different network environments, the node configuration varies. Before you configure the node, check the network environment first. In this part, we introduce six configuration methods about the common network environment.

For the stand-alone YMS, you need to configure one node. However, for the cluster YMS, you need to configure several nodes. In this part, we take the stand-alone configuration as an example.

**Go to the page of Node Management:**

1. Click **System Setting > Node Management**.

For the cluster version, you can see the information of several nodes.

2. Click  on the right of the desired node to edit the node.



**Note:** Note that you cannot disable the node casually. Otherwise, you can only control the server by connecting a display to the server rather than controlling the server via the web interface.

For NAT deployment, you need to configure the address port mapping first.

**Go to the page of Address Port Mapping:**

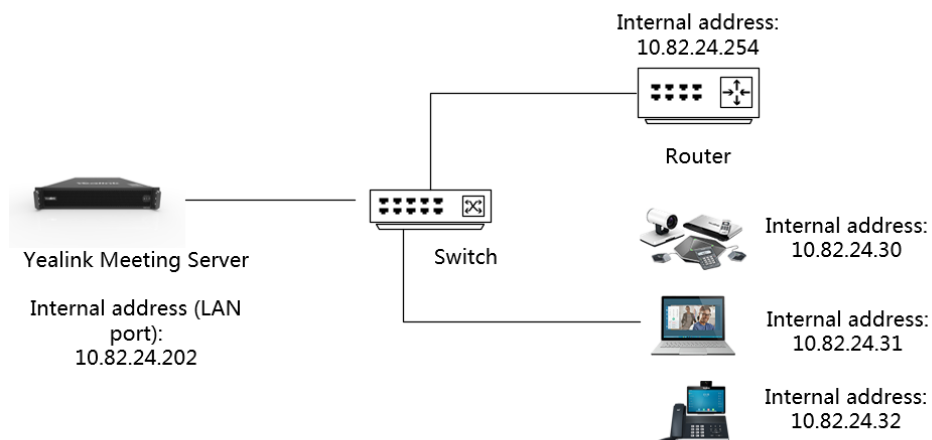
1. Click **System Setting > Address Port Mapping**.

2. Add an address port mapping.

- [Internal Deployment with One-IP NIC](#)
- [External Deployment with One-IP NIC](#)
- [External Deployment with One-IP NIC \(with NAT\)](#)
- [Internal and External Deployment with Dual-IP NIC \(with NAT\)](#)
- [Internal and External Deployment with Dual NIC](#)
- [Internal and External Deployment with Dual NIC \(with NAT\)](#)

**Internal Deployment with One-IP NIC**

If you register YMS accounts, place point-to-point calls or join video conferences only in the internal network, you can deploy YMS by this method. You only need to configure the internal NIC on YMS to finish the deployment.



**Go to the page of Node Management, and check the following configuration:**

- **Network**

**Edit Node** Cancel

Enabled :

\* Node name :   
The node name should be identifiable.

Network and Routing Configuration

ens192  Enabled Network status : Connected

Single NIC

Single IP address

Selected 0

Name	IPv4 Address	Subnet Mask	Public IP	Enabled	Operation
10.82.24.202	10.82.24.202	255.255.255.0		<input checked="" type="checkbox"/>	<input type="button" value="✎"/>

• **Gateway**

Enabled :

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

\* IPv4 default gateway :

\* IPv4 gateway priority :   
The higher the value, the lower the priority.

• **DNS**

Enabled :

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

Preferred DNS :

Alternate DNS :

• **Routing Rules**

Enabled :  ON

\* Node name :

---

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules

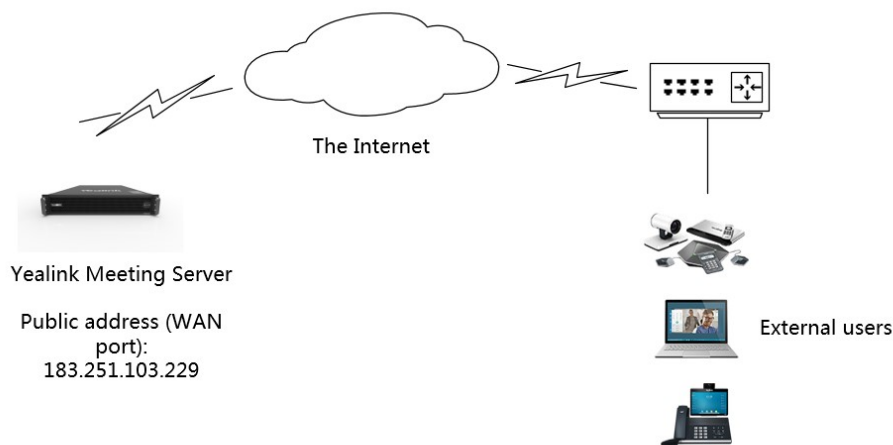
This routing rule is generated automatically and you cannot edit or delete it.

<input type="checkbox"/>	Destination network address	Gateway	Source IP	Priority	Enabled	Operation
<input type="checkbox"/>	10.82.24.0/24	---	10.82.24.202	0	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>
<input type="checkbox"/>	169.254.0.0/16	---	Default	1002	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>
<input type="checkbox"/>	default	10.82.24.254	Default	0	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>

The default routing rule One-IP NIC, and you can set it as the default one.

### External Deployment with One-IP NIC

If you register YMS accounts, place point-to-point calls or join video conferences only in the external network, you can deploy YMS by this method. You only need to configure the external NIC on YMS to finish the deployment.



Go to the page of Node Management, and check the following configuration:

- Network

Enabled :  ON

\* Node name :

The node name should be identifiable.

---

Network and Routing Configuration

ens192  Enabled Network status : Connected

Single NIC

Network Gateway DNS Routing Rules

Selected 0

<input type="checkbox"/>	Name	IPv4 Address	Subnet Mask	Enable this Public IP	Enabled	Operation
<input type="checkbox"/>	183.251.103.229	183.251.103.229	255.255.255.0	<input checked="" type="checkbox"/> ON	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>

Single IP address

- Gateway

Enabled :

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

\* IPv4 default gateway :

\* IPv4 gateway priority :   
The higher the value, the lower the priority.

• DNS

Enabled :

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

Preferred DNS :

Alternate DNS :

• Routing Rules

Enabled :

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

This routing rule is generated automatically and you cannot edit or delete it.

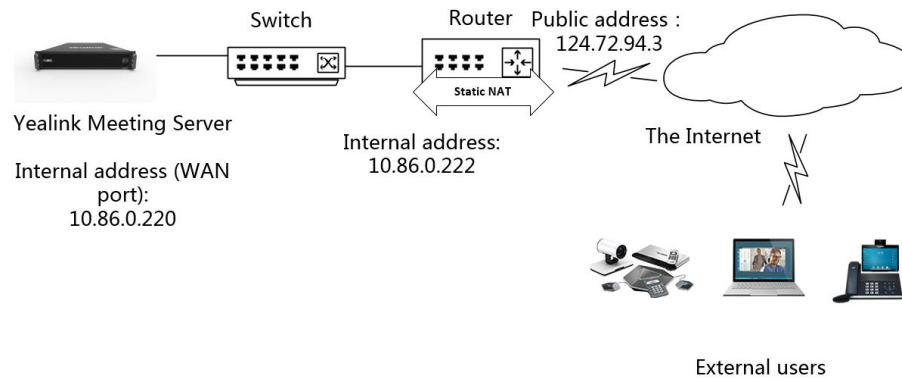
Destination network address	Gateway	Source IP	Priority	Enabled	Operation
<input type="checkbox"/> 183.251.103.0/24	--	183.251.103.229	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 169.254.0.0/16	--	Default	1002	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> default	183.251.103.254	Default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The default routing rule One-IP NIC, and you can set it as the default one.

## External Deployment with One-IP NIC (with NAT)

To secure YMS and the internal network, you can deploy YMS in the internal network and map the address by static NAT on the router and YMS. Therefore, users in the external network can access YMS.

The server has only one NIC and is only deployed with one IP, providing the external service rather than the internal service.



Go to the page of Node Management, and check the following configuration:

- Open the external service port in [Port Requirements of the Router](#).
- Network

Enabled :

\* Node name :   
 The node name should be identifiable.

---

Network and Routing Configuration

ens192  Enabled Network status : Connected

Single NIC

Selected 0

Name	IPv4 Address	Subnet Mask	Enable this Public IP	Enabled	Operation
Single IP address	10.86.0.220	255.255.255.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>

- Gateway

Enabled :  ON

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

\* IPv4 default gateway :

\* IPv4 gateway priority :

The higher the value, the lower the priority.

• DNS

Enabled :  ON

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

Preferred DNS :

Alternate DNS :

• Routing Rules

Enabled :  ON

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

This routing rule is generated automatically and you cannot edit or delete it.

Destination network address	Gateway	Source IP	Priority	Enabled	Operation
<input type="checkbox"/> 10.86.0.0/24	---	10.86.0.220	0	<input checked="" type="checkbox"/> ON	<input type="button" value="✎"/>
<input type="checkbox"/> 169.254.0.0/16	---	Default	1002	<input checked="" type="checkbox"/> ON	<input type="button" value="✎"/>
<input type="checkbox"/> default	10.86.0.254	Default	0	<input checked="" type="checkbox"/> ON	<input type="button" value="✎"/>

The default routing rule One-IP NIC, and you can set it as the default one.

Go to the page of Address Port Mapping, and check the following configuration:

- **Address Port Mapping**

Map the node 10.86.0.220 to the public network 124.72.94.3. Configure the port according to the business demand. The address port mapping should be the same as the mapping on the router.

**Add Configuration**

\* Enable :  ON

\* Name :

\* Public IP :

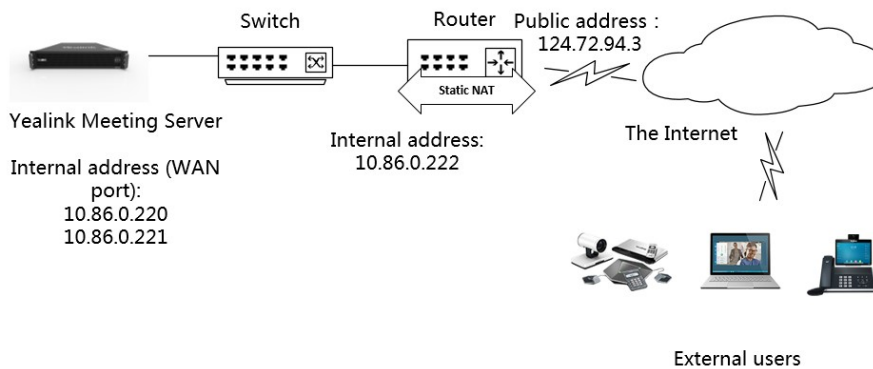
\* Public Port :  ~

\* Internal IP :

\* Internal Port :  ~

### Internal and External Deployment with Dual-IP NIC (with NAT)

To secure YMS and the internal network, you can deploy YMS in the internal network and map the address by static NAT on the router and YMS. Therefore, users in the external network can access YMS.



Go to the page of Node Management, and check the following configuration:

- Open the external service port in [Port Requirements of the Router](#) .



• Network

Enabled :  ON

\* Node name :   
The node name should be identifiable.

---

Network and Routing Configuration

ens192  Enabled Network status : Connected

Single NIC

Network Gateway DNS Routing Rules ?

Selected 0  For the externally-facing node, enable this

<input type="checkbox"/>	Name	IPv4 Address	Subnet Mask	Public IP	Enabled	Operation
<input type="checkbox"/>	10.86.0.220	10.86.0.220	255.255.255.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="✎"/>
<input type="checkbox"/>	10.86.0.221	10.86.0.221	255.255.255.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="✎"/>

Dual IP address  
We recommend that you use the same network segment

• Gateway

Enabled :  ON

\* Node name :

---

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

\* IPv4 default gateway :

\* IPv4 gateway priority :   
The higher the value, the lower the priority.

• DNS

Enabled :  ON

\* Node name :

---

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

Preferred DNS :

Alternate DNS :

- **Routing Rules**

Enabled :

\* Node name : Default(10.86.0.220/221)

Network and Routing Configuration

ens192  Enabled Network status : Connected

Network Gateway DNS Routing Rules ?

This routing rule is generated automatically and you cannot edit or delete it.

Destination network address	Gateway	Source IP	Priority	Enabled	Operation
<input type="checkbox"/> 169.254.0.0/16	---	Default	1002	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 10.86.0.0/24	---	10.86.0.221	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 192.168.0.0/16	10.86.0.254	10.86.0.221	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 172.16.0.0/12	10.86.0.254	10.86.0.221	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 10.0.0.0/8	10.86.0.254	10.86.0.221	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> default	10.86.0.254	10.86.0.220	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The routing rule for the internal network

The default routing rule

Specify those NICs to provide services of internal network.

Specify this NIC to provide services of external network.

**Go to the page of Address Port Mapping, and check the following configuration:**

- **Address Port Mapping**

Map the node 10.86.0.220 to the public network 124.72.94.3. Configure the port according to the business demand. The address port mapping should be the same as the mapping on the router.

**Add Configuration**

\* Enable :

\* Name : NAT deployment 1

\* Public IP : 124.72.94.3

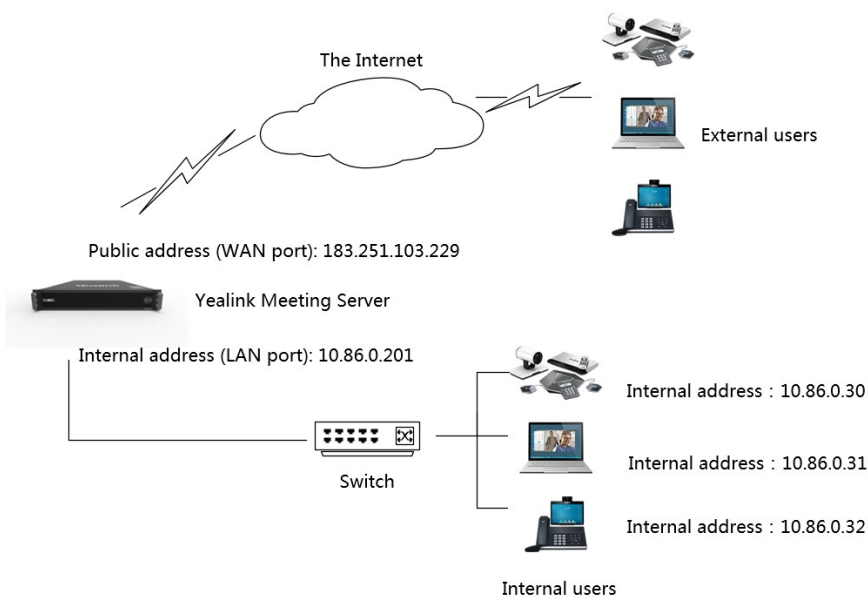
\* Public Port : 500 ~ 65499

\* Internal IP : 10.86.0.220 Enable the externally-facing node

\* Internal Port : 500 ~ 65499

## Internal and External Deployment with Dual NIC

If you register YMS accounts, place point-to-point calls or join video conferences in both the internal network and the external network, you can deploy YMS by this method. You need to configure the external and the internal NICs on YMS.



Go to the page of Node Management, and check the following configuration:

- Network

Configuration of the internal NIC

Enabled :

\* Node name :

The node name should be identifiable.

Network and Routing Configuration

ens192	ens195	Dual NIC					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Network status : Connected					
		Network	Gateway	DNS	Routing Rules ?		
		Selected 0 <input type="button" value="Delete"/>					<input type="button" value="+ Add"/>
<input type="checkbox"/>	<input type="checkbox"/>	Name	IPv4 Address	Subnet Mask	Public IP	Enabled	Operation
<input type="checkbox"/>	<input type="checkbox"/>	10.86.0.201	10.86.0.201	255.255.255.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="✎"/>

Configuration of the external NIC

Enabled :

\* Node name :

The node name should be identifiable.

Network and Routing Configuration

ens192	ens195	Dual NIC					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Network status : Connected					
		Network	Gateway	DNS	Routing Rules ?		
		Selected 0 <input type="button" value="Delete"/>					<input type="button" value="+ Add"/>
<input type="checkbox"/>	<input type="checkbox"/>	Name	IPv4 Address	Subnet Mask	Public IP	Enabled	Operation
<input type="checkbox"/>	<input type="checkbox"/>	183.251.103.229	183.251.103.229	255.255.255.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="✎"/>

For the externally-facing node, enable this

- Gateway

## Configuration of the internal NIC

Enabled :

ON 

\* Node name :

Dual-NIC

Save

Cancel

## Network and Routing Configuration

ens192	<input checked="" type="checkbox"/> Enabled	Network status : Connected
ens195	<div style="display: flex; justify-content: space-between;"> <span>Network</span> <span style="background-color: #007bff; color: white; padding: 2px 5px;">Gateway</span> <span>DNS</span> <span>Routing Rules ?</span> </div>	
Dual NIC	* IPv4 default gateway :	<input type="text" value="10.86.0.254"/>
	* IPv4 gateway priority :	<input type="text" value="3"/> <span style="color: orange;">Set a higher value than the one in the external NIC</span>
		<small>The higher the value, the lower the priority.</small>
		<input type="button" value="Save"/>

## Configuration of the external NIC

Enabled :

ON 

\* Node name :

Dual-NIC

Save

Cancel

## Network and Routing Configuration

ens192	<input checked="" type="checkbox"/> Enabled	Network status : Connected
ens195	<div style="display: flex; justify-content: space-between;"> <span>Network</span> <span style="background-color: #007bff; color: white; padding: 2px 5px;">Gateway</span> <span>DNS</span> <span>Routing Rules ?</span> </div>	
Dual NIC	* IPv4 default gateway :	<input type="text" value="183.251.103.254"/>
	* IPv4 gateway priority :	<input type="text" value="0"/> <span style="color: orange;">Set it as 0 to make it have higher priority than the internal NIC</span>
		<small>The higher the value, the lower the priority.</small>
		<input type="button" value="Save"/>

- DNS

## Configuration of the internal NIC

Enabled :  ON

\* Node name :

Dual-NIC

Save

Cancel

Network and Routing Configuration

ens192	<input checked="" type="checkbox"/> Enabled	Network status : Connected
ens195	<div style="display: flex; border: 1px solid #ccc; padding: 2px;"> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;">Network</div> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;">Gateway</div> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px; background-color: #007bff; color: white;">DNS</div> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;">Routing Rules ?</div> </div>	
Dual NIC	Preferred DNS :	<input type="text" value="10.100.1.10"/>
	Alternate DNS :	<input type="text" value="192.168.1.22"/>
		<input type="button" value="Save"/>

## Configuration of the external NIC

Enabled :  ON

\* Node name :

Dual-NIC

Save

Cancel

Network and Routing Configuration

ens192	<input checked="" type="checkbox"/> Enabled	Network status : Connected
ens195	<div style="display: flex; border: 1px solid #ccc; padding: 2px;"> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;">Network</div> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;">Gateway</div> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px; background-color: #007bff; color: white;">DNS</div> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;">Routing Rules ?</div> </div>	
Dual NIC	Preferred DNS :	<input type="text" value="192.168.0.1"/>
	Alternate DNS :	<input type="text"/>
		<input type="button" value="Save"/>

- **Routing Rules**

### Configuration of the internal NIC

Enabled :  ON

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

ens195  Disabled Network status : Disconnected

Dual NIC

This routing rule is generated automatically and you cannot edit or delete it.

Destination network address	Gateway	Source IP	Priority	Enabled	Operation
169.254.0.0/16	--	Default	1002	<input checked="" type="checkbox"/> ON	<input type="checkbox"/>
10.86.0.0/24	--	10.86.0.201	0	<input checked="" type="checkbox"/> ON	<input type="checkbox"/>
192.168.0.0/16	10.86.0.254	10.86.0.201	0	<input checked="" type="checkbox"/> ON	<input type="checkbox"/>
172.16.0.0/12	10.86.0.254	10.86.0.201	0	<input checked="" type="checkbox"/> ON	<input type="checkbox"/>
10.0.0.0/8	10.86.0.254	10.86.0.201	0	<input checked="" type="checkbox"/> ON	<input type="checkbox"/>
default	10.86.0.254	Default	0	<input type="checkbox"/> OFF	<input type="checkbox"/>

The routing rule for the internal network

Specify those NICs to provide services of internal network.

The default routing rule

Disable it or delete this rule.

### Configuration of the external NIC

Enabled :  ON

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

ens195  Disabled Network status : Disconnected

Dual NIC

This routing rule is generated automatically and you cannot edit or delete it.

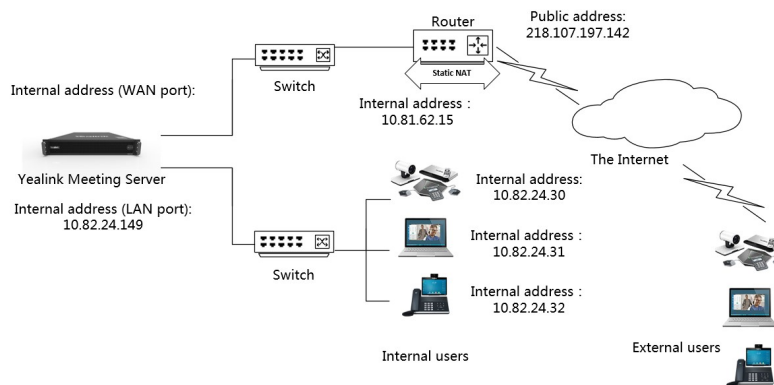
Destination network address	Gateway	Source IP	Priority	Enabled	Operation
183.251.103.0/24	--	183.251.103.229	0	<input checked="" type="checkbox"/> ON	<input type="checkbox"/>
169.254.0.0/16	--	Default	1002	<input checked="" type="checkbox"/> ON	<input type="checkbox"/>
default	183.251.103.254	Default	0	<input checked="" type="checkbox"/> ON	<input type="checkbox"/>

The default routing rule

One IP address and you can set it as the default one.

## Internal and External Deployment with Dual NIC (with NAT)

To secure YMS and the internal network, you can deploy YMS in the internal network and map the address by static NAT on the router and YMS. Therefore, users in the external network can access YMS. You need to configure the external and the internal NICs on YMS.



Go to the page of Node Management, and check the following configuration:

- Open the external service port in *Port Requirements of the Router* .
- Network

Configuration of the internal NIC

Enabled :  ON

\* Node name :

The node name should be identifiable.

Network and Routing Configuration

ens192	<input checked="" type="checkbox"/> Enabled	Network status : Connected												
ens195	<input checked="" type="checkbox"/> Enabled	Network status : Connected												
<p>Dual NIC</p> <p>Selected 0 <input type="button" value="Delete"/> <input type="button" value="+ Add"/></p> <table border="1"> <thead> <tr> <th>Name</th> <th>IPv4 Address</th> <th>Subnet Mask</th> <th>Public IP</th> <th>Enabled</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> 10.82.24.149</td> <td>10.82.24.149</td> <td>255.255.255.0</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/> ON</td> <td><input type="button" value="Edit"/></td> </tr> </tbody> </table>			Name	IPv4 Address	Subnet Mask	Public IP	Enabled	Operation	<input type="checkbox"/> 10.82.24.149	10.82.24.149	255.255.255.0	<input type="checkbox"/>	<input checked="" type="checkbox"/> ON	<input type="button" value="Edit"/>
Name	IPv4 Address	Subnet Mask	Public IP	Enabled	Operation									
<input type="checkbox"/> 10.82.24.149	10.82.24.149	255.255.255.0	<input type="checkbox"/>	<input checked="" type="checkbox"/> ON	<input type="button" value="Edit"/>									

Configuration of the external NIC

Enabled :  ON

\* Node name :

The node name should be identifiable.

Network and Routing Configuration

ens192	<input checked="" type="checkbox"/> Enabled	Network status : Connected												
ens195	<input checked="" type="checkbox"/> Enabled	Network status : Connected												
<p>Dual NIC</p> <p>Selected 0 <input type="button" value="Delete"/> <input type="button" value="+ Add"/></p> <p style="text-align: right; color: orange;">For the externally-facing node, enable this</p> <table border="1"> <thead> <tr> <th>Name</th> <th>IPv4 Address</th> <th>Subnet Mask</th> <th>Public IP</th> <th>Enabled</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> 10.81.62.14</td> <td>10.81.62.14</td> <td>255.255.255.0</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/> ON</td> <td><input type="button" value="Edit"/></td> </tr> </tbody> </table>			Name	IPv4 Address	Subnet Mask	Public IP	Enabled	Operation	<input type="checkbox"/> 10.81.62.14	10.81.62.14	255.255.255.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ON	<input type="button" value="Edit"/>
Name	IPv4 Address	Subnet Mask	Public IP	Enabled	Operation									
<input type="checkbox"/> 10.81.62.14	10.81.62.14	255.255.255.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ON	<input type="button" value="Edit"/>									

- Gateway

Configuration of the internal NIC

Enabled :  ON

\* Node name :

Network and Routing Configuration

ens192	<input checked="" type="checkbox"/> Enabled	Network status : Connected
ens195	<input checked="" type="checkbox"/> Enabled	Network status : Connected
<p>Dual NIC</p> <p><input type="button" value="Network"/> <input checked="" type="button" value="Gateway"/> <input type="button" value="DNS"/> <input type="button" value="Routing Rules ?"/></p> <p>* IPv4 default gateway : <input type="text" value="10.82.24.254"/></p> <p>* IPv4 gateway priority : <input type="text" value="3"/> <span style="color: orange;">Set a higher value than the one in the external NIC</span></p> <p>The higher the value, the lower the priority.</p> <p><input type="button" value="Save"/></p>		

## Configuration of the external NIC

Enabled :  ON

\* Node name :

## Network and Routing Configuration

ens192  Enabled Network status : Connected

ens195

Dual NIC

\* IPv4 default gateway :

\* IPv4 gateway priority :  **Set it as 0 to make it have higher priority than the internal NIC**  
The higher the value, the lower the priority.

## • DNS

## Configuration of the internal NIC

Enabled :  ON

\* Node name :

## Network and Routing Configuration

ens192  Enabled Network status : Connected

ens195

Dual NIC

Preferred DNS :

Alternate DNS :



Configuration of the external NIC

Enabled :  ON

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

ens195

Dual NIC

Preferred DNS :

Alternate DNS :

• Routing Rules

Configuration of the internal NIC

Enabled :  ON

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

ens195

Dual NIC

This routing rule is generated automatically and you cannot edit or delete it.

Destination network address	Gateway	Source IP	Priority	Enabled	Operation
<input type="checkbox"/> 169.254.0.0/16	---	Default	1002	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>
<input type="checkbox"/> 10.86.0.0/24	---	10.82.24.149	0	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>
<input type="checkbox"/> 192.168.0.0/16	10.86.0.254	10.82.24.149	0	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>
<input type="checkbox"/> 172.16.0.0/12	10.86.0.254	10.82.24.149	0	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>
<input type="checkbox"/> 10.0.0.0/8	10.86.0.254	10.82.24.149	0	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>
<input type="checkbox"/> default	10.86.0.254	Default	0	<input type="checkbox"/> OFF	<input type="button" value="✕"/>

The routing rule for the internal network

Specify those NICs to provide services of internal network.

Disable it or delete this rule.

Configuration of the external NIC

Enabled :  ON

\* Node name :

Network and Routing Configuration

ens192  Enabled Network status : Connected

ens195

Dual NIC

This routing rule is generated automatically and you cannot edit or delete it.

Destination network address	Gateway	Source IP	Priority	Enabled	Operation
<input type="checkbox"/> 10.81.62.0/24	---	10.81.62.14	0	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>
<input type="checkbox"/> 169.254.0.0/16	---	Default	1002	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>
<input checked="" type="checkbox"/> default	10.81.62.254	Default	0	<input checked="" type="checkbox"/> ON	<input type="button" value="✕"/>

The default routing rule

One IP address and you can set it as the default one.

Go to the page of Address Port Mapping, and check the following configuration:

- **Address Port Mapping**

Map the node 10.81.62.14 to the public network 218.107.197.142. Configure the port according to the business demand. The address port mapping should be the same as the mapping on the router.

**Add Configuration**

---

\* Enable :  ON

\* Name :

\* Public IP :

\* Public Port :  ~

\* Internal IP :  Enable the externally-facing node ▼

\* Internal Port :  ~

---

## Service Settings

---


- [Setting the Registration Service](#)
- [Setting the Traversal Service](#)
- [Setting the Interactive Media Service](#)

### Setting the Registration Service

You need to configure the registration service for the user in the internal and the external network to register YMS accounts. When you are registering an endpoint with an account, the address of the proxy server directs to the address of this node.

#### About this task

If you want to connect YMS and the LDAP server to synchronize the accounts on YMS with the accounts on LDAP, you need to configure the LDAP first ([Configuring the LDAP](#)).

 **Note:** If the node NIC is configured with the internal and the external network IP, you need to configure the registration service for the internal and the external network respectively.

#### Procedure

1. Click **Service > SIP Service > Registration Service**.
2. Add a registration service.

### 3. Set the parameters.

**Add**

Enabled :  ON

\* Name :

\* Node :

**Service address**

\*Network  \*TLS Port

### 4. Optional: Configure the security policy.

For adding a security group, see [Adding a Security Group](#)

Enable security policy  ON

Mode :  Whitelist  Blacklist

Security Group

Please select the security group

Allow the IP address in this group to register.

Forbid the IP address in this group to register.

### 5. Save the configuration.

## Setting the Traversal Service

If you want to make P2P calls, join conferences or do other call related operations, you should enable the traversal service first.

### About this task

- If you use the cluster version and all nodes are deployed in the internal network, you must add the traversal service on the master node.
- If you use the cluster version and you want to allow the user in the internal and the external network to register accounts and join conferences, you must add the traversal service on the business node which is mapped to the internal and the external network. Adding the traversal service on the node only mapped to the internal network is not allowed. Otherwise, the traversal service might be abnormal.

### Procedure

1. Click **Service** > **Traversal Service**.
2. Add a traversal service.
3. Configure the parameter and save it.

\* Enabled :  ON

\* Name :

\* Node :

\* Listener(UDP & TCP) :

\* Spare listener(UDP & TCP) :

\* Relay port range :  ~

## Setting the Interactive Media Service

If you want to join the conferences or do other conference related operations, you should enable the interactive media service first.

### Procedure

1. Click **Service > MCU Service > Interactive Media Service**.
2. Add an interactive media service.
3. Set the parameter and save it.

\* Enabled :  ON

\* Name :

\* Node :

\* External media port :  ~

\* All local networks :  10.83.1.152

## Activating a License

---

You can activate the license to make sure that the video conference service works normally.

Follow the steps to activate the license: 1. Import the device certificate. 2. Activate the license online or offline.

- [Importing the Device Certificate to the Server](#)
- [Activating a License Online](#)
- [Activating a License Offline](#)
- [Disassociating the License](#)

## Importing the Device Certificate to the Server

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

### Before you begin

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

## Procedure

1. Click **System Setting > License**.
2. Click **Select File** and select the device certificate.



**Note:** One device certificate for one YMS, that is, if you have imported the device certificate to one YMS, you cannot import this certificate to another YMS.

3. Click **OK**.

## Results

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



## Activating a License Online

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

### Before you begin

- If [Importing the Device Certificate to the Server](#) is finished, the hardware information will be sent to Yealink License server automatically.
- You provide the device ID, the license type, the number of concurrent calls and the validity for Yealink. Yealink will generate the authentication based on the above information.

## Procedure

Click **System Setting > License > Refresh**.

## Results

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

### What to do next

If the authorization expires, you can apply for a new one from Yealink and then refresh the page.

### Related information

[Failing to Activate a License Online](#)

## Activating a License Offline

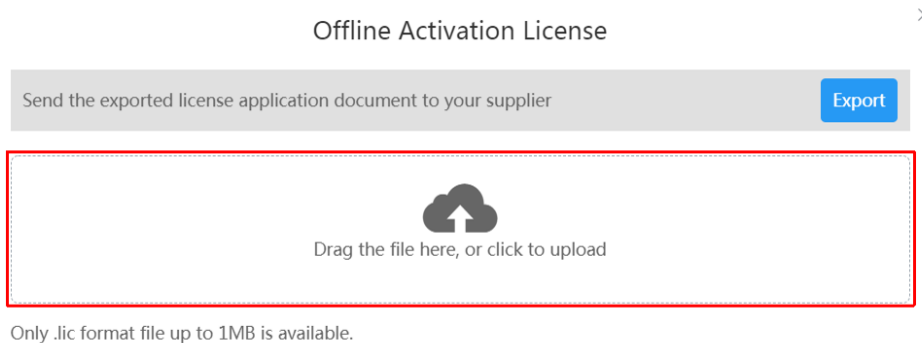
If the server cannot access the public network, you can activate the license offline.

### About this task

- [Importing the Device Certificate to the Server](#) is finished.
- You provide the device ID, the license type, the number of concurrent calls and the validity for Yealink. Yealink will generate the authentication based on the above information.

## Procedure

1. Click **System Setting > License > Offline Activation License**.
2. Click **Export**, and send the exported REQ file to Yealink. Yealink will generate the authentication after importing the REQ file. Yealink will generate the LIC authentication file and send it to you.
3. Click the area with the dotted box to upload the authorization file obtained from Yealink.



**Note:** The authentication file is unique, that is, different YMSs correspond to different authentication files. You cannot activate your server by importing the authentication files of other YMSs.

### Results

The license is displayed in the list.

### What to do next

If the authorization expires, you can apply for a new one from Yealink and import the new one.

### Related information

[Failing to Activate a License Offline](#)

## Disassociating the License

If you accidentally import the wrong device license, you can disassociate the license from the server.

### Procedure

1. Click **System Setting > License > Unbind License**.
2. Click **OK**.

### Results

If you disassociate the license from the server, the License page will return to the state of importing the device certificate. If you re-import the device certificate you apply for before, the related licenses will be imported too. If the device certificate is lost, you can see [Activating a License](#) to activate it again.

## Creating Accounts

The accounts can be divided into user accounts, room system accounts, other accounts, and LDAP accounts. This part mainly introduces how to create user accounts. For more information, refer to [Managing Accounts](#).

### Procedure

1. Click **Account > User Account**.
2. Add an account or import a batch of accounts.
  - **Add an account**

Basic Settings

Advanced Option

Account info :  Manual  Obtain from AD server

\* Name : test

\* Account : 8956

Password : .....

Password strength : Strong

A random password will be generated if not filled

Group : 1502.4 ×

Mailbox :

The mailbox is used to receive messages from system

Authority : A: All contacts are visible

 Enable schedule Enable Schedule Virtual Meeting Room (Cannot be opened at the same time with Schedule) Enable Meet Now

- **Import a batch of accounts**

Import

Instructions : please download templates and import data as required.

Download Template



Drag the file here, or click to upload

Only .xls format file is available, up to 5000 accounts can be imported each time.

OK

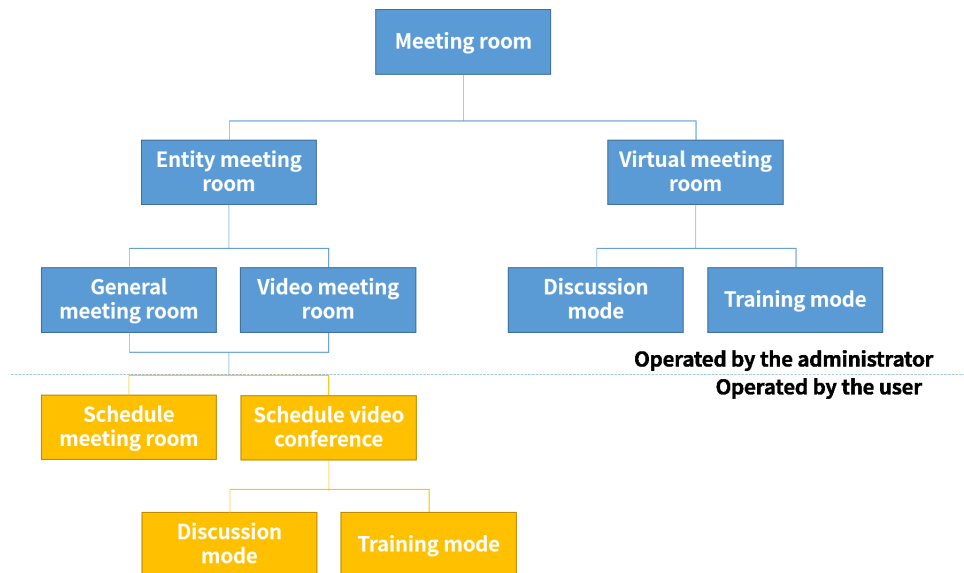
Cancel

3. Save the configuration.

## Creating Meeting Rooms

The meeting rooms include entity meeting rooms and virtual meeting rooms (VMR). This part mainly introduces how to create meeting rooms. For more information, refer to [Managing Meeting Rooms](#).

### About this task



### Procedure

1. Click **Meeting Room > Entity Meeting Room/Virtual Meeting Room**.
2. Add an entity meeting room or a VMR.

- **Adding Entity Meeting Rooms**

#### Add Meeting Room

\* Type :  Common  Video

\* Name :

\* Group :

- **Adding a VMR**



**Add Meeting Room**

Basic Settings

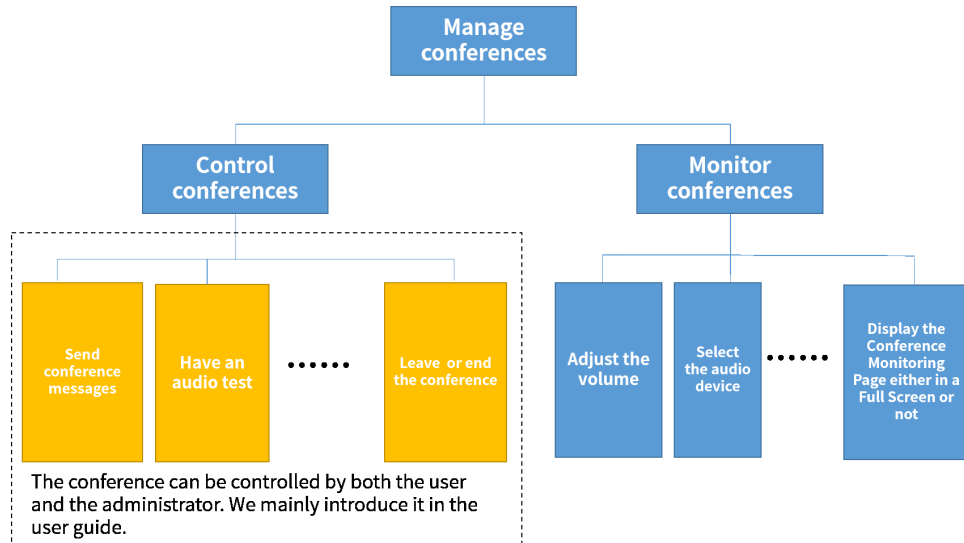
Advanced Option

**Common Setting**\* Name : \* Alias : \* Mode :  Discussion  Training\* Conference ID :  Require Password (Password is suggested for conference security)\* Password : ? \* Group :  ▾\* Organizer : ? Moderator : Favorites : **3. Save the configuration.**

## Managing Conferences

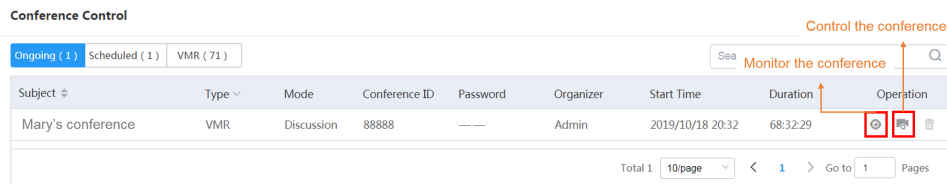
You can control and monitor the conferences. For more information, refer to [Managing Conferences](#) .

### About this task



### Procedure

Click **Conference > Conference Control**.



## The Checklist for the Configurations and the Common Features

You can check the configuration according to this checklist.

**Table 9: Checklist for the configurations**

No.	Item	Step	Result
1	Activate a license	Apply for it from Yealink technical support engineers.	
2	Account	Create accounts or import a batch of accounts	
3	Meeting room	Create entity meeting rooms and VMRs	
4	Set the registration service	Add a registration service	
5	Set the traversal service	Add a traversal service	

No.	Item	Step	Result
6	Set the interactive media service	Add an interactive media service	
7	Registration	Use the SIP account to register in	
8	P2P call	Make P2P calls between SIP accounts	
9	Join conferences	Call the VMR ID to join the conference	
10		Initiate Meet Now conferences	
11		Join the conference via a browser (WebRTC)	
12	Go to the user interface	Schedule entity meeting rooms	
13		Schedule video conferences	
14	Control the conferences	Invite participants to join the conference via the Conference Control page	
15		Share the content	

## System Setting

---

- *Basic Operations*
- *Setting the Web Service Address*
- *Setting the Log Service Address*
- *Setting the Time Zone*
- *Importing the Trusted CA Certificate*
- *Importing the HTTPS Certificate*
- *Importing the TLS Certificate*
- *Configuring the Port*
- *Setting the Data Space*
- *Allocating the Number Resource*
- *Setting the IP Property*
- *Setting the Intelligent Security Strategy*
- *Adding a Security Group*
- *Deleting the Abnormal IP*
- *Applying for the Accesskey*
- *Adding the User-Agent Blacklist*
- *Adding the User-Agent Compatible List*
- *Configuring the Email Template*
- *Setting SIP Trunk IVR*
- *Setting the Audio IVR*
- *Setting IVR language*

## Basic Operations

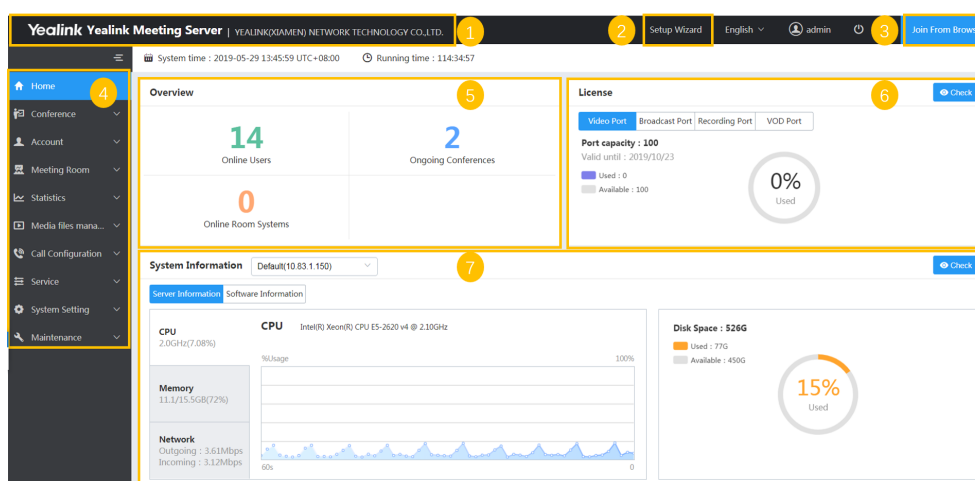
---

This chapter provides basic operations for the enterprise administrator to use YMS.

- [Introduction of the Home Page](#)
- [Changing the Display Language for the Website](#)
- [Editing the Registered Email](#)
- [Setting the Session Timeout](#)
- [Enabling Forced Https Authentication](#)
- [Adding a Sub Admin Account](#)
- [Customizing the Theme](#)
- [Setting the Password Policy](#)
- [Logging out of YMS](#)

## Introduction of the Home Page

The layout of the Home page is helpful for you to familiarize yourself with various operation interfaces and system notifications. YMS supports the management with different privileges. The system administrator account has the highest operation privilege on YMS. Accounts with different privileges will see different Home pages. Here is the Home page viewed by the system administrator account.



**Table 10:**

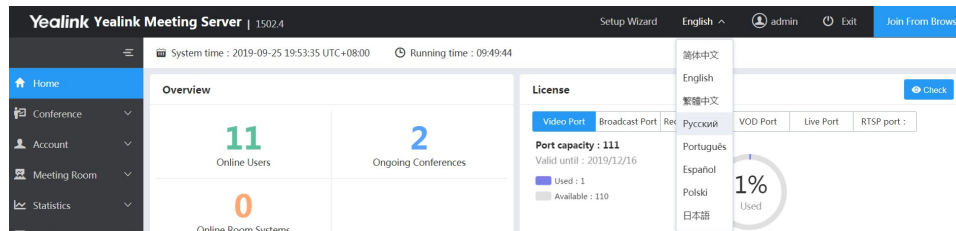
Number	Description
1	Go to the Home page quickly.
2	Go to the Setup Wizard.
3	Join the conference by browser. For more information, refer to <a href="#">Yealink Web App User Guide</a> .
4	The navigation bar.
5	<ul style="list-style-type: none"> <li>• View the number of the online users, the ongoing conferences, and the online room system accounts.</li> <li>• Go to the corresponding module quickly.</li> </ul>
6	<ul style="list-style-type: none"> <li>• Click <b>Check</b> to go to the Licenses page.</li> <li>• View the related port information, including the capacity, the validity, and the usage.</li> </ul>
7	<p>View the system information of the corresponding node.</p> <ul style="list-style-type: none"> <li>• View the server CPU, the memory, the network, and the disk space. You can click <b>Check</b> to view the detail information.</li> <li>• View the information about the software version.</li> </ul>

## Changing the Display Language for the Website

Seven languages are available on YMS.

### Procedure

In the top-right corner, select the desired language from the drop-down menu of **Language**.



## Editing the Registered Email

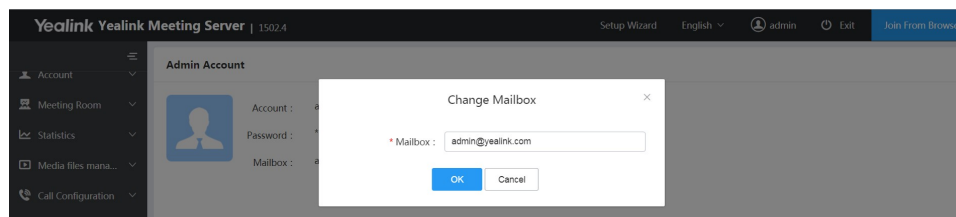
You can edit the registered email. This email is used to receive emails about resetting passwords and system alarms.

### About this task

The registered email is admin@yealink.com by default.

### Procedure

1. Click the account name in the top-right corner.
2. In the **Mailbox** field, click **Change**, enter the new email address and save it.



## Setting the Session Timeout

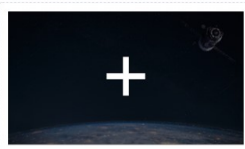
By default, YMS interface session will time out after 30-minute inactivity. After that, you need to log into YMS again.

### Procedure

1. Click **System Setting > Customization > Web and Conference**.
2. In the **Session timeout** field, click **Change**, enter the desired value, and save it.


Web Portal

Background image : ?



Only a jpg image up to 3MB is available

Email header logo : ?



Only a png image up to 3MB with 640\*100 is available

Enterprise name : 1502.4 [Change](#)

Platform name : Yealink Meeting Server [Change](#)

Display copyright : ?  OFF

Display Outlook plug-in download : ?  ON

Outlook plug-in download address : [https://download.yealinkops.com/outlook/yealink\\_outlook\\_plugin.exe](https://download.yealinkops.com/outlook/yealink_outlook_plugin.exe) [Change](#)

Session timeout : 60 mins [Change](#)

Enable forced Https authentication :  ON

## Enabling Forced Https Authentication

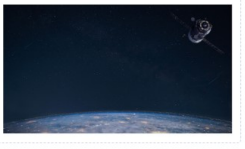
For the security reason, you can enable this feature so HTTP requests will compulsorily become HTTPS requests. For example, the HTTP request of the website access, WebRTC, webcast or others.

### Procedure

1. Click **System Setting > Customization > Web and Conference**.
2. Turn on **Enable forced Https authentication**.

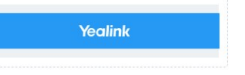
Web Portal

Background image : ?



Only a jpg image up to 3MB is available

Email header logo : ?



Only a png image up to 3MB with 640\*100 is available

Enterprise name : 1502.4 [Change](#)

Platform name : Yealink Meeting Server [Change](#)

Display copyright : ?  OFF

Display Outlook plug-in download : ?  ON

Outlook plug-in download address : [https://download.yealinkops.com/outlook/yealink\\_outlook\\_plugin.exe](https://download.yealinkops.com/outlook/yealink_outlook_plugin.exe) [Change](#)

Session timeout : 60 mins [Change](#)

Enable forced Https authentication :  ON

## Adding a Sub Admin Account

For the system security, you can add different sub admin accounts, and assign the desired module or permission to them.

### About this task

There are five types of the sub admin account: the conference manager, the conference operator, the operation manager, the enterprise administrator, and the customization. You can add up to 100 sub admin accounts.

The enterprise administrator can manage the user accounts and VMRs created by himself. Also, he can manage the sub-groups, the accounts, and VMRs under the root group.

- **The privilege of User Account**

#### Basic Settings



Account : 5001

Account info : Manual

\* Name :

\* Password :

Reset

Mailbox :

The mailbox is used to receive messages from system

- **The privilege of VMR**

#### Basic Settings



#### Common Setting

\* Name :

\* Alias :

\* Conference ID :

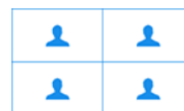
Require Password (Password is suggested for conference security)

\* Organizer :

Default layout :



onePlusN



Equal NxN



**Note:** For the enterprise administrator, you need to contact Yealink technical support engineers to enable it.

## Procedure

1. Click **System Setting > Sub Admin Account**.
2. Add a sub admin account.

**Add Sub Admin Account**

---

\* Username :

Password :

Role :  Conference manager  Conference operator  Operation manager  
 Enterprise administrator  Customization

Level :  Read-write  Read-only

Manageable modules :  Conference  Account  Meeting Room  Statistics

---



**Tip:** The password of the sub admin account is v12345678 by default.

## Customizing the Theme

According to the enterprise need, you can customize the following parameters, for example, the enterprise logo, the background image of WebRTC, and the display image of the video conference.

### About this task

The parameters are described as below:

**Table 11: Parameters of the Logo**


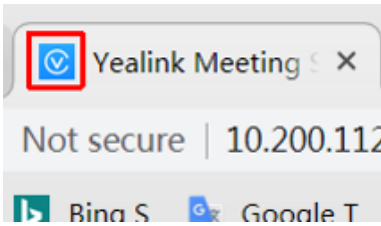
Parameter	Effect
Portal logo	
Tab logo	 <p><b>Note:</b> A free conversion tool is available on the Internet.</p>



Table 12: Parameters of the Web Portal

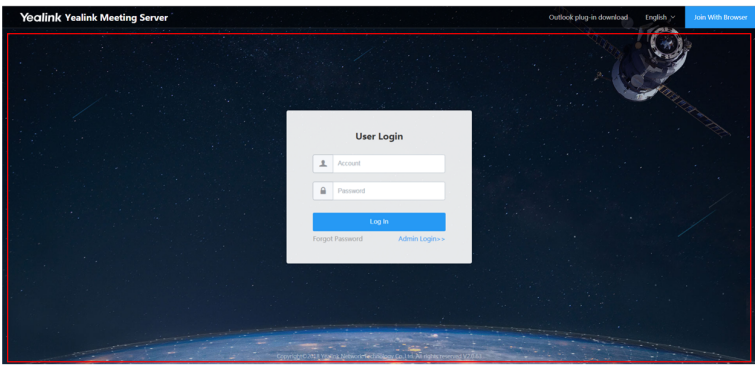
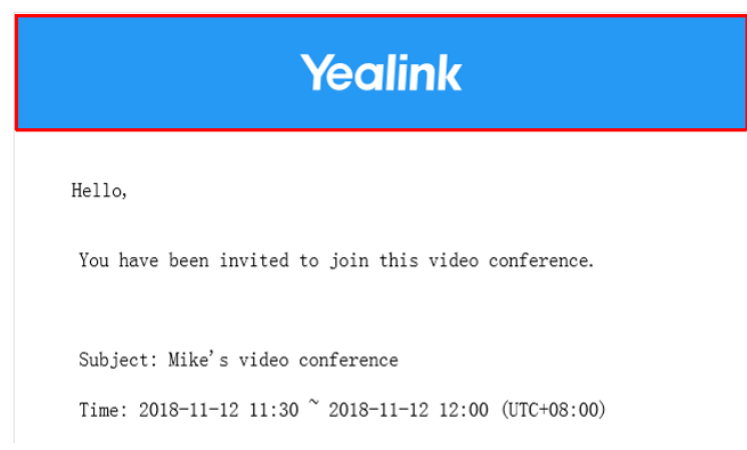
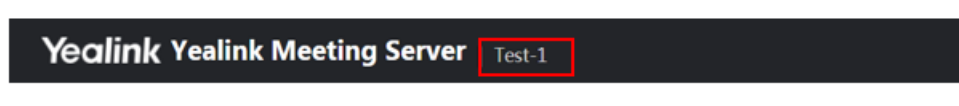
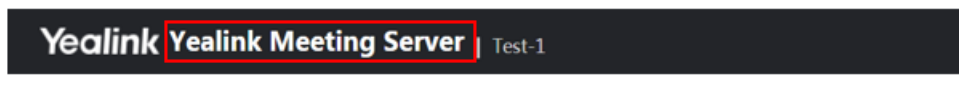
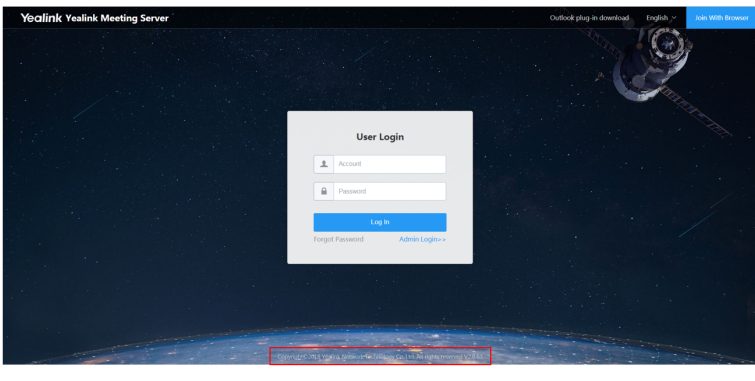
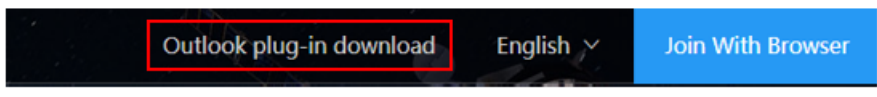
Parameter	Effect
<b>Background image</b>	
<b>Email header logo</b>	
<b>Enterprise name</b>	
<b>Platform name</b>	
<b>Display copyright</b>	
<b>Display Outlook plug-in download</b>	

Table 13: Parameters of the WebRTC Portal

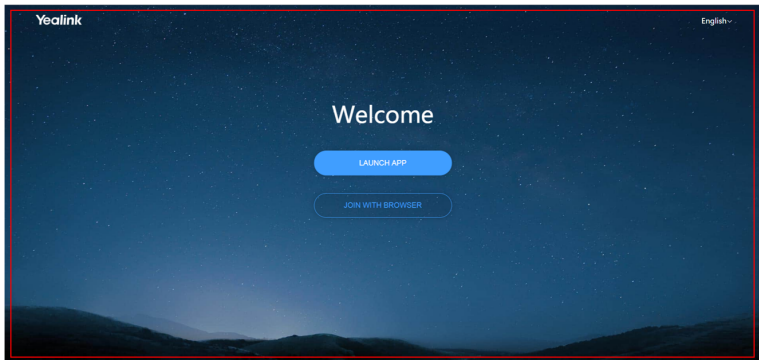
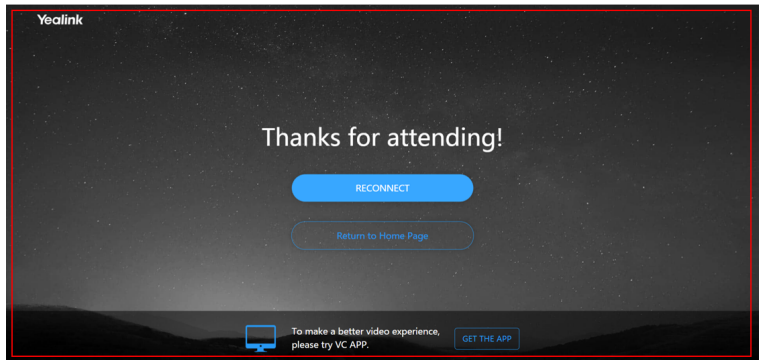
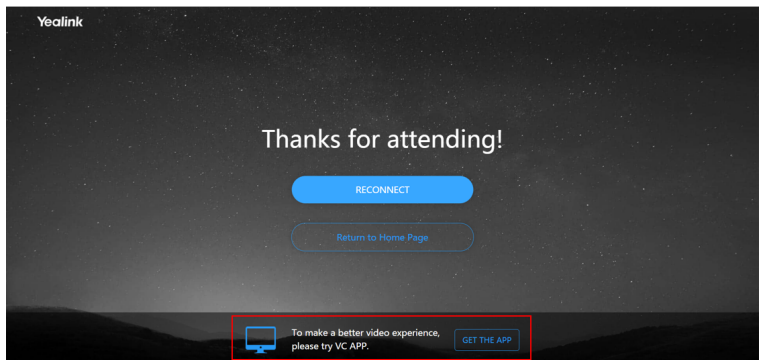
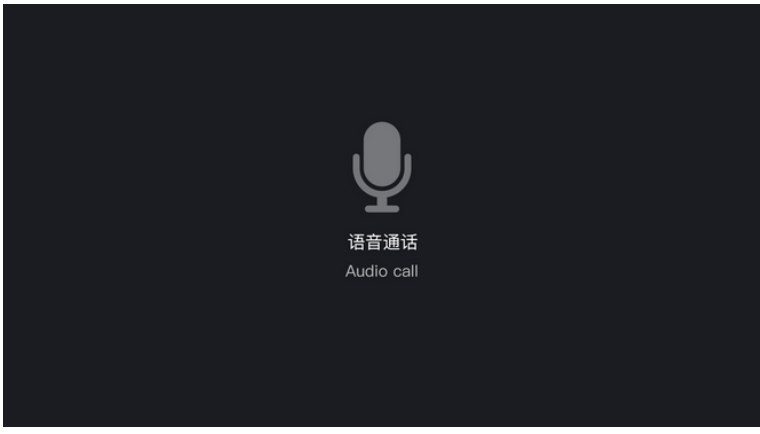
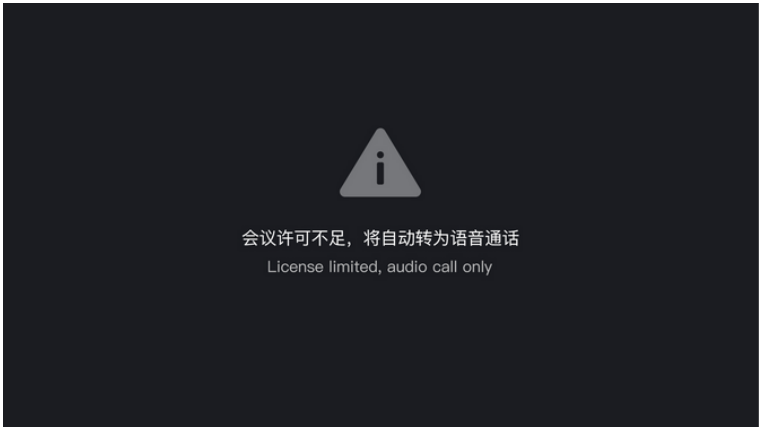
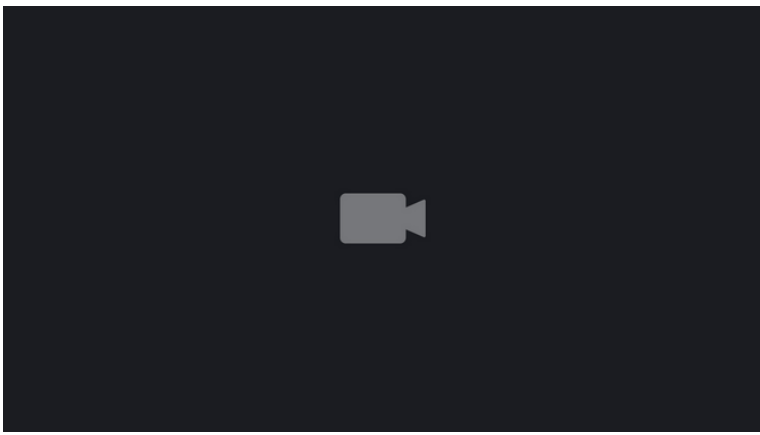

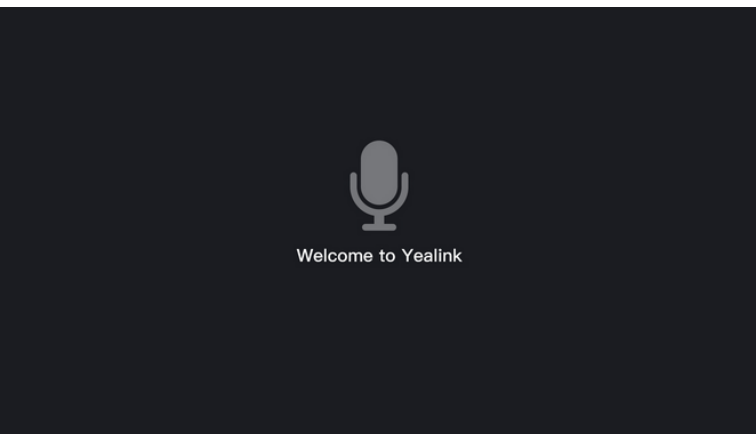
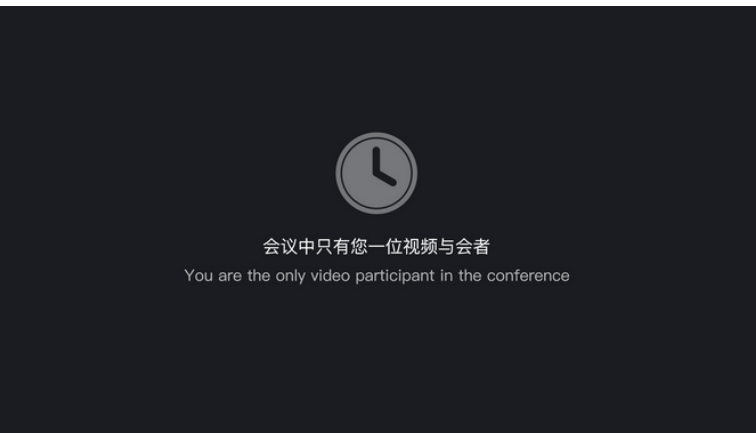
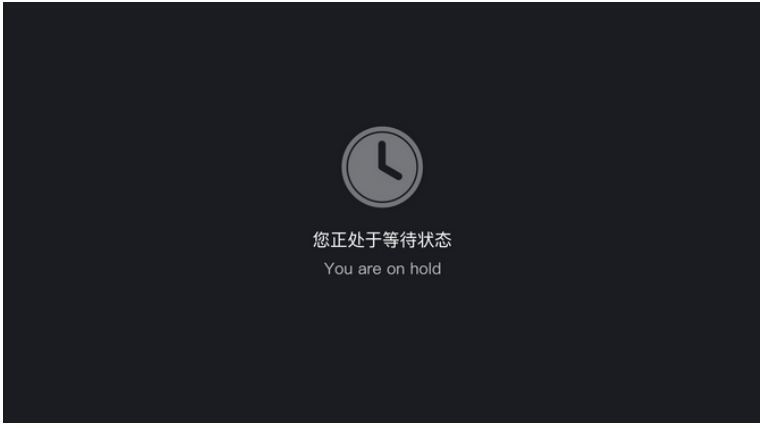
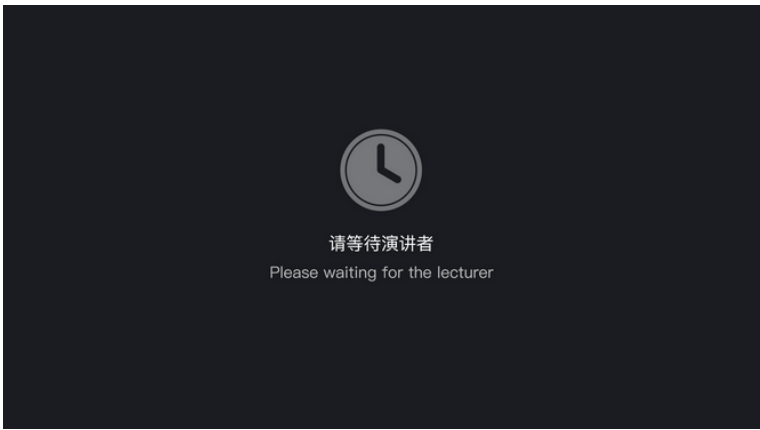
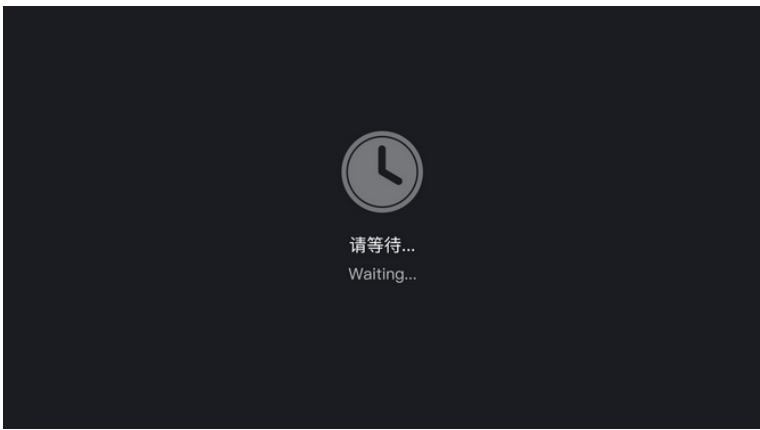
Parameter	Effect
<b>Enable WebRTC</b>	Allow or refuse the user to join the conference via browser.
<b>Background image for WebRTC home screen</b>	
<b>Background image of WebRTC end page</b>	
<b>Extension download address</b>	The address for downloading Yealink content sharing plugin that you can see when you use Google Chrome to visit Yealink Web App, and share content with the remote.
<b>Display PC soft-client download</b>	
<b>Windows</b>	Specify the address for downloading Yealink VC Desktop for Windows.
<b>Mac</b>	Specify the address for downloading Yealink VC Desktop for Mac.

Table 14: Parameters of the Video Conference

Parameter	Effect
<b>Audio call image</b>	 <p>A dark rectangular area containing a light gray microphone icon centered vertically. Below the icon, the Chinese characters '语音通话' and the English text 'Audio call' are displayed in a small, light gray font.</p>
<b>License limited image</b>	 <p>A dark rectangular area containing a light gray information icon (a triangle with a lowercase 'i' inside) centered vertically. Below the icon, the Chinese characters '会议许可不足, 将自动转为语音通话' and the English text 'License limited, audio call only' are displayed in a small, light gray font.</p>
<b>No video data image</b>	 <p>A dark rectangular area containing a light gray video camera icon centered vertically.</p>

Parameter	Effect
<b>Camera OFF image</b>	 A dark gray background with a white camera icon crossed out by a diagonal line. Below the icon, the text "摄像头已关闭" (Camera is closed) and "Camera OFF" is displayed in white.
<b>Welcome screen image</b>	 A dark gray background with a white microphone icon. Below the icon, the text "Welcome to Yealink" is displayed in white.
<b>The sole video call party image</b>	 A dark gray background with a white clock icon. Below the icon, the text "会议中只有您一位视频与会者" (Only one video participant in the conference) and "You are the only video participant in the conference" is displayed in white.

Parameter	Effect
Conference lobby image	
Waiting for the lecturer image	
Waiting image	

### Procedure

1. Click **System Setting > Customization > Web and Conference**.
2. Configure the enterprise logo, the background image of the web portal, the background image of WebRTC, and the display image of the video conference.

If the device negotiates with the server to use the resolution of 360P, 720P, and 1080P, the ratio of length to width of the video image is 16:9; if they negotiate to use the resolution of CIF and 4CIF, it is 4:3.

## Setting the Password Policy

You can set the maximum password age. When it is reached, the system will automatically remind users to change their passwords.

### Procedure

Click **Account** > **Password**.

**Password**

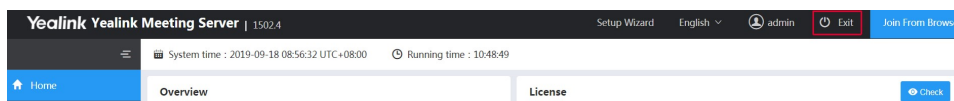
---

Max valid period :  Max valid period  (30-90) day(s)

## Logging out of YMS

### Procedure

Click **Exit** in the top-right corner to return to the Login page.



## Setting the Web Service Address

In the cluster deployment, to make endpoints obtain the Web service address (for example, when the device accesses contacts or downloads firmware), you can set the service URL for the internal and the external network respectively, and then the server will send the corresponding address to the device according to the network where the device locates.

### About this task



**Note:** This feature will not affect your access to YMS. If the device fails to access contacts, check the IP address and the port number.

### Procedure

1. Click **System Setting** > **Common Setting** > **Network Association**.
2. Add a web service address.

WEB service address :

Service network :	Service URL :
<input type="text" value="Internal network"/>	<input type="text" value="https://10.86.0.203"/>
<input type="text" value="External network"/>	<input type="text" value="https://124.72.94.30"/>
<input type="button" value="+ Add service address"/>	

If the domain name is resolved to both the internal network and the external network, you can select **All**.

The address in the internal service URL is the address of the master node, and the address in the external service URL is the mapped address of the public network.

If you have mapped port 80/443, the URL should be added to the mapped port.

3. Save the configuration.

## Setting the Log Service Address

---

In the cluster deployment, to make endpoints obtain the address of the log server, you can set the log URL server for the internal and the external network respectively, and the server will send the corresponding address to the device according to the network where the device locates.

### About this task

If you do not configure the log service address, the address is the same as the Web service address.



**Note:** If there is no device log being collected, check the IP address and the port number.

### Procedure

1. Click **System Setting > Common Setting > Network Association**.
2. Add a log service address.

Log service address :

Service network :	Transmission type :	IP address :
Internal network <input type="button" value="v"/>	UDP <input type="button" value="v"/>	10.3.3.2 <input type="button" value="X"/>
External network <input type="button" value="v"/>	UDP <input type="button" value="v"/>	100.1.1.1 <input type="button" value="X"/>
<input type="button" value="+ Add service address"/>		

If the domain name is resolved to both the internal network and the external network, you can select **All**.

The IP address of the internal network is the address of the master node, and the IP address of the external network is the mapped address of the public network.

3. Save the configuration.

## Setting the Time Zone

---

The time zone you set is the default time zone used by the user when they schedule conferences.

### About this task

The time displayed in the YMS web interface is your local time (except for the current time of the server), for example, the operation log, the system log, and the recording log. This time is obtained from the time zone configured on the computer which you use to access the web interface.

### Procedure

1. Click **System Setting > Common Setting > Time**.
2. Select the corresponding time zone.

Network Association **Time** Data Space SMTP Mailbox Number Resource Allocation

Current server time : 2019-09-18 09:56:40 UTC+08:00

Time access :  SNTP  Date & time configuration

Server domain :

NTP server :  OFF

Timezone :

Auto adjust conference DST :

3. Save the configuration and the system reboots.  
The current server time changes in real time.

## Importing the Trusted CA Certificate

---

When YMS sends the request of TLS connection to devices, the server needs to verify whether the device is reliable according to the CA certificate. There are 105 built-in CA certificates in YMS. If devices require their self-signed certificates, you need to import the custom CA certificates.

### About this task

Scenario: when [Configuring the SMTP Mailbox](#), if you select the secure connection, the role of the SMTP needs verifying.

### Procedure

1. Click **System Setting > Certificate > Trusted CA Certificate > Import**.



## Import Trusted CA Certificate ×

Name :

Certificate :

Only .crt,.cer,.pem format file up to 10MB is available

 20190730145624\_all.crt



2. Click **Upload** and select the desired file.

## Importing the HTTPS Certificate

---

When you access YMS by HTTPS, the browser might prompt that it is insecure. To solve this problem, you can import the certificate trusted by the browser.

### Before you begin

You have obtained the device certificate issued by CA and the certificate can match the server address.

### Procedure

1. Click **System Setting > Certificate > HTTPS Certificate > Import**.

## Import HTTPS Certificate ×

Name :

Certificate :

Only .pem format file up to 10MB is available

 20190730145624\_all.pem



2. Click **Upload** and select the desired file.

## Importing the TLS Certificate

---

When the device sends a request of TLS connection to YMS, the device will verify whether YMS is reliable according to the TLS certificate sent by YMS.

### About this task

Scenario: when [Setting the SFB Gateway](#), you need to import the TLS certificate and then the Sfb server will verify YMS.

### Procedure

1. Click **System Setting** > **Certificate** > **TLS Certificate** > **Import**.

×

### Import TLS Certificate

Name :

Certificate : 📁 Upload

Only .pem format file up to 10MB is available

📄 20190730145624\_all.pem

OK

Cancel

2. Click **Upload** and select the desired file.

## Configuring the Port

---

When the default port range fails to satisfy the actual demand, you can set the IVR port, the BFCP/FECC port, the stack signaling port, and the stack media port.

### About this task

To avoid the port conflict, the gap between the maximum port and the minimum port should not be less than 200. For example, you set 10000 as the minimum IVR port, and the maximum IVR port should not be less than 10199.

### Procedure

1. Click **System Setting** > **Common Setting** > **Network Association**.
2. Configure the port parameters.

* IVR port :	<input style="width: 20%; border: 1px solid #ccc;" type="text" value="10000"/>	~	<input style="width: 20%; border: 1px solid #ccc;" type="text" value="10999"/>
* BFCP/FECC port :	<input style="width: 20%; border: 1px solid #ccc;" type="text" value="11000"/>	~	<input style="width: 20%; border: 1px solid #ccc;" type="text" value="12999"/>
* Stack signalling port :	<input style="width: 20%; border: 1px solid #ccc;" type="text" value="13000"/>	~	<input style="width: 20%; border: 1px solid #ccc;" type="text" value="13199"/>
* Stack media port :	<input style="width: 20%; border: 1px solid #ccc;" type="text" value="13200"/>	~	<input style="width: 20%; border: 1px solid #ccc;" type="text" value="13399"/>

3. Save the configuration.

## Setting the Data Space

You can manually allocate the space quota for the **Syslog**, the **Device log**, the **Backup space**, the **Device firmware**, and the **Collaboration file**.

### Before you begin

The space quota should be an integer value, and the space quota of each part should not be less than its default space quota.

### Procedure

1. Click **System Setting > Common Setting > Data Space**.
2. Enter the desired quota in the corresponding field.

Capacity Allocation		Usage	
Syslog	Total <input type="text" value="50"/> GB Partition : /home (Storage space : 218.67GB available, total 440 GB )	<div style="width: 36.39%;"><div style="width: 36.39%;"></div></div> 36.39% 31.81GB available, total 50 GB System will auto clear data when more than 80% disk space are used	<a href="#">Clear</a>
Device log	Total <input type="text" value="5"/> GB Partition : /home (Storage space : 218.67GB available, total 440 GB )	<div style="width: 64.3%;"><div style="width: 64.3%;"></div></div> 64.3% 1.78GB available, total 5 GB System will auto clear data when more than 80% disk space are used	<a href="#">Clear</a>
Backup space	Total <input type="text" value="5"/> GB Partition : / (Storage space : 7.07GB available, total 49 GB )	<div style="width: 0.2%;"><div style="width: 0.2%;"></div></div> 0.2% 4.99GB available, total 5 GB <input checked="" type="checkbox"/> System will send email to inform when more than 80% disk space are used	<a href="#">Clear</a>
Device firmware	Total <input type="text" value="5"/> GB Partition : / (Storage space : 7.07GB available, total 49 GB )	<div style="width: 37.06%;"><div style="width: 37.06%;"></div></div> 37.06% 3.15GB available, total 5 GB <input checked="" type="checkbox"/> System will send email to inform when more than 80% disk space are used	<a href="#">Clear</a>
Collaboration file	Total <input type="text" value="20"/> GB Partition : / (Storage space : 7.07GB available, total 49 GB )	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0% 20.00GB available, total 20 GB <input checked="" type="checkbox"/> System will send email to inform when more than 80% disk space are used	

3. Save the configuration.

## Allocating the Number Resource

You can customize the range of the account number or the conference ID to meet the enterprise need.

### About this task

Edit the allocated number resource with caution, because it may cause the allocated number unavailable to use.

### Procedure

1. Click **System Setting > Common Setting > Number Resource Allocation**.
2. Add a number resource.
3. Configure the parameters.

×

## Add

\* Number type :  ▾

\* Origin section :

\* Rear section :

Description :

**Table 15: Parameters of the number resource**

Parameter	Description
<b>Number type</b>	<p>Specify the type of the number.</p> <p>The supported types are as follows:</p> <ul style="list-style-type: none"> <li>• <b>System account</b>: it contains the user accounts and the room system accounts.</li> <li>• <b>All conference</b>: it contains the conference IDs of scheduled conferences, Meet Now conferences and VMRs.</li> <li>• <b>Meet Now</b></li> <li>• <b>Scheduled conference</b></li> <li>• <b>VMR</b></li> </ul> <p><b>Note:</b> if you set <b>All conference</b> and <b>Meet Now</b>, the system will use the <b>Meet Now</b> with priority. This can also be applied to <b>Scheduled conference</b> and <b>VMR</b>.</p>

4. Save the configuration.

## Setting the IP Property

If there are multiple operators to choose for the external address, you can set the IP property, making the traversal server, the MCU server and the registration server use the same operator. Therefore, users can have a better conference experience.

### About this task



**Note:** If there is only one external address or you use the same operator for the external address, you do not need to configure IP Property.

### Procedure

1. Click **System Setting > Address Port Mapping > IP Property**.
2. Add an IP property.
3. Set the parameters.

* IP Address :	<input type="text" value="1.1.1.1"/>
* Operator :	<input type="text" value="China Telecom"/>

**Table 16:**

Parameter	Description
<b>IP address</b>	Specify the IP address for the external network.
<b>Operator</b>	Select the operator type. <b>Note:</b> If it is an operator other than China Telecom, China Unicom, China Mobile and Education Network (China Netcom), choose BGP.

4. Save the configuration.

## Setting the Intelligent Security Strategy

You can configure the security strategy, for example, the strategy for identifying or blocking the attacking IP.

### About this task



**Note:** If you want to unblock the abnormal IP in advance, refer to [Deleting the Abnormal IP](#).

### Procedure

1. Click **System Setting > Security > Intelligent Security Strategy**.
2. Set the parameters.

**SIP Signalling**

- \* Attack detection cycle :  second(s)
- \* Max frequency of IP call or auth failure :  ?
- \* Suspected attack banned duration :  minute(s)
- \* Max suspected attacks frequency within 24 hours :  ?
- \* Long term banned duration :  day(s) ?
- \* Max concurrent IP call per node :  ?

**Table 17: Intelligent Security Strategy**

Parameter	Description
<b>Attack detection cycle</b>	Specify the cycle for detecting an attack. <b>Default:</b> 25 seconds.
<b>Max frequency of IP call or auth failure</b>	It instructs YMS to block any source IP address, which fails several times to place calls to YMS or log into YMS during the attack detection cycle. Default: 10 times.
<b>Suspected attack banned duration</b>	Specify the duration of blocking the suspected attack. <b>Default:</b> 10 minutes.
<b>Max suspected attacks frequency within 24 hours</b>	It instructs YMS to block any source IP address where the suspected attacks come from, within 24 hours. Default: 3 times.
<b>Long term banned duration</b>	Specify the banned duration. <b>Default:</b> 7 days.
<b>Max concurrent IP call per node</b>	Specify the maximum concurrent calls to YMS placed by one IP from one node. When the number of concurrent IP calls exceeds the maximum number on a single node, the IP will be blocked. <b>Default:</b> 30.

- In the **Whitelist** field, select the desired security group or [Adding a Security Group](#) , and devices in this group will not be affected by the security strategy.
- Save the configuration.

## Adding a Security Group

You can add security groups, which are applied to the whitelist and the blacklist of various services, to secure the server.

### About this task

The service includes the following:

[Setting the Registration Service](#)

[Configuring the Third-Party Registration Service](#)

[Setting the IP Call Service](#)

[Communicating with the PSTN](#)

[Setting the Peer Trunk Service](#)

[Setting the SFB Gateway](#)

### Procedure

1. Click **System Setting > Security > Security Group**.
2. Add a security group.
3. Configure the parameters.

\* Name :

Description :

Content :

*Type :	*IP Address :	Description :	
Single IP	<input type="text" value="10.3.3.1"/>	<input type="text"/>	✕
Section IP	<input type="text" value="172.16.0.1"/>	<input type="text" value="172.16.0.20"/>	✕
+ Add			

4. Save the configuration.

## Deleting the Abnormal IP

The duration of blocking the abnormal IP depends on the attack result, but you can also manually delete the abnormal IP address.

### About this task

For the reason of abnormal IP, refer to [Setting the Intelligent Security Strategy](#).

### Procedure

1. Click **System Setting > Security > Abnormal IP**.
2. Select the desired device and click **Delete**.
3. Click **OK**.

## Applying for the Accesskey

YMS allows third parties to call the API to integrate with their systems. Before calling the API, you need to apply for the AccessKey for the authentication. For more information, refer to [API for Yealink Meeting Server](#).

### Procedure

1. Click **System Setting** > **Security** > **Accesskey**.
2. Click **Apply**, then AccessKey ID and AccessKey Secret will be generated automatically.

## Adding the User-Agent Blacklist

If you know the User-Agent of an attack and you want to forbid devices of this type to call into YMS or to register YMS accounts, you can add them into the blacklist.

### Procedure

1. Click **System Setting** > **Security** > **User-Agent Blacklist**.
2. Add a blacklist.
3. Configure the parameters.

Add ×

Enabled :  ON

\* Regular expression :

Description :

**Table 18:**

Parameter	Description
<b>Enabled</b>	Enable or disable this blacklist. <b>Default:</b> enabled.
<b>Regular Expressions</b>	Specify the Perl Compatible Regular Expressions (PCRE). <b>Note:</b> For example, if you set the regular expression as ^T49, all User-Agent of the endpoints whose model types start with T49 cannot call into YMS.
<b>Description</b>	Add a description for this list.

4. Click **OK**.



## Adding the User-Agent Compatible List

To be compatible with Yealink OEM devices in the old version and to allow these devices to call into YMS or to register YMS accounts, you can add them to the compatible list.

### About this task



**Note:** The type of the device in the new version is distinguished by Client-Info head filed, and no configuration is required.

### Procedure

1. Click **System Setting > Security > User-Agent Compatible List**.
2. Add a compatible list.
3. Set the parameters.

**Table 19:**

Parameter	Description
<b>Enabled</b>	Enable or disable this compatible list. <b>Default:</b> enabled.
<b>Regular Expressions</b>	Specify the Perl Compatible Regular Expressions (PCRE). <b>Note:</b> For example, if you set the PCRE as ^polycom, all User-Agent devices whose model types start with polycom can call into YMS.
<b>Description</b>	Add a description for this list.

4. Click **OK**.

## Configuring the Email Template

You can customize the email template for different uses. For administrators, they receive emails about the system alarm, SMTP mailbox testing or others. For users, they receive emails about the information of conferences that they are invited or create, the notification that the recording is finished or others.

### About this task

You cannot modify the string that starts with \$ in the **Subject** and **Content**. Otherwise, you might fail to send the email.

## Procedure

1. Click **System Setting > Customization > Email Template**.
2. Configure the parameters.

The screenshot shows the 'Email Template' configuration page. At the top, there are navigation tabs: 'Web and Conference', 'Email Template' (selected), 'SIP Trunk IVR', and 'Audio IVR'. Below the tabs, the 'Email type' section has two radio buttons: 'For administrator' (selected) and 'For user'. A blue bar contains three buttons: 'Mailbox Settings Test', 'Forgot Password', and 'System Warning'. The 'Scene' section displays 'Testing mailbox connected successful'. The 'Text language' section has a dropdown menu with 'English' selected, and other options include '简体中文', '繁體中文', 'Русский', 'Português', 'Español', 'Polski', and '日本語'. The 'Subject' field contains 'Mailbox setting test'. The 'Content' section features a rich text editor with a toolbar and the text 'Hello , Mailbox setting test'.

3. Save the configuration.

## Setting SIP Trunk IVR

You can customize SIP Trunk IVR so the user can join conferences or place P2P calls according to the voice prompt.

### About this task

Dial `main_ivr@server domain name` to go to the SIP trunk IVR.

## Procedure

1. Click **System Setting > Customization > SIP Trunk IVR**.
2. Configure the receptionist greetings, and do one of the following:
  - Select **Default Greeting**. The language depends on the IVR language, refer to [Setting IVR language](#) .

The screenshot shows the 'SIP Trunk IVR' configuration page. At the top, there are navigation tabs: 'Web and Conference', 'Email Template', 'SIP Trunk IVR' (selected), and 'Audio IVR'. Below the tabs, the 'Receptionist greeting prompt configuration' section has two radio buttons: 'Default Greeting' (selected) and 'Personal Greeting'. Below these is an 'Upload' button with an upload icon. A note below the button states: 'The uploaded personal greeting must be a .wav file up tp 10MB.'

- Select **Personal Greeting**.  
Click **Upload** to upload the desired file.  
Configure a feature for each key.

Web and Conference   Email Template   **SIP Trunk IVR**   Audio IVR

---

Receptionist greeting prompt configuration :

Default Greeting  
 Personal Greeting

[Upload](#)

The uploaded personal greeting must be a .wav file up tp 10MB.

Menu Options :

Enable first-level extension dialing

Key	Description	Operation	Action Data
0	conference 88888	Transfer to conference	88888
1	exit 2572	Transfer to extension	2572

- If you want to dial the extension directly without pressing the key, select the **Enable first-level extension dialing** check box.
3. Save the configuration.

## Setting the Audio IVR

You can customize the audio IVR so the user can join conferences according to the voice prompt.

### About this task

Dial *conference\_ivr@server domain name* to go to the audio IVR.

### Procedure

1. Click **System Setting > Customization > Audio IVR**.
2. Configure the voice prompt and do one of the following:

Web and Conference   Email Template   SIP Trunk IVR   **Audio IVR**

---

Conference reminder tone configuration :

Default Greeting  
 Personal Greeting

[Upload](#)

The uploaded personal greeting must be a .wav file up tp 10MB.

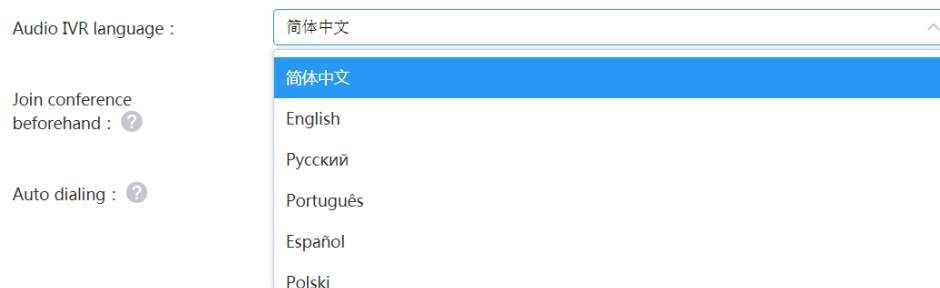
- Select **Default Greeting**. The language depends on the IVR language, refer to [Setting IVR language](#) .
  - Select **Personal Greeting**.  
Click **Upload** to upload the desired file.
3. Save the configuration.

## Setting IVR language

You can set the voice prompt language for the IVR service.

### Procedure

1. Click **Call Configuration > Call Control Policy**.
2. In the **Audio IVR language** field, select a language, and save it.



## Managing Services

- [Configuring the Redirection Service](#)
- [Broadcasting Interactive Conference](#)
- [Yealink Recording Service](#)
- [Configuring the Media Bypass Service](#)
- [Yealink Live Service](#)
- [Collaboration Service](#)
- [Configuring the Third-Party Registration Service](#)
- [Configuring the GK Service](#)
- [H.323 Gateway](#)
- [Setting the IP Call](#)
- [Call Routing](#)

## Configuring the Redirection Service

If you use the cluster version, when there are multiple registration services, you only need to configure the redirection service. When you are registering an endpoint with an account, the address of the proxy server directs to the address of the redirection server. When the IP of the registration server is changed, you do not need to change the configuration on the endpoint.

### Before you begin

[Setting the Registration Service](#) is enabled on several nodes.

### Procedure

1. Click **Service > SIP Service > Redirect Service**.
2. Add a redirection service.
3. Configure the parameter and save it.

We recommend that you select the node without any enabled registration services; otherwise, the page prompts for the port conflict.

Enabled :  ON

\* Name :

\* Node :

Service address

*Network	TLS Port
<input type="text" value="10.83.1.151 (Enabled)"/>	<input type="text" value="5062"/>
<input type="button" value="+ Add"/>	

## Broadcasting Interactive Conference

---

The broadcasting interactive conference can contain hundreds or thousands of participants or venues, which is suitable for large training. It is also applicable to different administrative areas. There are interactive parties and broadcasting parties. The broadcasting parties only receive the audio, the video and the content, which meet the demand of some venues.

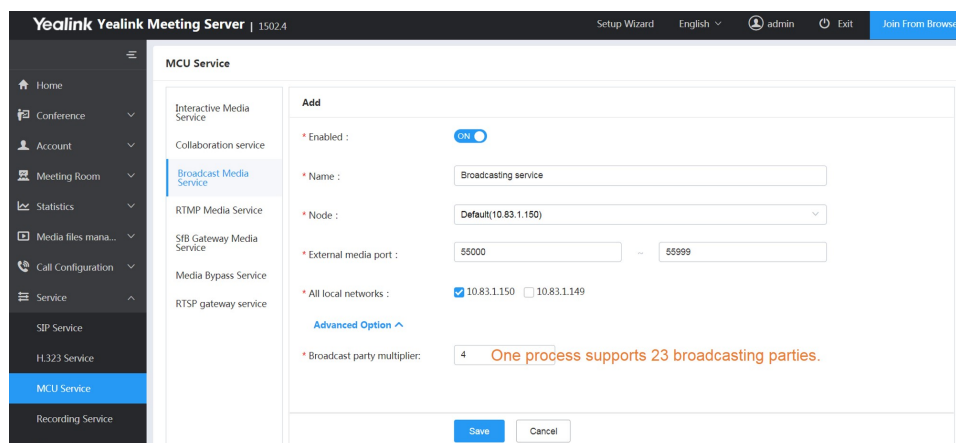
You can follow the steps below to enable the broadcasting interactive conference.

1. [Configure the Broadcast Media Service](#)
2. [Setting the Interactive Media Service](#)
3. For scheduled conferences, refer to [Enabling Broadcasting Interactive for Scheduled Conferences](#) to enable **Broadcasting Interactive** in the Global Setting and users can enable it when they schedule training mode conferences. For more information, refer to [Yealink Meeting Server User Guide](#).
4. For VMR, refer to [Enabling Broadcasting Interactive for VMR](#) to enable **Broadcasting Interactive**.
  - [Configure the Broadcast Media Service](#)
  - [Enabling Broadcasting Interactive for Scheduled Conferences](#)
  - [Enabling Broadcasting Interactive for VMR](#)

## Configure the Broadcast Media Service

### Procedure

1. Click **Service > MCU Service > Broadcast Media Service**.
2. Add a broadcast media service.
3. Configure the parameter and save it.



### Related tasks

[Enabling Broadcasting Interactive for Scheduled Conferences](#)

## Enabling Broadcasting Interactive for Scheduled Conferences

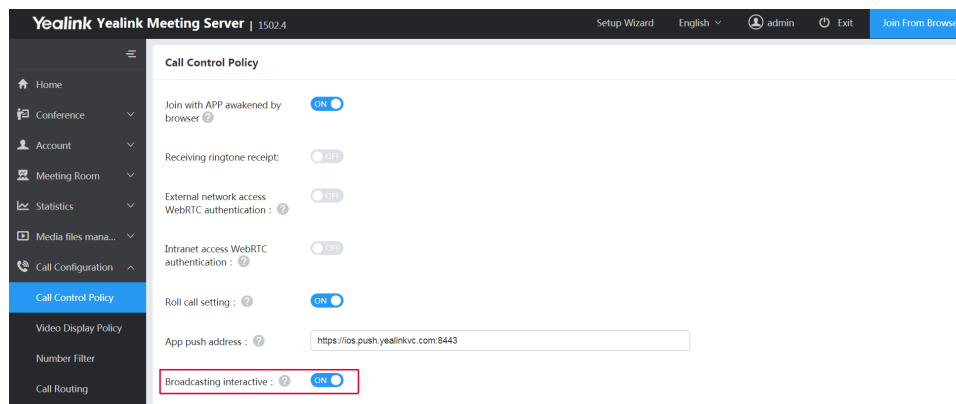
If you disable the feature of **Broadcasting Interactive**, this configuration is invisible to users when they schedule conferences.

### Before you begin

- You have enabled the broadcast license, refer to [Activating a License](#).
- [Setting the Interactive Media Service](#) and [Configure the Broadcast Media Service](#) are finished.

### Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Broadcasting interactive** and save it.



### Related tasks

[Configure the Broadcast Media Service](#)

## Enabling Broadcasting Interactive for VMR


This feature is only applicable to the training mode VMR.

### Procedure

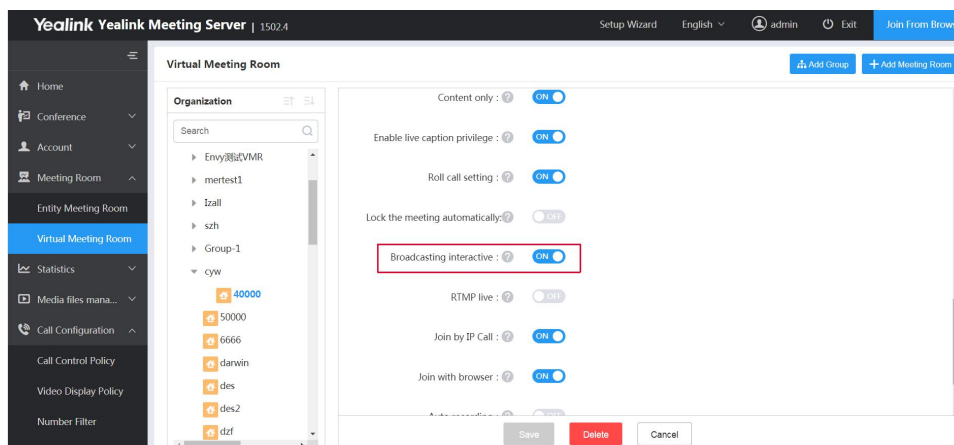
Click **Meeting Room** > **Virtual Meeting Room** and do one of the following:

- If you want to add a VMR, click **Add Meeting Room**.

In the **Permission setting** field, enable **Broadcasting interactive**, and save it.

If you want to edit a VMR, click .

In the **Permission setting** field, enable **Broadcasting interactive**, and save it.



## Yealink Recording Service

Yealink recording service can allow you to record conferences, play recorded videos on demand, and manage recorded files. Users can record multiple concurrent conferences at the same time. You can follow the steps below to record conferences and manage the recording files.

1. [Enabling the Recording Service](#) .
  2. Customize the recording parameters, for example, [Recording Template](#) , [Displaying the Recording Icon during Recording](#) , and [Adding Watermark for Recording Files](#) . For more information, refer to [Managing the Recording Settings](#) .
  3. Enable recording privileges for user accounts, refer to [Enabling the Recording Privileges for User Accounts](#) .
  4. For scheduled conferences, when users schedule conferences, users can set the recording privilege. For more information, refer to [Yealink Meeting Server User Guide](#).
  5. For VMRs, users can see [Enabling the Recording Privileges for VMRs](#) to set the recording privilege.
  6. The conference moderator goes to the Conference Control page, and start recording the conference. For more information, refer to [Yealink Meeting Server User Guide](#). If you enable the feature of Auto recording in step 4 or 5, you can skip this step.
  7. Manage the generated recording files, for example, [Managing the Recording Files](#) , [Managing the Sharing Link](#) , and [Making Backups for Recording Files](#) . For more information, refer to [Managing the Recording Files](#) .
- [Enabling the Recording Service](#)
  - [Managing the Recording Settings](#)
  - [Enabling the Recording Privileges for User Accounts](#)
  - [Enabling the Recording Privileges for VMRs](#)
  - [Managing the Recording Files](#)
  - [Viewing the Recording Log](#)

## Enabling the Recording Service

If you want to use the recording service of YMS, you need to set the recording service.

### Before you begin

- [Activating a License](#) is finished.
- The disk space of the home directory of the node used by this service should not be less than 50G.

### Procedure

1. Click **Service > Recording Service > Add**.
2. Set the parameter and save it.

\* Enabled :  ON

\* Name :

\* Node :

\* External media port :  ~

\* All local networks :  10.83.1.152

## Managing the Recording Settings

YMS allows you to record the video, the audio, and the shared contents generated in a conference and to save them in the recording server, which you can configure the recording space (see [Setting the Data Space](#) ).

- [Recording Template](#)
- [Displaying the Recording Icon during Recording](#)
- [Adding Watermark for Recording Files](#)

### Recording Template

After you successfully configure the recording server, the server will automatically generate a default recording template. When you enable recording privileges for users, you can use the default recording template, or you can use the custom one.



**Note:** The conference organizer will use the recording template to record conferences.

- [Parameters of the Recording Template](#)
- [Adding the Recording Template and Applying it to Users](#)
- [Selecting Recording Templates for Accounts](#)
- [Managing Recording Templates](#)

### Parameters of the Recording Template

Before adding or editing the recording template, you need to familiarize yourself with the parameters of the recording template.

**Table 20: Parameters of the Recording Template**

Parameter	Description
Template name	The name of this template.



Parameter	Description
<b>Video resolution</b>	Set the maximum video resolution for the recording file. <b>Default:</b> 720P/30FPS.
<b>Audio and video code rate</b>	Set the maximum bandwidth for the recording file. <b>Default:</b> 2 Mbps. If you set the <b>Video resolution</b> as 360P and the <b>Audio and video code rate</b> as 4M, you can only record a video of 360P even though the bandwidth is 4M.
<b>Layout</b>	Configure the layout of the recording file. If no participants share content, the video layout of the recorded video is displayed in 1+N format with the voice-activated feature enabled. The current speaker is displayed in the large video image and up to 1+N participants are displayed in live thumbnails which will be switched automatically. If a participant is sharing content, the video layout of the recorded video is displayed in 1+4 format with the content as the large video image. Up to 1+4 participants are displayed in live thumbnails which will be switched automatically. The maximum number of N is 20. <b>Default:</b> 1+4.
<b>Recording File</b>	If you select the video, when you finish the recording, video files and images will be generated.  If you and select the audio, when you finish the recording, audio-only files will be generated.  If you select both the video and the audio, when you finish the recording, audio files, video files, and the images will be generated.
<b>Speech-to-text</b>	If you enable this feature, when you finish the recording, a text (the conference summary) will be generated. You can contact Yealink technical support engineer to subscribe to this service.
<b>Generate multiple files with different resolutions</b>	If you enable this feature, when you finish the recording, video files with different resolutions will be generated. Users can select any video file.  If the resolution in the recording template is set to 1080P, recording files with the resolution of 1080P and 720P are generated.  If the resolution in the recording template is set to 720P, recording files with the resolution of 720P and 360P are generated.
<b>Display time stamp in the video file</b>	If you enable this configuration, a timestamp with the format as xxxx-xx-xx xx:xx:xx, will be displayed in the top-right corner of the generated recording files, for example, 2019-07-22 17:40:04.
<b>File format</b>	MP4 and AVI are available.

## Adding the Recording Template and Applying it to Users

### Procedure

1. Click **Media file management > Recording Setting**.
2. Click **Add Template**.
3. Set the parameter and save it.

* Template name	<input type="text" value="test"/>
Video resolution	<input type="text" value="720P/30FPS"/>
Audio and video code rate	<input type="text" value="2 Mbps"/>
Layout	<input type="text" value="1+N"/>
Recording file:	<input checked="" type="checkbox"/> Video <input type="checkbox"/> Audio
Speech-to-text <sup>?</sup>	<input type="radio"/> OFF
Generate multiple files with different resolutions	<input type="radio"/> OFF
Display time stamp in the video file	<input type="radio"/> OFF
File format:	<input type="text" value="mp4"/>

4. You can select users who can use this template. You can also do it later. Refer to [Managing Recording Templates](#) or [Selecting Recording Templates for Accounts](#) .



### Selecting Recording Templates for Accounts

- **For newly added accounts:**

1. Click **Account > User Account/Room System Account > Add Account/Add**.
2. In the tab of **Advanced Options**, set the recording space, and select the recording template.

Basic Settings	Advanced Option
Recording space :	<input checked="" type="radio"/> Unlimited <input type="radio"/> Customization
Recording template	<input type="text" value="默认模板"/>

- **For the existing accounts, do one of the following:**

- Click **Account > User Account/Room System Account**.
  1. On the right of the desired account, click  .
  2. In the tab of **Advanced Options**, set the recording space, and select the recording template.
- Click **Media file management > Recording usage**.
  1. On the right of the desired account, click  .
  2. Set the recording space, select the recording template, and save it.

Recording Setting ×

Recording permission :  ON

Recording Space:  Unlimited  
 Customization

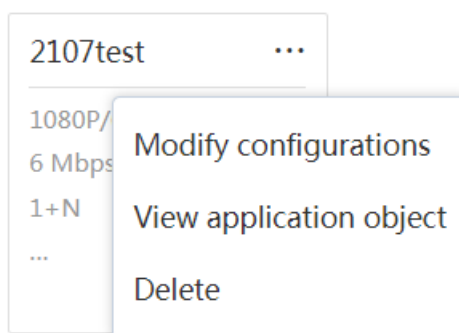
Recording template :

## Managing Recording Templates

You can edit the parameters of recording templates, select users for different templates, and delete templates.

### Procedure

1. Click **Media file management > Recording Setting**.
2. Click **...** on the right of the default template and do one of the following.



- Click **Modify configurations** and edit the parameters.
  - Click **View application object** and select the desired users.
  - Click **Delete** to delete the template.
3. Save the configuration.

## Displaying the Recording Icon during Recording

During the recording, if you want to display the recording icon and the recording duration in the MCU image, you can enable **Show recording icon**.

### Procedure

1. Click **Media file management > Recording Setting**.
2. Enable **Show recording icon**.

## Adding Watermark for Recording Files

If you enable **Add watermark to recording file**, you can see a watermark in the top-right corner of the generated recording file.

### Procedure

1. Click **Media file management > Recording Setting**.
2. Enable **Add watermark to recording file**, set the parameter, and save it.

- **Default watermark**

The screenshot shows the 'Default watermark' configuration interface. At the top, there are two radio buttons: 'Default watermark (Yealink logo+Name of recorder+Account)' which is selected, and 'Customization'. Below this, there is a 'Preview:' label followed by a rectangular box containing the text 'Michael (8987) Yealink'.

- **Customization**

The screenshot shows the 'Customization' configuration interface. At the top, there are two radio buttons: 'Default watermark (Yealink logo+Name of recorder+Account)' and 'Customization', with the latter selected. Below this, there are two input fields: 'Watermark text:' with a text box containing 'Company', and 'Watermark position:' with a dropdown menu showing 'Top right'. Underneath, there is a 'Watermark image:' label and a button that says 'Click to upload image'. A note below the button states: 'Only supports images with dimension 94\*20 and size less than 1MB, formats should be png or jpg format.' At the bottom, there is a 'Preview:' label followed by a rectangular box containing the text 'Company'.

## Enabling the Recording Privileges for User Accounts

If you disable the recording privilege for a user, the configuration of Auto recording is invisible to him when he schedules conferences. Besides, the user can not record the conference when he controls the conference.

- **For newly added accounts:**


1. Click **Account > User Account/Room System Account > Add Account/Add**.
2. In the tabs of **Basic Settings** and **Advanced Option**, set the recording parameters.

- Enable schedule
- Enable Schedule Virtual Meeting Room (Cannot be opened at the same time with Schedule)
- Enable Meet Now
- Enable call authority (Only the contacts visible can be called)
- Enable Recording ( The user will be allowed to record during the meeting )
- Enable live caption privilege (If enabled, conferences started by this user will support live caption)

- **For the existing accounts, do one of the following:**

- Click **Account > User Account/Room System Account**.


- 1.

On the right of the desired account, click .

2. In the tabs of **Basic Settings** and **Advanced Option**, set the recording parameters.

- Click **Media file management > Recording usage**.

- 1.

On the right of the desired account, click .

2. Set the parameter and save it.

Recording Setting ×

Recording permission :  ON

Recording Space:  Unlimited  
 Customization  G

Recording template :

## Enabling the Recording Privileges for VMRs


### Procedure

Click **Meeting Room > Virtual Meeting Room** and do one of the following:

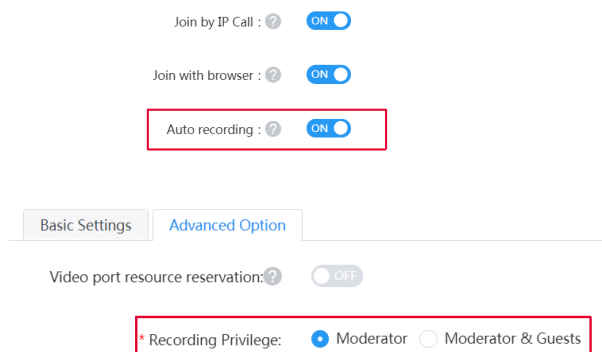
- If you want to add a VMR, click **Add Meeting Room**.

In the tabs of **Basic Settings** and **Advanced Option**, set the recording parameters.

- 

If you want to edit a VMR, click .

In the tabs of **Basic Settings** and **Advanced Option**, set the recording parameters.



## Managing the Recording Files

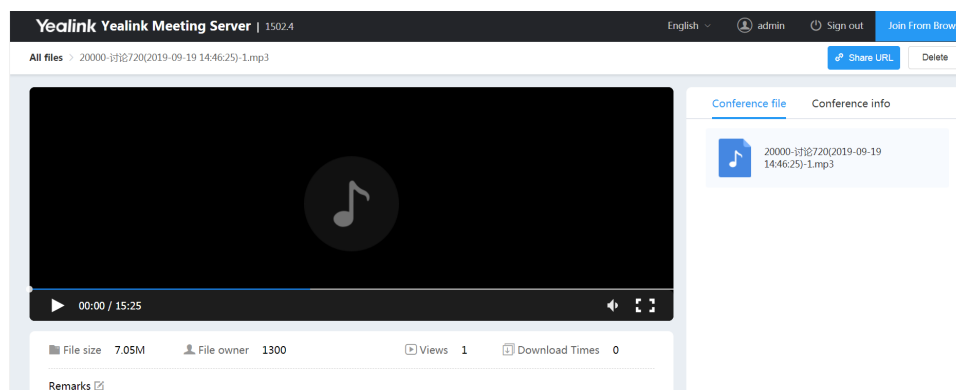
- [Managing the Recording Files](#)
- [Making Backups for Recording Files](#)
- [Managing the Sharing Link](#)
- [Viewing the Usage](#)



### Managing the Recording Files


You can view, edit, and share the recording files created by any user account or room system account.

#### Procedure

1. Click **Media file management > File Management > Recordings**.
2. Click the corresponding recording file, and do one of the following:



- Play the recording file.
- Click  on the right side of **Remarks** and add your remark.
- Click **Share URL** in the top-right corner, and share the link with others or set the link authority.
- Click **Delete** in the top-right corner, and delete the recording according to the prompts.
- Click **Conference file**, and click  on the right side of the desired file to download it.

 **Note:** The type of the recording file depends on the parameter you set for the recording template used by the user.

- Click **Conference info**, and view the conference subject, ID, the start time, the location, and the participants.

#### Related tasks

[Managing the Sharing Link](#)

## Disabling the Sharing Link

### Making Backups for Recording Files

#### Before you begin

The FTP server is available.

#### Procedure

1. Click **Media file management > FTP Backup**.
2. Add the FTP server.

If you do not configure the path or leave it blank, the recording files will be stored in the root directory of the FTP server.

×

### Add FTP server

\* FTP server name:

\* IP :

\* port :

Username :

Password :

Path:

3. Click .

#### FTP Backup

FTP server name/IP

Selected 0

FTP server name
<input type="checkbox"/> Backup-1
<input type="checkbox"/> Select all pages

#### Backup

Select backup time range:  -

Delete local files when backing up

Operation	
<input type="button" value="Copy"/>	<input type="button" value="Delete"/>

< 1 > Go to 1 Pages

## Managing the Sharing Link

### Procedure

1. Click **Media file management > File Management > URL Share MGMT.**
2. Do one of the following:

Recordings Collaboration file **URL Share MGMT**

Search

Selected 0

<input type="checkbox"/>	File Name	file type	Sharing time	Require password	File owner	Operation
<input type="checkbox"/>	20000-讨论720(2019-09-...	Recordings	2019/09/30 18:50	---	1300	<input type="button" value="Share"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>
<input type="checkbox"/>	40000(2019-09-11 11:03:...	Recordings	2019/09/30 10:35	---	测试9998	<input type="button" value="Share"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>
<input type="checkbox"/>	720p30(2019-09-26 09:1...	Recordings	2019/09/26 09:19	---	1300	<input type="button" value="Share"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>
<input type="checkbox"/>	20000-讨论720(2019-09-...	Recordings	2019/09/20 15:18	---	1300	<input type="button" value="Share"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>

- Click  to share the link.
- Click  to edit the link parameter.
- Click  to cancel the sharing.

### Related tasks

[Managing the Recording Files](#)

### Viewing the Usage

You can view the usage of the recording space of user accounts or room system accounts, and the number of the recording files and the shared links.

### Procedure

Click **Media file management > Recording usage.**

Recording Usage

Organization

Search

1502.4

Selected 0

Search

<input type="checkbox"/>	Username	Account	Capacity used (MB)	Capacity available (MB)	Number of recordings	shared recordings	Operation
<input type="checkbox"/>	mary	2222	0	Unlimited	0	0	<input type="button" value="Settings"/>
<input type="checkbox"/>	monica	3333	401	Unlimited	3	1	<input type="button" value="Settings"/>
<input type="checkbox"/>	3502	3502	0	Unlimited	0	0	<input type="button" value="Settings"/>
<input type="checkbox"/>	3503	3503	0	Unlimited	0	0	<input type="button" value="Settings"/>
<input type="checkbox"/>	3504	3504	0	Unlimited	0	0	<input type="button" value="Settings"/>
<input type="checkbox"/>	3501	3501	0	Unlimited	0	0	<input type="button" value="Settings"/>
<input type="checkbox"/>	3505	3505	0	Unlimited	0	0	<input type="button" value="Settings"/>

## Viewing the Recording Log

You can view the recording file name, the file size, the time the file is generated and the file owner via the recording log.

### Procedure

Click **Maintenance > Operation Log > Recording log.**



Recording File Name	File size (MB)	Create time	File owner
20000-讨论720	0.77	2019/09/30 19:09	1300
20000-讨论720	0.72	2019/09/30 19:09	1300
20000-讨论720	0.71	2019/09/30 19:08	1300
20000-讨论720	0.07	2019/09/30 19:07	1300



**Tip:** You can also click **Export Log** in the top right corner to download the log to your computer.

## Configuring the Media Bypass Service

If you enable this feature, it can not only reduce the usage of ports but also improve the media experience and allow more concurrency since the media does not require the secondary encoding and decoding. If you want to know the port consumption in different situations, see [Resource Consumption](#).

### Before you begin

If you want to use this service, you also need to enable the media Bypass feature for the corresponding services.

[Configuring the Third-Party Registration Service](#)

[Setting the IP Call Service](#)

[Setting the Peer Trunk Service](#)

[Configuring the REG Trunk Service](#)

[#unique\\_208](#)

### Procedure

1. Click **Service > MCU Service > Media Bypass Service**.
2. Add a media bypass service.
3. Set the parameter and save it.

The default number of ports is 500. The media bypass service should provide 18 ports for each call. If your environment can support 150 calls, the media bypass service should provide 2700 ports (150\*18=2700).

\* Enabled :  ON

\* Name :

\* Node :

\* External media port :  ~

\* All local networks :  10.83.1.151

## Yealink Live Service

Some activities, for example, lectures or training, have large audiences but limited interaction between the lecturers and the audience. Moreover, the cost is high, and it takes many video port resources if held by the general video conferences. In this situation, the audience who do not need to join the activity can choose to watch the webcast.

Yealink Live service provides the webcast service and ports, which allows the user to watch the webcast of the conference. You can following the steps below:

1. [Enabling Live Service](#)
2. [Configuring YMS System RTMP Live](#)
3. For scheduled conferences, when users schedule conferences, enable **RTMP live**. For more information, refer to [Yealink Meeting Server User Guide](#).
4. For VMR, refer to [Setting the RTMP Live for VMRs](#) , enable **RTMP live**.
5. The conference moderator goes to the Conference Control page, and starts the webcast. For more information, refer to [Yealink Meeting Server User Guide](#).

If you want to use the RTMP Live service, make sure that the network is available and check the following:

- The server can access the external network.
- If your company restricts the Internet access, make sure that the server has the video privilege.
- [Enabling Live Service](#)
- [Configuring YMS System RTMP Live](#)
- [Setting the RTMP Live for VMRs](#)

## Enabling Live Service

### Procedure

1. Click **Service > Live Service > Add**.
2. Configure the parameters.

**Add live service**

---

\* Enabled :  ON

\* Name :

\* Node :  ▾

\* External media port :  ~

\* All local networks :  10.83.1.150

---

## Configuring YMS System RTMP Live

### Before you begin


- [Activating a License](#) .
- [Enabling Live Service](#) .

### Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **System RTMP live**.

System RTMP live: ?  ON

Organizer Logo :



Organizer logo must be a png or jpg image with 300 pixels width and 300 height, which cannot exceed 1MB.

## Setting the RTMP Live for VMRs

### Procedure


Click **Meeting Room** > **Virtual Meeting Room** and do one of the following:

RTMP live : ?  ON

Definition :  ▼

Layout :  ▼

Details :

- If you want to add a VMR, click **Add Meeting Room**.  
In the **Permission setting** field, set the parameters.
- If you want to edit a VMR, click  .  
In the **Permission setting** field, set the parameters.

**Table 21: RTMP live parameters**

Parameter	Description
RTMP Live	Enable or disable the RTMP live. If it is enabled, the users can watch the webcast of the conference. <b>Default:</b> disabled.

Parameter	Description
<b>Definition</b>	<p>It refers to the video resolution that the MCU sends to a live streaming platform.</p> <p>The supported video resolution is as below:</p> <ul style="list-style-type: none"> <li>• 1080P(1080P)</li> <li>• HD(720P)</li> </ul> <p><b>Default:</b> 720P.</p>
<b>Layout</b>	<p>Configure the video layout displayed in the webcast.</p> <p>The supported layouts are as below:</p> <ul style="list-style-type: none"> <li>• <b>1+N:</b> the video layout of the webcast is displayed in 1+N format with the voice-activated feature enabled. If no participants share content, the current speaker is displayed in a large video image. Otherwise, the shared content is displayed in the large video image. Up to 1+N participants are displayed in a single row of live thumbnails at the bottom, that is, the video images in the row are switched automatically.</li> <li>• <b>Picture in picture:</b> the video layout of the webcast is displayed in Picture in picture format. If no participants share content, the current speaker is displayed in a large video image. Otherwise, the shared content is displayed in the large video image and the video image of the current speaker is reduced to a thumbnail at the bottom-right corner.</li> <li>• <b>Selected speaker:</b> the video layout of the webcast is displayed in Selected speaker format. If no participants share content, the current speaker is displayed in a large video image. Otherwise, the shared content is displayed in the large video image.</li> </ul>
<b>Event details</b>	It refers to the text displayed on the Live page.

## Collaboration Service

---

YMS collaboration service provides the following:

- Allow you to use the whiteboard collaboration and make notes
- Allow you to forward the collaboration data or combine the collaboration data with others.
- Allow you to store, share, and download the collaboration file.
- The collaboration privilege: For discussion mode conferences, all participants can initiate/receive/edit/delete the whiteboard collaboration and the content notes. They can also save the whiteboard collaboration on their devices or share the whiteboard collaboration with others. For training mode conferences, only moderators and lecturers can initiate whiteboard collaboration and content notes. Others are the same as the discussion mode conference.
- Storing the collaboration data in a cache: for participants who join halfway through the conference, they can also get the complete collaboration data. If you close the whiteboard collaboration during a conference and you resume it later, the previous collaboration data will not be deleted. If participants initiate whiteboard collaboration at the same time, the whiteboard collaboration is the same. If you end the conference or the content, the collaboration data will be removed.
- For third-party devices that do not support the collaboration feature, they can only receive the collaboration data.
- If you join the conference via WebRTC, you can only receive the collaboration data and the content note, but you cannot initiate them.
- For the audience who see the webcast of the conference, they can also see the whiteboard collaboration and the content notes.
- If you record the conference, the whiteboard collaboration and the content notes will be recorded too.

- [Setting the Collaboration Service](#)
- [Managing Collaboration Files](#)

## Setting the Collaboration Service

If you want to use the collaboration feature of the endpoint, you need to enable the collaboration service.

### About this task

The devices that support the collaboration feature are VC880&VC800&VC500&VC200 video conferencing system in version X.41.0.10 or later.

### Procedure

1. Click **Service > MCU Service > Collaboration service > Add**.
2. Add a collaboration service.
3. Configure the corresponding parameters.

* Enabled :	<input checked="" type="checkbox"/> ON
* Name :	<input type="text" value="collaboration"/>
* Node :	<input type="text" value="Default(10.83.1.151)"/>
* External media port :	<input type="text" value="63000"/> ~ <input type="text" value="63999"/>
* All local networks :	<input checked="" type="checkbox"/> 10.83.1.151

4. Save the configuration.

## Managing Collaboration Files


**Before you begin:** [Setting the Collaboration Service](#)

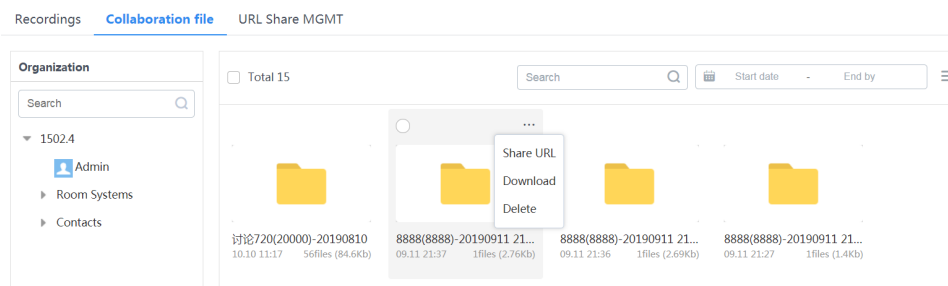
- [Managing Collaboration Files](#)
- [Managing the Sharing Link](#)

### Managing Collaboration Files

After you use the supported device to initiate the whiteboard collaboration or make notes on the shared contents, those files will be stored under the collaboration files in YMS. You can view, edit and share the collaboration files created by any user account or room system account.

### Procedure


1. Click **Media file management > File Management > Collaboration file**.
2. Click the corresponding collaboration file.
3. Click  in the top-right corner of the file.
4. Do one of the following:

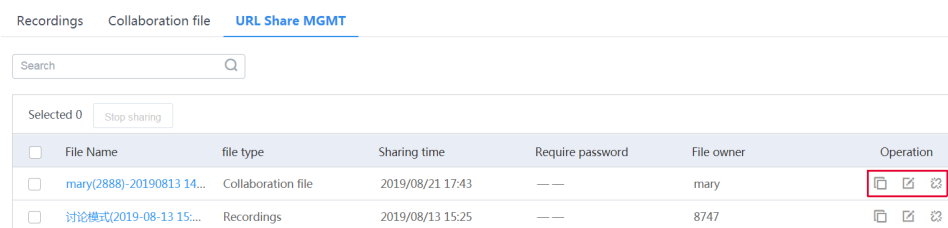





- Click **Share URL**, and share the link with others and set the link parameter.
- Click **Delete** to delete the collaboration file.
- Click **Download** to download the collaboration file.

## Managing the Sharing Link

### Procedure

1. Click **Media file management > File Management > URL Share MGMT**.
2. Do one of the following: click  on the right side of the desired link.



- Click  to copy the link.
- Click  to edit the link parameter.
- Click  to cancel the sharing.

## Configuring the Third-Party Registration Service

To solve the compatibility problem with the third-party devices, you can configure the third-party REG service. If there is an abnormal situation when all third-party devices are registered in a server, you only need to fix the server.

### About this task

Using TLS to register third-party devices in a server is not supported.

### Procedure

1. Click **Service > SIP Service > Third Party REG Service**.
2. Add a third-party registration service.
3. Configure the basic parameters.

Enabled :

\* Name :

\* Node :

**Service address**

*Network	UDP/TCP Port
<input type="text" value="10.83.1.151 (Enabled)"/>	<input type="text" value="5060"/>
<input type="button" value="+ Add"/>	

Support video

Support content sharing

4. Enable **Media Bypass** to improve the server performance and to support a larger number of participants in the conference. Note that the third-party devices have lower compatibility.

If **Support video** is enabled, **Media Bypass** is recommended to be enabled.

If **Media Bypass** is enabled, Media bypass service should be enabled too. For more information, refer to [Configuring the Media Bypass Service](#).

5. Optional: Configure the security policy.

For adding a security group, see [Adding a Security Group](#)

Enable security policy

Mode :  Whitelist  Blacklist

Security Group

Please select the security group

Allow the device in the security group to register in.

Refuse the device in the security group to register in.

## Configuring the GK Service

You can register H.323 devices on YMS via GK service. Therefore, the H.323 devices can call each other, join conferences, and communicate with the SIP devices.

- [Setting the GK Service](#)
- [Enable GK Registration for Accounts](#)

### Setting the GK Service

#### Procedure

1. Click **Service > H.323 Service > Embedded GK Server**.
2. Add a GK service.
3. Configure the parameter.

\* Enabled :  ON

\* Name :

\* Node :

**Registration Service**

\* GK ID :

\* TTL timeout duration :  (Only10~600s)

\* IRR timeout duration :  (Only10~600s)

\* RAS broadcast port(UDP) :

\* RAS port(UDP) :

\* H.225 listener(TCP) :

\* Q.931/H.245(TCP) :  ~

\* Media forwarding port(UDP) :  ~

---

**Conference Gateway**

REG Status : Registered

\* H.225 listener :

\* Q.931/H.245(TCP) :  ~

**Table 22: Basic Parameters**

Parameter	Description
<b>H.235 encryption</b>	<p>The supported types are as follows:</p> <ul style="list-style-type: none"> <li><b>Optional</b>—negotiate with the remote party about whether or not H.235 encryption can be used in H.323 calls.</li> <li><b>Compulsory</b>—H.235 encryption has to be used in H.323 calls.</li> <li><b>Disable</b>—H.235 encryption is disabled in H.323 calls.</li> </ul> <p><b>Default:</b> Optional.</p>
<b>H.239</b>	<p>Enable or disable the H.239.</p> <p><b>Default:</b> enabled. When the H.323 devices call into YMS to join in video conferences via H.323, H.239 is used to receive and share content.</p>
<b>Conference media ByPass</b>	<p>Enable it to improve the server performance and to support a larger number of participants in the conference. Note that the third-party devices have lower compatibility.</p> <p><b>Note:</b> it is disabled by default.</p> <p>If <b>Conference media ByPass</b> is enabled, media bypass service should be enabled too. For more information, see <a href="#">Configuring the Media Bypass Service</a>.</p>

4. Save the configuration.



## Enable GK Registration for Accounts

### Procedure

Click **Account** > **User Account/Room System Account**, and do one of the following:

- If you want to add an account, click **Add Account/ Add**.

Set the parameter.

- If you want to edit an added account, click , or select the account and click .

Set the parameter.

GK REG :  Support H.323 registration

Enable GK authentication (Enable auth is suggested for system security)

## H.323 Gateway

---

To make the call between H.323 devices more convenient, [Setting H.323 Gateway](#) and [Adding a Call Routing Rule](#) should be finished. You can also take H.323 gateway as an endpoint, and register it on a third-party GK server for communication.

- [Setting H.323 Gateway](#)
- [H.323 Gateway Example](#)
- [H.323 Gateway Example \(Taking H.323 Gateway as an Endpoint\)](#)

## Setting H.323 Gateway

### Procedure

1. Click **Service** > **H.323 Service** > **H.323 Gateway** .
2. Add an H.323 gateway.
3. Set the parameters.

\* Enabled :  ON

\* Name :

\* Node :

REG Status : Unregistered

Username : If you take the H.323 gateway as an endpoint and register it in the GK server, you need set these parameters. Otherwise, you do not.

GK address :

\* GK authentication :  ON

\* GK auth name :

\* GK auth password :

\* H.225 listener(TCP) :

\* Q.931/H.245(TCP) :  -

**Table 23: Basic Parameters**

Parameter	Description
<b>H.235 encryption</b>	<p>The supported types are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Optional</b>—negotiate with the remote party about whether or not H.235 encryption can be used in H.323 calls.</li> <li>• <b>Compulsory</b>—H.235 encryption has to be used in H.323 calls.</li> <li>• <b>Disable</b>—H.235 encryption is disabled in H.323 calls.</li> </ul> <p><b>Default:</b> Optional.</p>
<b>H.239</b>	<p>Enable or disable H.239.</p> <p><b>Default:</b> enabled. When the H.323 devices join YMS video conferences via H.323, H.239 is used to receive and share content.</p>
<b>H.460</b>	<p>Enable the H.460 protocol to support firewall traversal for H.323 signaling or not.</p>
<b>Conference media ByPass</b>	<p>Enable it to improve the server performance and to support a larger number of participants in the conference. Note that the third-party devices have lower compatibility.</p> <p><b>Note:</b> it is disabled by default.</p> <p>If <b>Conference media ByPass</b> is enabled, media bypass service should be enabled too. For more information, see <a href="#">Configuring the Media Bypass Service</a>.</p>

4. Click **Advance Option**, and configure the outgoing call rule.

Outgoing Rule :

Priority :	Incoming regex match :	Incoming regex replace string :
1	^00\d{4}	\$1@10.86.0.201.xip.io
+ Add		
Priority :	Outgoing regex match :	Outgoing regex replace string :
1	^3501	95588
+ Add		

H.323 account 3501 registered in YMS (10.86.0.33.xip.io) can dial 003701 to call the H.323 account 3701 registered in YMS (10.86.0.201.xip.io).

Make the caller ID as 95588 rather than 3501.

5. Configure the incoming call rule.

Incoming Rule :

Priority :	Incoming regex match :	Incoming regex replace string :
1	^11\d{4}	\$1@10.86.0.33.xip.io
+ Add		
Priority :	Outgoing regex match :	Outgoing regex replace string :
1	^3701	96866
+ Add		

H.323 account 3701 registered in YMS (10.86.0.201.xip.io) can dial 113501 to call the H.323 account 3501 registered in YMS (10.86.0.33.xip.io).

Make caller ID as 96866 rather than 3701.

6. If you take H.323 gateway as an endpoint and register it on the third-party GK server, configure the GW call rule. The H.323 account on the GK server can directly call the conference ID to join the conference, but the conference ID should match the GW call rule.


GW call rule

Regular expression
410
+ Add

If H.323 account 2558 registered in YMS (10.83.1.221.xip.io) wants to join in the conference 41001 held in YMS (10.83.1.62.xip.io), the following conditions should be met:

1. Conference ID 41001 should match the GW call rule set in YMS (10.83.1.62.xip.io).
2. An H.323 account of YMS (10.83.1.221.xip.io) is registered in YMS (10.83.1.62.xip.io).

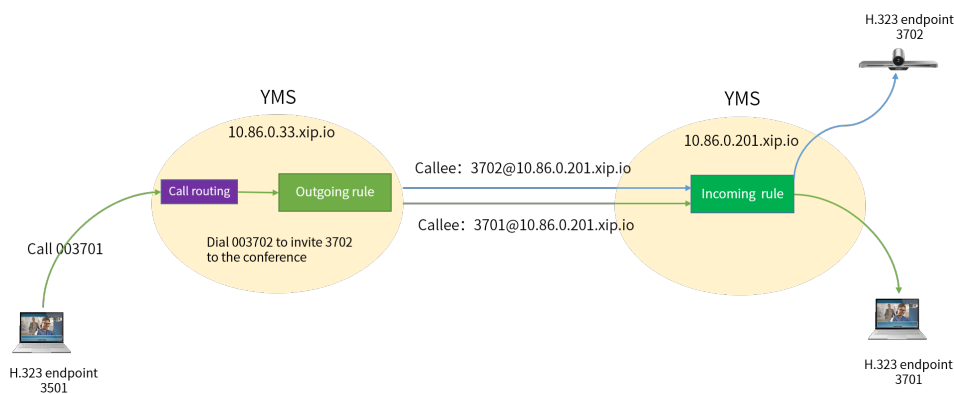
7. Save the configuration.

 **Note:** If the H.323 accounts fail to join conferences by IP call, make sure that *Setting the Interactive Media Service* is correct.

**Related concepts**

*Common Regular Expressions and Replacement Strings*

**H.323 Gateway Example**



• **Situation**

- H.323 account 3501 can dial 003701 to call another YMS H.323 account 3701. You can make the caller ID displayed as 8888 rather than 3701.

- In a conference, you can dial 003702 to call YMS account 3702 to join the conference. You can make the caller ID displayed as 8888 rather than 3701.
- **The configurations are as below:**
  - Enable the H.323 gateway service on both servers
  - Set the outgoing call rule and the call routing on server 10.86.0.33.xip.io

Outgoing Rule :

Priority :	Incoming regex match :	Incoming regex replace string :
1	^00\d{4}	\$1@10.86.0.201.xip.io
+ Add		

---

test      1      ^00\d{4}      H.323 GW / aa       ON

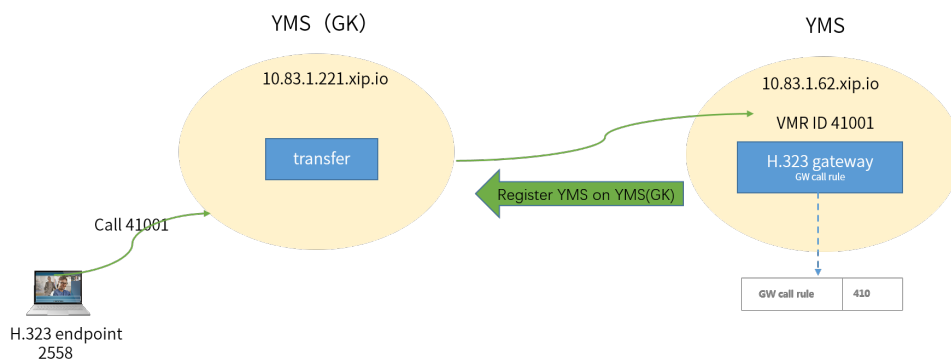
- Set the incoming call rule on server 10.86.0.201.xip.io

Incoming Rule :

Priority :	Incoming regex match :	Incoming regex replace string :
+ Add		

Priority :	Outgoing regex match :	Outgoing regex replace string :
1	.+	8888@10.86.0.201.xip.io
+ Add		

### H.323 Gateway Example (Taking H.323 Gateway as an Endpoint)



- **Situation**
  - H.323 account 2558 can dial 41001 to call the conference 41001 held in another YMS.
- **The configurations are as below:**
  - Set the GK Service on server 10.83.1.221.xip.io
  - Enable the H.323 gateway service on server 10.83.1.62.xip.io
  - Set the GK authentication and the GW call rule on server 10.83.1.62.xip.io

Username :	<input type="text" value="2224"/>						
GK address :	<input type="text" value="10.83.1.221"/>						
* GK authentication :	<input checked="" type="checkbox"/> ON						
	<table> <tr> <td>* GK auth name :</td> <td><input type="text" value="2224"/></td> </tr> <tr> <td>* GK auth password :</td> <td><input type="password" value="*****"/></td> </tr> </table>	* GK auth name :	<input type="text" value="2224"/>	* GK auth password :	<input type="password" value="*****"/>		
* GK auth name :	<input type="text" value="2224"/>						
* GK auth password :	<input type="password" value="*****"/>						
GW call rule	<table> <tr> <td>Regular expression</td> <td><input type="text" value="410"/></td> <td><input type="button" value="X"/></td> </tr> <tr> <td></td> <td><input type="button" value="+ Add"/></td> <td></td> </tr> </table>	Regular expression	<input type="text" value="410"/>	<input type="button" value="X"/>		<input type="button" value="+ Add"/>	
Regular expression	<input type="text" value="410"/>	<input type="button" value="X"/>					
	<input type="button" value="+ Add"/>						

## Setting the IP Call

---

For convenience, you can set the rules for the incoming and outgoing IP calls, and you need [Setting the IP Call Service](#) and [Adding a Call Routing Rule](#) .

- [Setting the IP Call Service](#)
- [IP Call Example](#)

## Setting the IP Call Service

### About this task



**Note:** If you want to make IP calls on your VCD/VCM, you need to sign out your YMS account first.

### Procedure

1. Click **Service** > **SIP Service** > **IP Call Service**.
2. Add an IP call service.
3. Set the parameters.

Enabled :

\* Name :

\* Node :

\* Outgoing protocol :

**Service address**

*Network	UDP/TCP Port	TLS Port
10.83.1.150 (Enabl	5060	5062

Support video

4. Enable **Replace the calling domain with the local IP**, and when you invite participants to join the conference by IP call, the devices of the invited participants will display the server IP address as the caller ID.

It is enabled by default.

5. Enable **Media Bypass** to improve the server performance and to support a larger number of participants in the conference. Note that the third-party devices have lower compatibility.

If **Support video** is enabled, **Media Bypass** is recommended to be enabled.

If **Media Bypass** is enabled, Media bypass service should be enabled too. For more information, refer to [Configuring the Media Bypass Service](#).

6. Optional: Configure the security policy.

For adding a security group, see [Adding a Security Group](#)

Enable security policy

Mode :  Whitelist  Blacklist

Security Group

Please select the security group

Allow the IP address in this group to call into.

Refuse the IP address in this group to call into.

7. Configure the outgoing call rule.

Outgoing Rule :

Priority :	Incoming regex match :	Incoming regex replace string :
1	<code>^10086</code>	10.81.43.7
1	<code>^conf_(id(5))@</code>	<code>\$1@10.86.0.201.xip.io</code>
+ Add		

Priority :	Outgoing regex match :	Outgoing regex replace string :
1	<code>^3802</code>	<code>95588@10.86.0.33.xip.io</code>
1	<code>.+</code>	<code>95599@10.86.0.201.xip.i</code>
+ Add		

SIP account 3802 can dial 10086 to call 10.81.43.7.

Account 8888 registered in YMS (10.86.0.33.xip.io) can dial conf\_55555 to call the conference 55555 held in YMS (10.86.0.201.xip.io).

Make the caller ID displayed in the remote call or conference as 95588 rather than 3802.

Make the caller ID displayed in the conference 55555 as 95599 rather than 3802@10.86.0.33.xip.io.

8. Configure the incoming call rule.

Incoming call rule

Priority :	Callee regex match :	Callee regex replace string :
2	<code>^(id(5))*123456@</code>	<code>\$1@10.86.0.220.xip.io</code>
+ Add		

Priority :	Caller regex match :	Caller regex replace string :
1	10.81.43.7	10086
+ Add		

A user (10.81.43.7) can dial 22222\*\*123456@10.86.0.220 to call the conference 22222\*\*123456@10.86.0.220.xip.io.

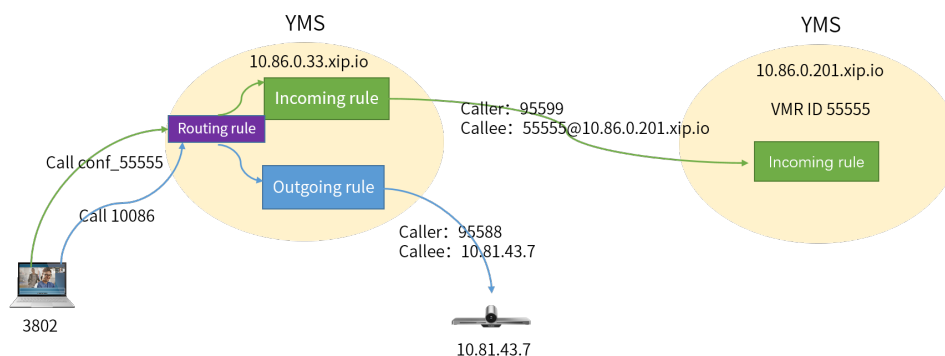
Make the caller ID displayed in a conference as 10086 rather than 10.81.43.7.

9. Save the configuration.

**Related concepts**

*Common Regular Expressions and Replacement Strings*

**IP Call Example**



• **Situation**

- Call a number and transfer it to an endpoint, for example, SIP account 3802 can dial 10086 to call 10.81.43.7 via the automatical IP call. You can make the caller ID displayed as 95588 rather than 3802.
- Dial conf\_conference ID to join the conference held in another server, for example, account 3802 registered in YMS (IP address 10.86.0.33) can dial conf\_55555 to call the conference (VMR ID 55555) in YMS (IP address 10.86.0.201). You can make the caller ID displayed in the VMR as 95599 rather than 3802@10.86.0.33.xip.io.

• **The configurations are as below:**

- Enable the IP call services on both servers

- Set the outgoing call rule and the call routing on server 10.86.0.33.xip.io

#### Outgoing call rule

Priority :	Callee regex match :	Callee regex replace string :
1	^10086	10.81.43.7
1	^conf_(d{5})@	\$1@10.86.0.201.xip.io
<a href="#">+ Add</a>		

Priority :	Caller regex match :	Caller regex replace string :
1	^3802	95588@10.86.0.30.xip.io
1	.+	95599@10.86.0.201.xip.io
<a href="#">+ Add</a>		

#### Call Routing

Name	Priority	Destination match	Call Target/Out Location	Enabled	Operation
对等trunk	1	^55(d+)	Peer Trunk / 对等Trunk	OFF	<a href="#">✎</a>
rr	1	^030	Register Trunk / e	ON	<a href="#">✎</a>
dd	1	^10086	H.323 GW / 150	ON	<a href="#">✎</a>
IP call 2	2	^conf	IP Call / IP直播	ON	<a href="#">✎</a>
zhibo	3	^10086	IP Call / IP直播	ON	<a href="#">✎</a>

Total 5 10page < 1 > Go to 1 Pages

- set the incoming call rule on server 10.86.0.201.xip.io

#### Incoming call rule

Priority :	Callee regex match :	Callee regex replace string :
2	.+	conference_ivr@10.86.0.:
1	^(d{5})@	\$1@10.86.0.201.xip.io
<a href="#">+ Add</a>		

## Call Routing

Call routing rule is used for routing the incoming calls to YMS and the outgoing calls made by YMS to a destination. For the incoming calls from a gateway, you need to configure the inbound rule and the number translation rule to match this gateway. Likewise, you need to configure the outbound rule and the number translation rule for the outgoing calls to match the desired gateway.

If you use the following gateway for the incoming/outgoing calls, you need to configure the corresponding number translation rule.

[Setting the IP Call Service](#)

[Communicating with the PSTN](#)

[Setting the Peer Trunk Service](#)



*Configuring the REG Trunk Service*

*Setting the SFB Gateway*

*H.323 Gateway*

- *Process of Call Routing*
- *Regular Expressions*
- *Adding a Call Routing Rule*
- *Setting the Call Routing Rule for Rejecting*
- *Add a Number Filter*

## Process of Call Routing

Familiar yourself with the following terms:

Call routing rule: it applies to the outgoing calls and matches the outgoing-number translation rule of the gateway.

Incoming-number translation rule: it matches the incoming calls when the calls are routed through the gateway.

Outgoing-number translation rule: it matches the outgoing calls when the calls are routed through the gateway.



## Regular Expressions

Regular expressions can be used for configuring the call routing rules and the number translation rules.

- [Metacharacters](#)
- [Common Regular Expressions and Replacement Strings](#)

### Metacharacters

**Table 24: Metacharacters in regular expressions**

Characters	Description
^	Matches the starting position of a line.
\$	Matches the ending position of a line.
*	Matches zero or more times of the preceding character or expression.
+	Matches one or more times of the preceding character or expression.
?	Matches zero or one time of the preceding character or expression.
	Matches either the expression before or the expression after the choice operator.
{n}	Matches n times of the preceding character or expression.
{n,}	Matches at least n times of the preceding character or expression.
{n,m}	Matches n to m times of the preceding character or expression.
[xyz]	Matches any character specified in the brackets.
[^xyz]	Matches anything except the character specified in the brackets.
[a-z]	Matches the characters within the range specified in the brackets.
[^a-z]	Matches anything except the characters within the range specified in the brackets.
\d	Matches a digit character.
\D	Matches a non-digit character.

### Common Regular Expressions and Replacement Strings

**Table 25: Common Regular Expressions and Replacement Strings**

PCRE	Description
.+	Matches any character except for \n.
^(1\d{10})\$	Matches the 11-digit number which starts with 1. For example, 12345678912
^0(d+)\$	Matches the number with 2 or more digits which starts with 0. For example, 02, 0157

PCRE	Description
<code>^(13[0-9] 14[57] 15[012356789] 18[012356789])\d{8}\$</code>	<p>Matches 11-digit mobile phone number, the first 3 digits includes the following types, and the last 8 digits can be any digits:</p> <ul style="list-style-type: none"> <li>• Start with 13 and the third number is any digit from 0 to 9</li> <li>• Start with 14 and the third number is 5/7</li> <li>• Start with 15 and the third number is 0/1/2/3/5/6/7/8/9</li> <li>• Start with 18 and the third number is 0/1/2/3/5/6/7/8/9</li> </ul> <p>For example, 13012345678, 14512345678, 15987654321 or 18243218765</p>
<code>^(d{3,4})?d{7,8}\$</code>	<p>Matches the following number format:</p> <ul style="list-style-type: none"> <li>• <b>XXX-XXXXXXXX, 10-digit</b></li> <li>• <b>XXX-XXXXXXXX, 11-digit</b></li> <li>• <b>XXXX-XXXXXXXX, 11-digit</b></li> <li>• <b>XXXX-XXXXXXXX, 12-digit</b></li> <li>• <b>XXXXXXXX, 7-digit</b></li> <li>• <b>XXXXXXXX, 8-digit</b></li> </ul> <p>For example, XXXX-XXXXXXXX represents 07311234567 or other 7-digit number</p>
<code>\d{3}-\d{8} \d{4}-\d{7}</code>	<p>Matches the following number format:</p> <ul style="list-style-type: none"> <li>• <b>XXX-XXXXXXXX, 11-digit</b></li> <li>• <b>XXXX-XXXXXXXX, 11-digit</b></li> </ul> <p>For example, XXX-XXXXXXXX represents 012-12345678 or other 11-digit number, XXXX-XXXXXXXX represents 0123-1234567 or other 11-digit number</p>
<code>(d{11}) ((d{3,4})?(d{7,8})-(d{1,4}))?</code>	<p>Matches the following number format:</p> <ul style="list-style-type: none"> <li>• <b>11-digit mobile phone number</b></li> <li>• <b>XXXXXXXX, 8-digit number</b></li> <li>• <b>XXXXXXXX, 7-digit number</b></li> <li>• <b>XXX/XXXX-XXXXXXXX/XXXXXXXX, 4 formats in total</b></li> <li>• <b>XXX/XXXX-XXXXXXXX/XXXXXXXX-X/XX/XXX/XXXX, 16 formats in total</b></li> <li>• <b>XXXXXXXX/XXXXXXXX-X/XX/XXX/XXXX, 8 formats in total</b></li> </ul> <p>For example, XXXX-XXXXXXXX represents 0731-8784888 or other 11-digit number</p>

**Table 26: Regex replace string**


PCRE	Description
\$1@\$2	Matches the content in the first and the second parentheses of the regular expression. For example, the regular expression is <code>avmcu\.(\\d{1,10})@(xiamen.yealinksfb\\.com)</code> , and the regex replace string is <code>(\\d{1,10})@(xiamen.yealinksfb\\.com)</code> .

## Adding a Call Routing Rule

### Procedure

1. Click **Call Configuration > Call Routing**.
2. Add a call routing rule.
3. Configure the parameters of the call routing rules.

**Table 27: Parameters of the Call Routing Rule**

Parameter	Description
<b>Enabled</b>	Enable or disable the call routing rule. <b>Default:</b> enabled.
<b>Name</b>	Specify the name of the call routing rule.
<b>Priority</b>	The priority of the call routing rule. The smaller the number is, the higher the priority is. When you place a call, the server will look up the first appropriate call routing rule according to the priority in ascending order.
<b>Destination regex match</b>	Specify the desired regular expressions or the number field to match the target call number.  <b>Note:</b> This configuration should be the same as the incoming regex match of the outgoing call rule you set in each service. If the match succeeds, the server will use this call routing rule.

4. Optional: If you want to restrict the number you call, enable **Caller filtering policy**, and configure the parameters.  
Add a filtering policy, see [Add a Number Filter](#)

\* Caller filtering policy : ?  ON

\* Mode :  Whitelist  Blacklist

\* Filter :

Select filter

test ✕

→ Allow the account in the filter to call into.  
→ Refuse the account in the filter to call into.

5. Configure the parameter of the outgoing location.

**Table 28:**

Parameter	Description
<b>Call target</b>	Specify the call target. <ul style="list-style-type: none"> <li>• <b>Reject</b></li> <li>• <b>IP Call</b></li> <li>• <b>Federation service</b></li> <li>• <b>Peer Trunk</b></li> <li>• <b>PSTN</b></li> <li>• <b>SfB</b></li> <li>• <b>Register Trunk</b></li> <li>• <b>H.323 GW</b></li> </ul>
<b>Outgoing location</b>	Specify the gateway used to place the call. If the call number matches this call routing rule, it is called via this gateway.

6. Save the configuration.

#### Related tasks

[Add a Number Filter](#)

## Setting the Call Routing Rule for Rejecting

You can add the call routing rules for rejecting the outgoing calls, that is, when the number you call matches the regular expression set in the call routing rule, your call will be rejected.

### Procedure

1. Click **Call Configuration > Call Routing**.
2. Add a call routing rule.
3. Set the parameters.

**Routing Information**

\* Enabled :  ON

\* Name :

\* Priority :  (Only1~200)

**Rule Settings**


\* Destination regex match : 

\*Call target :  \*Outgoing location :

4. To restrict the number you call, enable **Caller filtering policy**, and set the parameters.

For example, if you want to reject the call to the YMS account whose number is not from 5555 to 9999, you can put the number from 5555 to 9999 into the blacklist. Otherwise, you can put the number into the whitelist.

Add a filter, refer to [Add a Number Filter](#)

\* Caller filtering policy :   ON

\* Mode :  Whitelist  Blacklist

\* Filter :

Select filter

test ×

5. In the **Call target** field, select **Reject**.

\* Outgoing location :

\*Call target : \*Outgoing location :

Reject ×

6. Save the configuration.

## Add a Number Filter

### Procedure

1. Click **Call Configuration > Number Filter > Add**.
2. Set the parameters.

Enabled :  ON

\* Name :

Description :

3. Click **Add** and set the number filter.

Add ×

\* Type :  Extension section  Regular expression

\* Origin extension :

\* Rear extension :

Description :

4. Save the configuration.

**Related concepts**[Common Regular Expressions and Replacement Strings](#)**Related tasks**[Adding a Call Routing Rule](#)

## Managing Accounts

---

You can manage the user accounts, the room system accounts and other accounts by group, and you can add, edit, and delete the above accounts.

- [User Account, Room System Account and Other Accounts](#)
- [Managing Accounts by Group \(Optional\)](#)
- [Parameters of User Account and Room System Account](#)
- [Add a User Account](#)
- [Importing a Batch of Accounts](#)
- [LDAP](#)

## User Account, Room System Account and Other Accounts

---

The differences among user accounts, room system accounts and other accounts are as follows.

Type	Description	Note
User Account	It can be used to log into YMS and register in Yealink video conferencing devices. You can register the same user account on five devices at most at the same time.	They are called as YMS accounts.
Room system account	The account is used to associate with the device in the video meeting room. You can register the same room system account on five devices at most at the same time.	
Other account	The devices you add by entering the IP address or URL. You can invite these devices during a conference. Those devices do not have YMS accounts.	No limit.

**Related concepts**[Parameters of User Account and Room System Account](#)**Related tasks**[Add a User Account](#)[Importing a Batch of Accounts](#)

## Managing Accounts by Group (Optional)

---

If you want to manage user accounts, room system accounts, and other accounts by group, you can customize the group according to the enterprise organization.



**Note:** The organization root is the enterprise name by default. You can manage user accounts, room system accounts, and other accounts of your group and your subordinate groups.

- **Adding a Group**

1. Click **Account > User Account/Room System Account/Other Account > Add Group**.

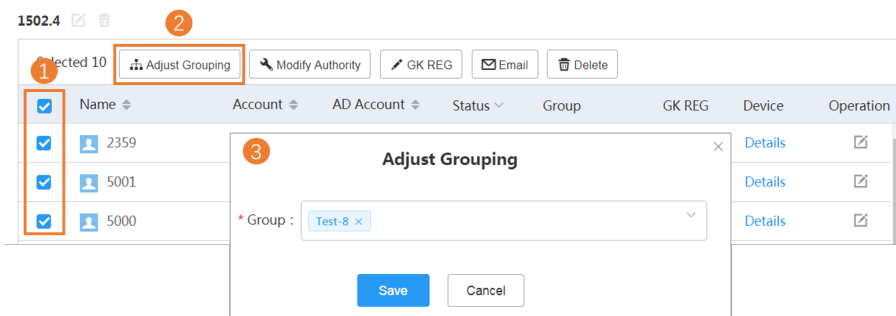
### Add Group

\* Group name :

\* Upper group :

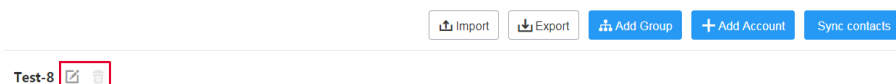
- **Adjusting the Group**


1. Click **Account > User Account/Room System Account/Other Account**.



- **Editing/Deleting the Group**

1. Click **Account > User Account/Room System Account/Other Account**.



 **Note:** If a group has subordinated groups, you cannot delete this group.

## Parameters of User Account and Room System Account

You need to know the account parameters before adding accounts.

**Table 29: Introduction of the corresponding parameters**

Parameter	Description
<b>Common parameters</b>	
<b>AD Account</b>	If you select <b>Obtain from AD server</b> , specify the AD account, which you use to obtain the AD account name and account number. You can get the AD account from the AD server administrator.



Parameter	Description
<b>Authority</b>	<p>The authorities owned by this account.</p> <p>The available authorities are as below:</p> <ul style="list-style-type: none"> <li>• <b>A</b>: this account can see all user accounts, room system accounts, VMRs (synced to the directory) and other accounts.</li> <li>• <b>B</b>: this user account/room system account can see only the user accounts/the room system accounts in his group and the groups with the same level as his group.</li> </ul> <p>If the user is in the root node, the range that he can see is the same as A.</p> <ul style="list-style-type: none"> <li>• <b>C</b>: this user account/room system account can see only the user accounts/room system accounts in his group.</li> <li>• <b>D</b>: this account can only see himself.</li> <li>• <b>Custom</b>: you can customize the visible range for this account.</li> </ul>
<b>Enable schedule</b>	<p>Allow or refuse this account to schedule meeting rooms and conferences.</p> <p><b>Default:</b> enabled.</p>
<b>Enable Meet Now</b>	<p>Allow or refuse this account to create Meet Now conferences.</p> <p><b>Default:</b> enabled.</p>
<b>Enable call authority</b>	<p>If you enable this feature, this account can only call the contacts, which are visible to him.</p> <p><b>Default:</b> disabled.</p>
<b>Enable live caption privilege</b>	<p>If you enable this feature, the live caption is available on the video image of the conference scheduled by this account. You need to contact Yealink technical support engineers to enable this feature.</p> <p><b>Default:</b> disabled. The voice transfer server should support this feature. For more information about it, contact Yealink technical support engineers.</p>
<b>The parameters only owned by the user accounts</b>	
<b>Enable Schedule Virtual Meeting Room</b>	<p>If you enable this configuration and this account is the moderator of a VMR, this account can only schedule VMRs via Outlook. If you enable this configuration, but this account is not the moderator of a VMR, this account has no privilege to schedule VMRs via Outlook.</p> <p><b>Note:</b> only when you contact Yealink technical support engineers to enable this feature can you see this configuration.</p>

**Related concepts**

*User Account, Room System Account and Other Accounts*

**Related tasks**

*Add a User Account*

*Importing a Batch of Accounts*

*Configuring the LDAP*

## Add a User Account

### About this task


 **Note:** For adding an AD Account, refer to [LDAP](#).

### Procedure

1. Click **Account > User Account/Room System Account/Other Account**.
2. Add an account.

**Add Account**

Basic Settings Advanced Option



User account

Account info :  Manual  Obtain from AD server

\* Name :

\* Account :

Password :   
Password strength : Strong  
A random password will be generated if not filled


Group :

Mailbox :   
The mailbox is used to receive messages from system

Authority :

Enable schedule  
 Enable Schedule Virtual Meeting Room (Cannot be opened at the same time with Schedule)  
 Enable Meet Now  
 Enable call authority (Only the contacts visible can be

Basic Settings    Advanced Option



Account info :  Manual    Obtain from AD server

\* Name :

\* Account :  ✕

Password :   
■■■■■■■■■■ Password strength : Strong  
A random password will be generated if not filled

**Room system account**

Group :  ✕ ▼

Mailbox :   
The mailbox is used to receive messages from system

Authority :  ▼

Enable schedule

Enable Meet Now

Enable call authority (Only the contacts visible can be called)

Enable Recording ( The user will be allowed to record during the meeting )

**Add Account**

---

\* Name :

\* Number :

**Room system account**

Group :

Mailbox :

The mailbox is used to receive messages from system

---

3. If you enter the email addresses when adding accounts, click **Send mail**, and the account information will be sent to the users.



**Note:** If you do not, you need to inform the corresponding users of the initial passwords, and remind them to change the passwords promptly.

#### Related concepts

[User Account, Room System Account and Other Accounts](#)

[Parameters of User Account and Room System Account](#)

#### Related tasks

[Configuring the LDAP](#)

## Importing a Batch of Accounts

---

You can import a template to add a batch of accounts. Before that, you need to download the template first.

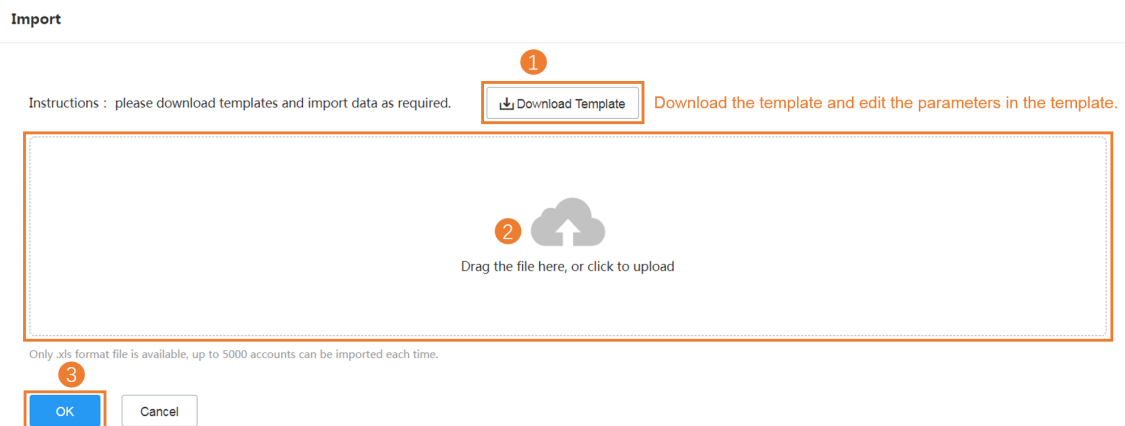
#### About this task



**Note:** For adding an AD Account, refer to [LDAP](#).

#### Procedure

Click **Account** > **User Account/Room System Account/Other Account** > **Import**.



### Related concepts

[User Account, Room System Account and Other Accounts](#)

[Parameters of User Account and Room System Account](#)

### Related tasks

[Configuring the LDAP](#)

## LDAP

---

You can connect YMS to the LDAP server that supports LDAPv3. Therefore, when the devices register in YMS via SIP/H.323, the devices can obtain LDAP contacts. Microsoft Active Directory is supported.

YMS not only allows you to add an LDAP account but also allows you to synchronize accounts on YMS with the accounts on LDAP server. The accounts registered on YMS can see the synchronized LDAP accounts in their contact list, which allows them to place P2P calls with their contacts or invite their contacts to join conferences.

- [Configuring the LDAP](#)
- [Adding an LDAP Account](#)
- [Synchronizing LDAP Accounts](#)

## Configuring the LDAP

### About this task

#### Procedure

1. Click **Account** > **LDAP**.
2. Configure the parameters.

**LDAP**

Enable :  ON  
Used to obtain information from AD server

\* Server address :

\* Port :

\* Base DN :

\* Username :

\* Password :

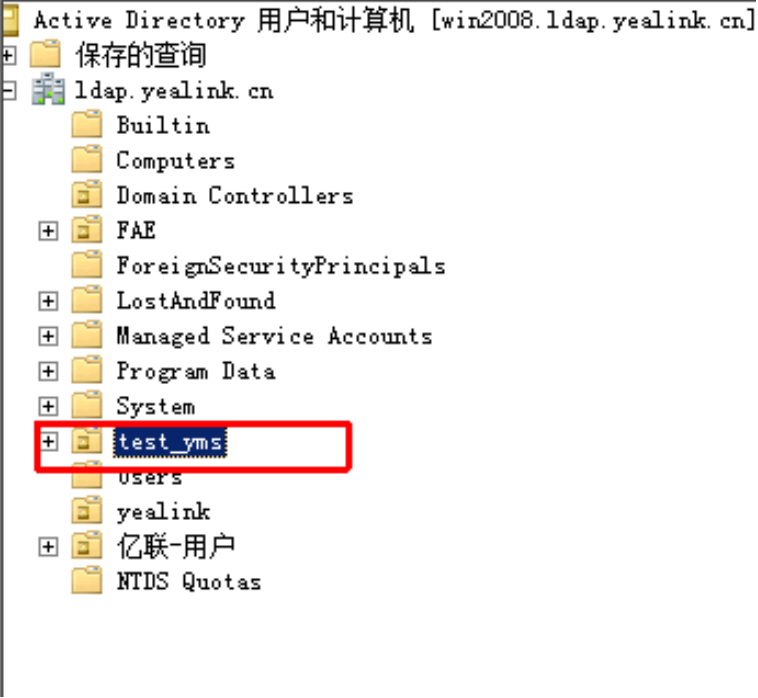
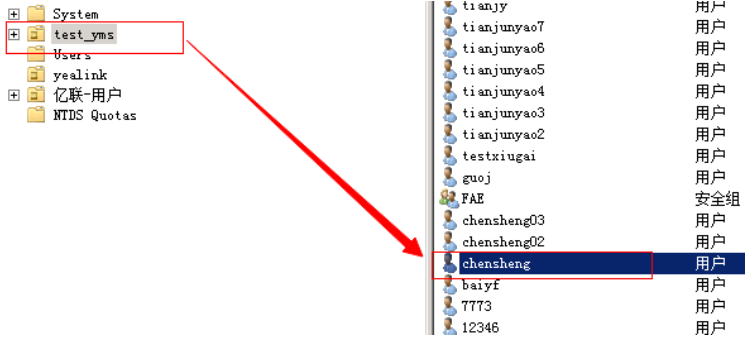
\* Name Property :

\* Number Property :

\* AD account Property :

**Table 30: LDAP parameters**

Parameter	Description
<b>Enable</b>	Enable or disable the LDAP. <b>Default:</b> disabled.
<b>Server address</b>	Specify the domain name or the IP address of the LDAP server.
<b>Port</b>	Specify the port of the LDAP server.

Parameter	Description																																
<b>Base DN</b>	<p>Set the root path for YMS to obtain the LDAP accounts.</p> <p><b>For example</b>, OU=test_yms,DC=ldap,DC=yealink,DC=cn</p> <p><b>Obtaining method:</b> the image below is the directory of AD server. If YMS wants to obtain the user information under this contents, right click test_yms-&gt;Attribute-&gt;Attribute Editor,, view the attribute value <i>OU=test_yms,DC=ldap,DC=yealink,DC=cn</i>, and fill this value in the <b>Base ND</b> field on YMS.</p>  <p>The screenshot shows the Active Directory console for 'win2008.ldap.yealink.cn'. The directory structure includes folders like 'ldap.yealink.cn', 'BuiltIn', 'Computers', 'Domain Controllers', 'FAE', 'ForeignSecurityPrincipals', 'LostAndFound', 'Managed Service Accounts', 'Program Data', 'System', 'test_yms', 'Users', 'yealink', '亿联-用户', and 'NTDS Quotas'. The 'test_yms' folder is highlighted with a red box.</p>																																
<b>Username</b>	<p>Specify the username used to log into the LDAP server.</p> <p><b>Note:</b> The username is provided by the AD server administrator.</p> <p>For example, the “chensheng” account in the test_yms contents. The user in the <i>test_yms</i> directory is acceptable. The username is <i>chensheng@ldap.yealink.cn</i>.</p>  <p>The screenshot shows the 'test_yms' folder highlighted with a red box. A red arrow points from this box to a list of users. The user 'chensheng' is highlighted with a blue box in the list.</p> <table border="1" data-bbox="1023 1413 1339 1749"> <tbody> <tr><td>tianjy</td><td>用户</td></tr> <tr><td>tianjunyao7</td><td>用户</td></tr> <tr><td>tianjunyao6</td><td>用户</td></tr> <tr><td>tianjunyao5</td><td>用户</td></tr> <tr><td>tianjunyao4</td><td>用户</td></tr> <tr><td>tianjunyao3</td><td>用户</td></tr> <tr><td>tianjunyao2</td><td>用户</td></tr> <tr><td>testxiugai</td><td>用户</td></tr> <tr><td>guoj</td><td>用户</td></tr> <tr><td>FAE</td><td>安全组</td></tr> <tr><td>chensheng03</td><td>用户</td></tr> <tr><td>chensheng02</td><td>用户</td></tr> <tr><td>chensheng</td><td>用户</td></tr> <tr><td>baiyf</td><td>用户</td></tr> <tr><td>7773</td><td>用户</td></tr> <tr><td>12346</td><td>用户</td></tr> </tbody> </table>	tianjy	用户	tianjunyao7	用户	tianjunyao6	用户	tianjunyao5	用户	tianjunyao4	用户	tianjunyao3	用户	tianjunyao2	用户	testxiugai	用户	guoj	用户	FAE	安全组	chensheng03	用户	chensheng02	用户	chensheng	用户	baiyf	用户	7773	用户	12346	用户
tianjy	用户																																
tianjunyao7	用户																																
tianjunyao6	用户																																
tianjunyao5	用户																																
tianjunyao4	用户																																
tianjunyao3	用户																																
tianjunyao2	用户																																
testxiugai	用户																																
guoj	用户																																
FAE	安全组																																
chensheng03	用户																																
chensheng02	用户																																
chensheng	用户																																
baiyf	用户																																
7773	用户																																
12346	用户																																

Parameter	Description
<b>Password</b>	Specify the password used to log into the LDAP server. <b>Note:</b> The password is provided by the LDAP server administrator. <b>For example</b> , the LDAP username is <i>chensheng@ldap.yealink.cn</i> Enter the password of this username.
<b>Name Property</b>	Set the name property of the returned LDAP account. <b>For example</b> , name or cn. When the name property is name and when you create a YMS account by obtaining from the AD server, the name of YMS account corresponds to the value of name of the corresponding AD account.
<b>Number Property</b>	Set the number property of the returned LDAP account. <b>For example</b> , telephoneNumber, mobile, or ipPhone. When the number property is telephoneNumber and when you create a YMS account by obtaining from the AD server, the number of YMS account corresponds to the value of number of the corresponding AD account. Additionally, the value of telephoneNumber in the AD account should be within the number range of the system account (refer to <a href="#">Allocating the Number Resource</a> ) and cannot be empty. If it does not meet this condition, there will be an error when creating a YMS account by obtaining from the AD server.
<b>AD account Property</b>	Set the account property of the returned LDAP account. <b>For example</b> , sAMAccountName
<b>Mailbox Property</b>	Set the property name of the mailbox in the LDAP server. <b>For example</b> , mail or email.
<b>Web portal login with AD is preferred</b>	If users often use the LDAP account to log into YMS, you can enable this feature. If you enable it, users will go to the AD Login when they access the Login page. Otherwise, they will go to the User Login by default.

### 3. Click **Connection Test**.

If the configuration is correct, the prompt “Connection successful” will pop up.

### 4. Click **Save**.

#### **Related concepts**

[Parameters of User Account and Room System Account](#)

#### **Related tasks**

[Add a User Account](#)

[Importing a Batch of Accounts](#)

## Adding an LDAP Account

### **Before you begin**

[Configuring the LDAP](#)

### **Procedure**

1. Click **Account > User Account/Room System Account**.
2. Add the account and save the configuration.



The account number should be within the number field (see [Allocating the Number Resource](#)). Otherwise, the page prompts that the account is invalid.

Account info :  Manual  Obtain from AD server

AD Account : 1523 Enter an AD account.

Name : 1523 The name and account will be filled in automatically.

Account : 1523

## Synchronizing LDAP Accounts

### Before you begin

- [Configuring the LDAP](#)
- You need to contact Yealink technical support engineers to subscribe to this feature.

### Procedure

1. Click **Account** > **User Account**.
2. Click **Sync contacts**.

Test-8

Selected 0

<input type="checkbox"/>	Name	Account	AD Account	Status	Group	GK REG	Device	Operation
<input type="checkbox"/>	3505	3505	---	Offline	35XX	No	Details	<input type="checkbox"/>

### Results

If you succeed in synchronizing accounts, you can see the LDAP accounts in the User Account list. Those LDAP accounts meet the condition you set in the OU parameter.



**Note:** The account number should be within the number field (see [Allocating the Number Resource](#)). Otherwise, the page prompts that the synchronization fails.

## Managing Meeting Rooms

You can add meeting rooms, manage the meeting rooms by group, invite participants to join the VMRs via emails, or others.

- [Entity Meeting Room and the Virtual Meeting Room](#)
- [Managing Meeting Rooms by Groups \(Optional\)](#)
- [Adding Entity Meeting Rooms](#)
- [Adding a VMR](#)
- [Discussion Mode and Training Mode](#)
- [Sending Emails to VMR Participants](#)

## Entity Meeting Room and the Virtual Meeting Room

The meeting room includes the entity meeting room and the virtual meeting room(VMR).

**Table 31: Entity Meeting Room and the Virtual Meeting Room**

Meeting room	Definition	Classification
Entity meeting room	The entity meeting rooms can be used to schedule OA conferences.	General meeting room Without video conferencing devices deployed in the meeting room.
		Video meeting room With video conferencing devices deployed in the meeting room.
VMR	Users can join VMRs at any time to have video conferences, and they can also schedule VMRs via Outlook.	No

For more information about scheduling meeting rooms, refer to [Yealink Meeting Server User Guide](#).

### Related tasks

[Adding Entity Meeting Rooms](#)

[Adding a VMR](#)

## Managing Meeting Rooms by Groups (Optional)

According to the meeting room locations, you can customize the organization relationship to manage meeting rooms by groups. The organization root is the enterprise name by default. You can manage meeting rooms in your group and the subordinate groups.

- **Adding a Group**

1. Click **Meeting Room > Entity Meeting Room/Virtual Meeting Room > Add Group**.

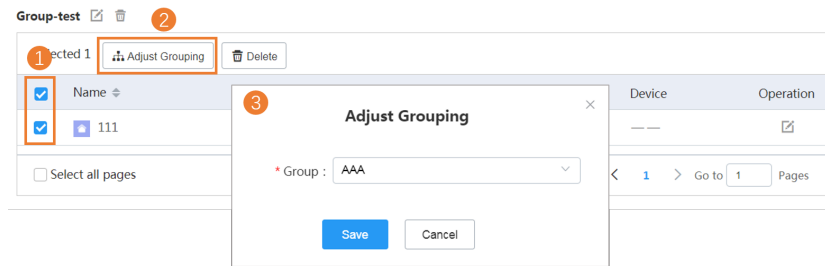
Add Group ×

\* Group name :

\* Upper group :

- **Adjusting the Group**


1. Click **Meeting Room > Entity Meeting Room/Virtual Meeting Room** .



- **Editing/Deleting the Group**

1. Click **Meeting Room > Entity Meeting Room/Virtual Meeting Room**.



 **Note:** If a group has subordinated groups, you cannot delete this group.

## Adding Entity Meeting Rooms

You can add entity meeting rooms for users to schedule conferences.

### Before you begin

If you want to add a video meeting room, you need to add a room system account/other account first, see [Add a User Account](#).

### Procedure

1. Click **Meeting Room > Entity Meeting Room**.
2. Add a meeting room.

**Add Meeting Room**

\* Type :  Common  Video

\* Name :

\* Group :

\* Account bound :

*If you select Video, select an account to bind with.*

### Related concepts

[Entity Meeting Room and the Virtual Meeting Room](#)

## Adding a VMR

You can add a VMR so users can call into the VMR to join the video conference at any time.

### Procedure

1. Click **Meeting Room > Virtual Meeting Room**.
2. Add a meeting room.

**Add Meeting Room**

Basic Settings | **Advanced Option**

**Common Setting**

\* Name :

\* Alias :

\* Mode :  Discussion  Training

\* Conference ID :

Require Password (Password is suggested for conference security)

\* Password :

\* Group :

\* Organizer :

Moderator :

Favorites :

Sync contacts :

\* Max video parties :  (1-1500)

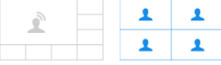
\* Max audio-only parties :  (1-1500)

**Permission setting** ^

Max video resolution :

Max content resolution :

Max call bandwidth :

Default layout : 

onePlusN  Equal NxN

Display native video :

Content only :

Enable live caption privilege :

Mute participants upon entry :

Lock the meeting automatically :

RTMP live :

Join by IP Call :

Join with browser :

Auto recording :

Auto redialing :

---

Basic Settings | **Advanced Option**

Video port resource reservation:  OFF

\* Recording Privilege:  Moderator  Moderator & Guests

**Table 32: Introduction of the corresponding parameters**

Parameter	Description
<b>Alias</b>	The call rules based on the alias will be generated after you create the VMR. <b>Prerequisite:</b> <a href="#">Setting the IP Call</a> and <a href="#">Setting H.323 Gateway</a> are finished. For example, if the alias of the VMR is test and the meeting room ID is 88888, the call rules will be generated automatically in the IP call service and gateway service. Users can directly dial test@domain name to call into 88888.
<b>Enable live caption privilege</b>	If you enable this feature, the live caption is available on this VMR. You can contact Yealink technical support engineer to subscribe to this service. <b>Note:</b> it is disabled by default. The voice transfer server should support this feature. For more information about it, contact Yealink technical support engineers.
<b>Join by IP Call</b>	If it is enabled, the user can join the conference by IP call.
<b>Join with browser</b>	If it is enabled, the user can join the conference by Yealink Web app.

**Related concepts**[Discussion Mode and Training Mode](#)[Entity Meeting Room and the Virtual Meeting Room](#)

## Discussion Mode and Training Mode

---

The conference modes of VMR includes the discussion mode and the training mode.

**Table 33: Discussion Mode and Training Mode**

Difference	Discussion Mode		Training Mode	
<b>Participant Role</b>	<b>Moderator</b>	You can set any participants in the enterprise directory as moderators.	<b>Moderator</b>	You can set any participants in the enterprise directory as moderators. If the broadcasting interactive feature is enabled, the moderators are the interactive parties by default.
	<b>Guest</b>	It refers to the participants who join the VMR but are not set as moderators.	<b>Lecturer</b>	Moderators can set any moderators or guests as lecturers during the conference.
			<b>Guest</b>	It refers to the participants who join the VMR but are not set as moderators. If the broadcasting interactive feature is enabled, the guests are the broadcasting parties by default.

Difference	Discussion Mode	Training Mode
<b>Feature Privilege</b>	Moderators can configure the layout during the discussion mode conferences or Meet Now conferences.	Moderators can configure the layout in the training mode conference, they can also allow/reject the participant application for speaking, make the roll call, export the roll call result, and switch the roles between lecturers and moderators/guests.
	Moderators can edit conferences and delete conferences, and during the conference, they can also send messages, call participants, call participants from the call history, invite participants, invite the third parties, invite participants by email, share the conference information, search for participants, hang up participants, move the participants into the lobby, allow/reject the participants to join the conference, mute/unmute participants, turn on/off the camera, block/unblock the voice, enable/disable RTMP Live, switch the roles between the moderators and guests, control the far-end camera, lock or unlock conferences, record the conference, pause/end the recording, view the conference recording, manage the recording files, disable the link, and end the conference.	
	Other participants can only view the conference details.	
<b>Layout</b>	Moderators and guests can view all participants. You can set the default layout, refer to <a href="#">Setting the Default Layout</a> .	<ul style="list-style-type: none"> <li>The moderators can view all participants by default. You can set the default layout, refer to <a href="#">Setting the Default Layout</a> .</li> </ul> <p>If the broadcasting interactive feature is enabled, the moderators can view all interactive parties by default.</p> <ul style="list-style-type: none"> <li>For guests, the video images of all lecturers are displayed in equal parts by default. If there is no lecturer, all guests can view the reminder of waiting for the lecturer.</li> </ul> <p>If the broadcasting interactive feature is enabled, the broadcasting parties will see that the video images of all lecturers are displayed in equal parts by default. If there are no lecturers, all broadcasting parties can view the reminder of waiting for the lecturer.</p>
<b>Speaking Rule</b>	Free speaking.	All guests and moderators are muted by default. Moderators can speak after unmuting themselves. Guests can speak only when the moderators allow their application for speaking.
<b>Contents</b>	All moderators and guests can share content by default.	Only moderators and lecturers can share content. Guests cannot share content.

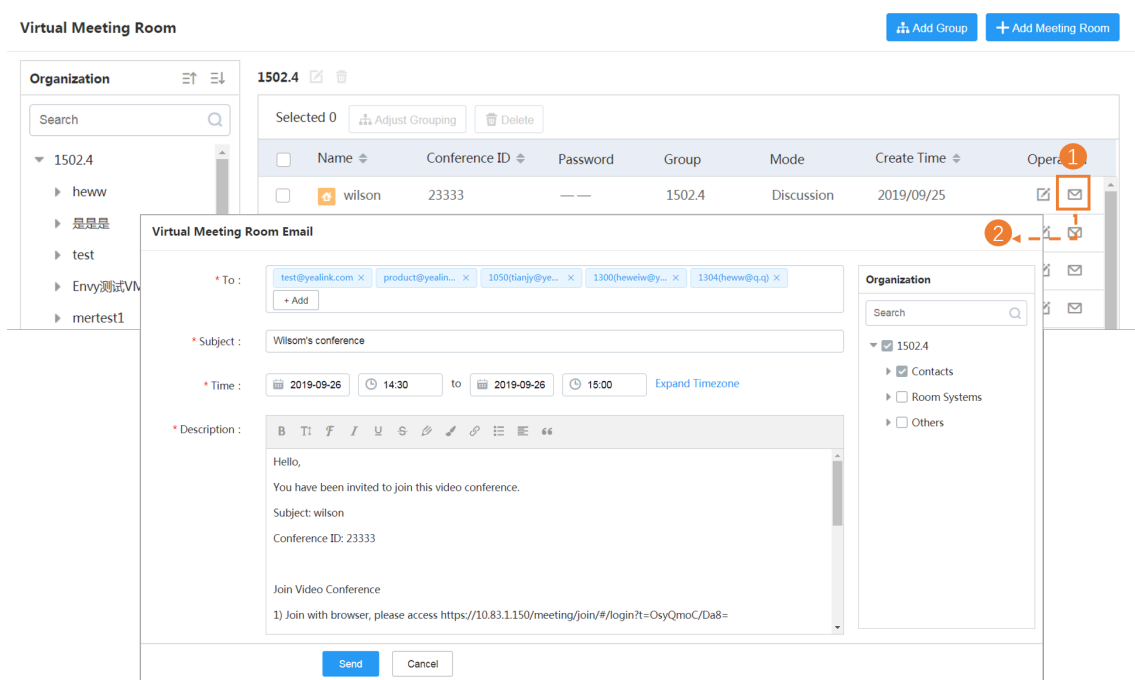
**Related tasks**[Adding a VMR](#)

## Sending Emails to VMR Participants

If you want to create a one-off conference in the VMR, you can inform the corresponding participants by email.

### Procedure

Click **Meeting Room > Virtual Meeting Room**.



**Note:** If the account you select does not associate with a mailbox, you fail to send emails to them.

## Managing Conferences

You can manage the call settings, monitor conferences, control conferences, delete conferences, and view the usage of meeting rooms. The video conferences include scheduled conferences, Meet Now conferences and VMRs.

- [Call Settings](#)
- [Controlling Conferences](#)
- [Monitoring the Conference](#)
- [Deleting Conferences](#)
- [Viewing the Usage of Meeting Rooms](#)

### Call Settings

You can set the Call Control Policy and the Video Display Policy to improve the conference experience.

- [Setting the Video and Content Resolution](#)
- [Setting the Call Bandwidth](#)
- [Configuring the Max Video Parties per Conference](#)
- [Configuring the Max Audio-Only Parties per Conference](#)
- [Setting the Time for Joining Conference Beforehand](#)

- [Enabling Auto Dialing](#)
- [Enabling Audio Redialing](#)
- [Enabling Mute Participants upon Entry](#)
- [Setting the Audio Prompt When Participants Join or Leave Conferences](#)
- [Displaying the Native Video](#)
- [Setting the Last Participant Backstop Timeout](#)
- [Setting the Auto End Conference Without Moderator](#)
- [Enabling Content Only](#)
- [Setting the Join with APP Awakened by Browser](#)
- [Enabling Receiving Ringtone Receipt](#)
- [Enabling External/Internal Network Access WebRTC Authentication](#)
- [Enabling the Roll Call](#)
- [Setting the App Push Address](#)
- [Setting the QoS](#)
- [Setting the Default Layout](#)
- [Displaying the Participant Name](#)
- [Display Participant Status](#)
- [Displaying the Participant Quantity](#)
- [Displaying the Audio-Only Participant](#)

## Setting the Video and Content Resolution

Due to the limitation of the enterprise bandwidth, you can set the maximum video resolution and the maximum content sharing resolution for a better video quality.

- **Global Setting:**

1. Click **Call Configuration > Call Control Policy**.
2. Set the content and the video resolution and save it.

Max video resolution :	720P/30FPS
Max content resolution :	4K/30FPS
Max call bandwidth : ?	1080P/60FPS
Max video parties per conference :	720P/60FPS
	<b>720P/30FPS</b>
	360P/30FPS
Max content resolution :	1080P/30FPS
Max call bandwidth : ?	<b>1080P/30FPS</b>
Max video parties per conference :	1080P/15FPS
	1080P/5FPS
	720P/30FPS
	720P/15FPS
Max audio-only parties per conference :	720P/5FPS


- **VMR:**

1. Click **Meeting Room > Virtual Meeting Room** and do one of the following:

- If you want to add a VMR, click **Add Meeting Room**.

In the **Permission setting** field, set the maximum content and video resolution, and save it.



- If you want to edit a VMR, click  .


In the **Permission setting** field, set the maximum content and video resolution, and save it.

## Setting the Call Bandwidth


According to the limitation of the enterprise bandwidth, you can limit the media bandwidth sent by the server to conference participants. For example, you set the call bandwidth as 2M. If the bandwidth used by a participant is 4M, when he joins the conference and his devices negotiate with the server, the bandwidths he receives and sends are 2M.

- **Global Setting:**

1. Click **Call Configuration > Call Control Policy**.
2. In the **Max call bandwidth** field, select the desired bandwidth, and save it.

Max call bandwidth : 	2Mbps
Max video parties per conference :	6Mbps
Max audio-only parties per conference :	5Mbps
Audio IVR language :	4Mbps
	3Mbps
	2Mbps
	1.5Mbps

- **VMR:**

1. Click **Meeting Room > Virtual Meeting Room** and do one of the following:
  - If you want to add a VMR, click **Add Meeting Room**.  
In the **Permission setting** field, select the desired bandwidth, and save it.
  - If you want to edit a VMR, click  .  
In the **Permission setting** field, select the desired bandwidth, and save it.

## Configuring the Max Video Parties per Conference


You can limit the maximum video parties for a conference to reserve video port resources for other important conferences. If the number of video parties in a conference exceeds the maximum number, users cannot place video calls to join the conference.

- **Global Setting:**

1. Click **Call Configuration > Call Control Policy**.
2. In the **Max video parties per conference** field, enter the desired number and save it.

The default value is 1500 parties.

- **VMR:**

1. Click **Meeting Room > Virtual Meeting Room** and do one of the following:
  - If you want to add a VMR, click **Add Meeting Room**.  
Set the maximum video parties and save it. The default value is 1500 parties.
  - If you want to edit a VMR, click  .  
Set the maximum video parties and save it.  
The default value is 1500 parties.

## Configuring the Max Audio-Only Parties per Conference

You can limit the maximum audio-only parties for a conference to reserve audio port resources for other important conferences. If the number of audio-only parties exceeds the maximum number, the participants cannot place an audio call to join the conference.

- **Global Setting:**

1. Click **Call Configuration > Call Control Policy**.
2. In the **Max audio-only parties per conference** field, enter the desired number and save it.

The default value is 1500 parties.


- **VMR:**

1. Click **Meeting Room > Virtual Meeting Room** and do one of the following:

- If you want to add a VMR, click **Add Meeting Room**.

Set the maximum audio parties and save it. The default value is 1500 parties.

- 

If you want to edit a VMR, click .

Set the maximum audio parties and save it. The default value is 1500 parties.

## Setting the Time for Joining Conference Beforehand

You can specify the time when users can join the scheduled conferences in advance.

### Procedure

1. Click **Call Configuration > Call Control Policy**.
2. In the **Join conference beforehand** field, enter the desired value, and save it.

The default value is 60 minutes.

## Enabling Auto Dialing

You can enable the feature of **Auto dialing**. When the scheduled conference begins, YMS will automatically place invitation calls to the invited participants.

### About this task

- The supported devices are PVT950/PVT980, VC880/VC800/VC500/VC400/VC200/VC120/VC110 video conferencing system, SIP VP-T49G and VP59 IP phone, and third-party devices.
- If you disable the feature of **Auto dialing**, it is invisible to users when they schedule conferences.

### Procedure

1. Click **Call Configuration > Call Control Policy**.
2. Enable **Auto dialing**.  
It is enabled by default.
3. In the **Device** field, select the desired device, and save it.

When scheduling conferences, if you want to invite third parties, select the check box of **Third party**.

Auto dialing : ?

ON

Device :  PVT950/980  VC880/800/500  VC400  VC200  
 VC120  VC110  T49G  VP59  Third party

**What to do next**

Schedule a video conference and enable the feature of **Auto dialing**. For more information, refer to [Yealink Meeting Server User Guide](#).

**Enabling Audio Redialing**

During a conference/VMR, you can enable this feature to redial the participant whose device is disconnected from the server and reconnected to the server.

**Note:**

- This feature is not available to the broadcasting parties.
- If you disable the feature of **Auto redialing**, it is invisible to users when they schedule conferences.

- **Global Setting:**

**Before you start**


[Enabling Auto Dialing](#) is finished.

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Auto redialing** and save it.

**What to do next**

Schedule video conferences and enable **Auto redialing**. For more information, refer to [Yealink Meeting Server User Guide](#).

- **VMR:**

1. Click **Meeting Room** > **Virtual Meeting Room** and do one of the following:
  - If you want to add a VMR, click **Add Meeting Room**.  
In the **Permission setting** field, enable **Auto redialing**, and save it.
  - If you want to edit a VMR, click .  
In the **Permission setting** field, enable **Auto redialing**, and save it.

**Enabling Mute Participants upon Entry**

If you enable the feature of **Mute Participants upon Entry**, the participant will be muted automatically once he joins the conference.



**Note:** If you disable this feature in the Global Setting, it is invisible to users when they schedule conferences.

- **Global Setting:**

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Mute Participants upon Entry** and save it.

**What to do next**


Schedule a video conference and enable **Mute Participants upon Entry**. For more information, refer to [Yealink Meeting Server User Guide](#).

- **VMR:**

1. Click **Meeting Room > Virtual Meeting Room** and do one of the following:

- If you want to add a VMR, click **Add Meeting Room**.

In the **Permission setting** field, enable **Mute Participants upon Entry**, and save it.

- If you want to edit a VMR, click  .

In the **Permission setting** field, enable **Mute Participants upon Entry**, and save it.

## Setting the Audio Prompt When Participants Join or Leave Conferences

You can set the audio prompt for different participants.



### Note:

#### For scheduled conferences or Meeting Now conferences:

- When users schedule conferences or create Meet Now conferences, if you set the audio prompt in the Global Setting as **Close**, this configuration is invisible on the Conference Control page.
- During the conference, if you change the audio prompt in the Global Setting, it affects the new scheduled conferences and created Meet Now conferences rather than the ongoing conferences.
- For more information about setting the audio prompts when you are controlling the conference, refer to [Yealink Meeting Server User Guide](#).

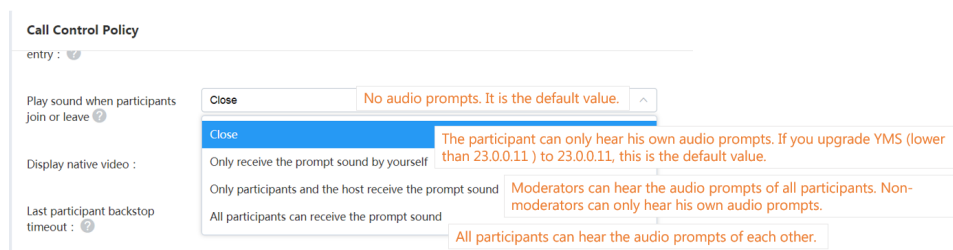
#### For VMRs:

- When adding or editing VMRs, if you set the audio prompt in the Global Setting as **Close**, this configuration is invisible on the Conference Control page.
- During the conference, if you change the audio prompt in the Global Setting, it does not affect the ongoing conferences.
- For more information about setting the audio prompts when you are controlling the conference, refer to [Controlling Conferences](#) .


- **Global Setting:**


1. Click **Call Configuration > Call Control Policy**.

2. Set the audio prompt and save it.




**Call Control Policy**

entry : 

Play sound when participants join or leave  Close No audio prompts. It is the default value.

Display native video : Close The participant can only hear his own audio prompts. If you upgrade YMS (lower than 23.0.0.11) to 23.0.0.11, this is the default value.


Last participant backstop timeout :  Only receive the prompt sound by yourself Only participants and the host receive the prompt sound All participants can receive the prompt sound Moderators can hear the audio prompts of all participants. Non-moderators can only hear his own audio prompts. All participants can hear the audio prompts of each other.

- **VMR:**

1. Click **Meeting Room > Virtual Meeting Room** and do one of the following:

- If you want to add a VMR, click **Add Meeting Room**.


In the **Permission setting** field, set the audio prompt, and save it.

- If you want to edit a VMR, click  .

In the **Permission setting** field, set the audio prompt, and save it.

## Displaying the Native Video

If you enable this feature, you can see the native video image displayed in the MCU image. If you disable it, you can only see the video images of other participants rather than yours in the MCU image.

- **Global Setting:**
  1. Click **Call Configuration > Call Control Policy**.
  2. Enable **Display native video** and save it.
- **VMR:**
  1. Click **Meeting Room > Virtual Meeting Room** and do one of the following:
    - If you want to add a VMR, click **Add Meeting Room**.  
In the **Permission setting** field, enable **Display native video**, and save it.
    - If you want to edit a VMR, click .  
In the **Permission setting** field, enable **Display native video**, and save it.

## Setting the Last Participant Backstop Timeout

You can set the length of time that a conference will continue when only one participant remains, to manage the useless conference and free up the server resource.

### Procedure

1. Click **Call Configuration > Call Control Policy**.
2. Enable **Last participant backstop timeout**.
3. Set the time and save it.

Last participant backstop timeout :   ON  (1~180)mins

## Setting the Auto End Conference Without Moderator

When there is no moderator in the Meet Now conference, you can configure the auto-timeout to end the useless conference and free up the server resource.


### Procedure


1. Click **Call Configuration > Call Control Policy**.
2. Enable **Auto end conference without moderator**.
3. Set the time and save it.

Auto end conference without moderator :   ON  (1~180)mins

## Enabling Content Only

If you want the device that does not support dual-stream protocol to receive the content, you can enable **Content only**. When the devices share content in a call, these devices can only receive the content and the audio. If you disable this feature, these devices can only receive video images.

 **Note:** This feature does not affect the audio transmission.

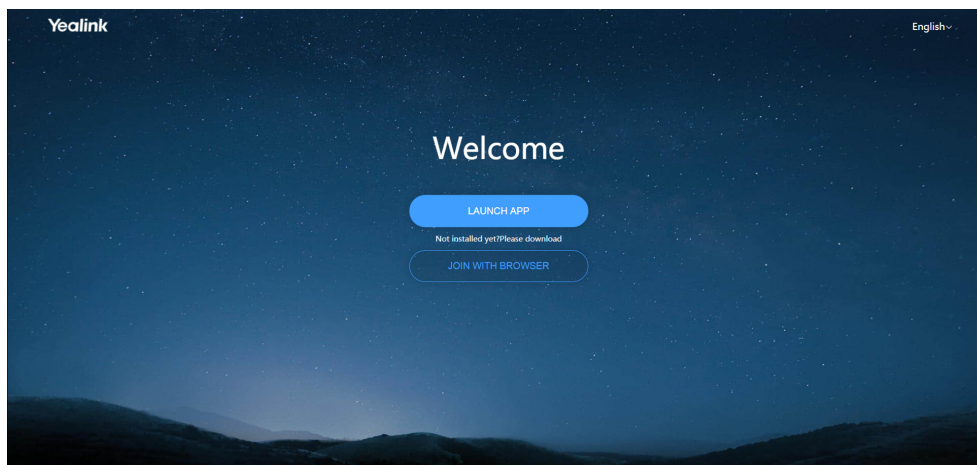
- **Global Setting:**
  1. Click **Call Configuration > Call Control Policy**.
  2. Enable **Content only** and save it.
- **VMR:**
  1. Click **Meeting Room > Virtual Meeting Room** and do one of the following:
    - If you want to add a VMR, click **Add Meeting Room**.  
In the **Permission setting** field, enable **Enabling Content Only, account and save.**, and save it.
    - If you want to edit a VMR, click  .  
In the **Permission setting** field, enable **Enabling Content Only, account and save.**, and save it.

## Setting the Join with APP Awakened by Browser

If you want to get the entrance to Yealink VC Desktop when you join the conference by browser, you can enable **Join with APP awakened by browser**.

### About this task

If this feature is enabled, the Home page of Yealink Web App is displayed as below:



### Procedure

1. Click **Call Configuration > Call Control Policy**.
2. Enable **Join with APP awakened by browser** and save it.

## Enabling Receiving Ringtone Receipt

If you want to hear the Ringback Tone from the callee when you place the call via PSTN (for example, the fixed-line), you can enable this feature.

### Procedure

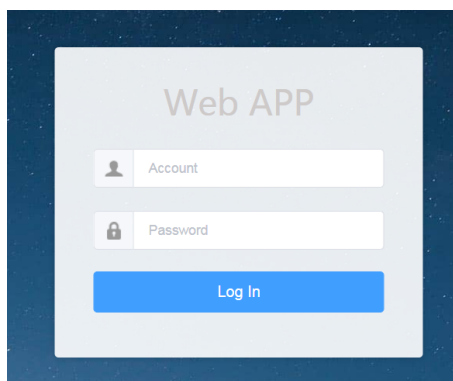
1. Click **Call Configuration > Call Control Policy**.
2. Enable **Receiving ringtone receipt** and save it.

## Enabling External/Internal Network Access WebRTC Authentication

If you enable this feature, users need YMS accounts and the passwords to join conferences via browser.

### About this task

The page is shown as below:



### Procedure

1. Click **Call Configuration > Call Control Policy**.
2. Enable **External network access WebRTC authentication/Intranet access WebRTC authentication**, and save it.

### Related information

[The Configuration of Access WebRTC Authentication Is Invalid](#)

## Enabling the Roll Call

If you enable this feature, during the roll call, the called party is unmuted by default. If other participants do not want to hear the voice of the called party who is muted at that moment, you can disable this feature.



**Note:** This feature is only applicable to the training mode conference.


- **Global Setting:**

1. Click **Call Configuration > Call Control Policy**.
2. Enable **Roll call setting** and save it.

### What to do next

When controlling conferences, the moderators can call the roll. For more information, refer to [Yealink Meeting Server User Guide](#).

- **VMR:**

1. Click **Meeting Room > Virtual Meeting Room** and do one of the following:
  - If you want to add a VMR, click **Add Meeting Room**.  
In the **Permission setting** field, enable **Roll call setting**, and save it.
  - If you want to edit a VMR, click .  
In the **Permission setting** field, enable **Roll call setting**, and save it.

### What to do next

When controlling conferences, the moderators can call the roll. For more information, refer to [Controlling Conferences](#).

## Setting the App Push Address

You can configure the iOS push address so the user can receive the incoming calls or conference notifications when Yealink VC Mobile for iOS is running in the background or exited.

### About this task

A YMS account is registered on Yealink VC Mobile for iOS.

### Procedure

1. Click **Call Configuration > Call Control Policy**.
2. In the **App push address** field, enter the address, and save it.

The default value is *https://ios.push.yealinkvc.com:8443*.

## Setting the QoS

You can set Differentiated Services Code Points (DSCP) for the audio or video packets, which can be used to adjust the traffic and modify the flow when transmitting the audio and video packets. The DSCP value should be consistent with the one set in the switch or the one set in the network topology, to ensure that the data packet is not lost during the transmission.

### Procedure

1. Click **Call Configuration > Call Control Policy**.
2. Enter the corresponding value in the **Video QoS** field.  
The default value is 34.
3. Enter the corresponding value in the **Audio QoS** field and save it.  
The default value is 63.

## Setting the Default Layout

You can set the conference default layout, and the MCU image received by the participants is subject to the default layout you set.



### Note:

#### For scheduled conferences or Meeting Now conferences:

- When users schedule conferences or create Meet Now conferences, the default layout of the Conference Control page is the same as the one you set in the Global Setting.
- During the conference, if you change the default layout in the Global Setting, it affects the new scheduled conferences and created Meet Now conferences rather than the ongoing conferences.
- For more information about setting the default layout when you are controlling the conference, refer to [Yealink Meeting Server User Guide](#) [Yealink Unified Communication User Guide](#).

#### For VMRs:

- When adding or editing VMRs, the default layout of the Conference Control page is the same as the one you set in the Global Setting.
- During the conference, if you change the default layout in the Global Setting, it does not affect the ongoing conferences.
- For more information about setting the default layout when you are controlling the conference, refer to [Controlling Conferences](#).

- **Global Setting:**

1. Click **Call Configuration > Video Control Policy**.

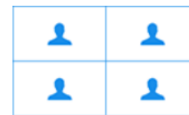


**Layout Settings**

Default layout :



onePlusN



Equal NxN

Equal NxN :

4\*4

Max number of videos displayed in equal NxN layout

When the number of videos exceed the maximum, every

seconds polling once :

Single video switches (One video switches per cycle)

Full screen switches (All videos switch per cycle)

Voice activated time :

**Table 34: Introduction of the corresponding parameters**

Parameter	Description
<b>1+N</b>	In the video layout of 1+N, if the number of current participants exceeds the maximum number of the video images per screen, the system will switch among the video images of participants automatically.
<b>Equal N×N</b>	In the video layout of Equal N×N, if the number of current participants exceeds the maximum number of the video images per screen, the system will switch among the video images of participants automatically.
<b>Voice activated speaker</b>	The system will automatically identify the speaking participant if he continues speaking during the preconfigured voice-activated time.  For 1+N, the video image of the speaking participant is enlarged to a large window, and the video images of other participants are reduced to thumbnails. For Equal N×N, his video image is circled with a yellow frame.


- **VMR:**

1. Click **Meeting Room > Virtual Meeting Room** and do one of the following:

- If you want to add a VMR, click **Add Meeting Room**.

In the **Permission setting** field, set the default layout.

- 

If you want to edit a VMR, click  .

In the **Permission setting** field, set the default layout.



## Displaying the Participant Name

To display the participant name in the MCU video image, you can enable this feature.

### About this task

- When users schedule conferences or create Meet Now conferences, if you disable this feature, this configuration is invisible to the Conference Control page, and the MCU video image will not display the participant name.
- During the conference, if you enable this feature, the Conference Control page will display the configuration.
- During the conference, if you disable this feature, this configuration is invisible to the Conference Control page, and the MCU video image will not display the participant name.
- During the conference, if you edit the display position, it affects the new scheduled conferences, created Meet Now conferences, and created VMRs rather than the ongoing conferences.

For more information about setting the participant name when you are controlling the conference, refer to [Yealink Meeting Server User Guide](#).

### Procedure

1. Click **Call Configuration > Video Display Policy**.
2. Set the parameter and save it.

#### Display Settings

Display participant name :



Location selection :

- Top left
- Top center
- Bottom left
- Bottom center

## Display Participant Status

If you want to view the status in the MCU image, for example, the participant is muted or blocked, you can enable **Display participant status**.

### About this task

- When users schedule conferences and create Meet Now conferences, if you disable this feature, this configuration is invisible to the Conference Control page, and the MCU video image will not display the participant status.
- During the conference, if you enable this feature, the Conference Control page will display the configuration.
- During the conference, if you disable this feature, this configuration is invisible to the Conference Control page, and the MCU video image will not display the participant status.

For more information about setting the participant status when you are controlling the conference, refer to [Yealink Meeting Server User Guide](#).

**Procedure**

1. Click **Call Configuration > Video Display Policy**.
2. Enable **Display participant name** and save it.

**Displaying the Participant Quantity**

If you want to view the number of participants that join the conference by audio or video, you can enable the **Display Participant Quantity**.

**Procedure**

1. Click **Call Configuration > Video Display Policy**.
2. Enable **Display participant quantity** and save it.

Display participant  
quantity :



Type :  Video  Audio

**Displaying the Audio-Only Participant**

If you want to display the video images of audio-only participants in the MCU image, you can enable **Display audio-only participants**.


**Procedure**

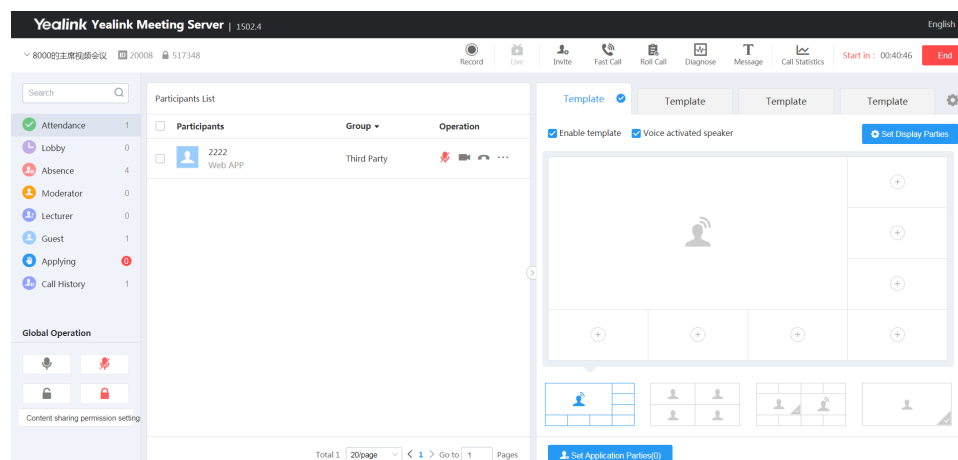
1. Click **Call Configuration > Video Display Policy**.
2. Enable **Display the audio-only participants** and save it.

**Controlling Conferences**

You can monitor the VMRs, the ongoing conference (including Meet Now conference, scheduled conferences, and VMRs), and the scheduled conference that can join in advance (refer to [Setting the Time for Joining Conference Beforehand](#)). The conference control includes configuring the conference layout, configuring messages, managing conference participants, and more.

**Procedure**

1. Click **Conference > Conference Control**.
2. Select **Ongoing, Scheduled, and VMR**.
3. On the right side of the desired conference, click  to go to the Conference Control page.
4. Do the desired operation. For more information, refer to [Yealink Meeting Server User Guide](#).



## Monitoring the Conference

You can monitor the VMRs, the ongoing conference (including Meet Now conference, scheduled conferences, and VMRs), and the scheduled conference that can join in advance (refer to [Setting the Time for Joining Conference Beforehand](#)). You can subscribe to this service from Yealink technical support engineers.


If you go to the Conference Monitoring page, you can view the video and the shared contents, listen to the participants but you are not displayed in the MCU image and included in the participant list.

- [Going to the Conference Monitoring Page](#)
- [Selecting an Audio Output Device](#)
- [Adjusting the Output Volume](#)
- [Changing the Display Language](#)
- [Configure the Video Images in Equal N×N](#)
- [Setting the Video Carousel](#)
- [Displaying a Participant in a Full Screen/Exiting the Full Screen](#)
- [Scaling the Video Image](#)
- [Hiding/Showing the Conference Video](#)
- [Switching Between the Video Window and the Content Window](#)
- [Displaying the Conference Monitoring Page in a Full Screen/Exiting the Full Screen](#)

### Going to the Conference Monitoring Page

If you want to monitor the conference, you need to go to the Conference Monitoring page first.

#### Procedure

1. Click **Conference > Conference Control**.
2. Select **Ongoing**, **Scheduled**, and **VMR**.
3. On the right side of the desired conference, click  to go to the Conference Monitoring page.

### Selecting an Audio Output Device

If you use the new audio or video device during a conference, the new device will not be enabled automatically. You need manually enable the new audio or video device.

#### Before you begin

Go to the Conference Monitoring page.

**Procedure**

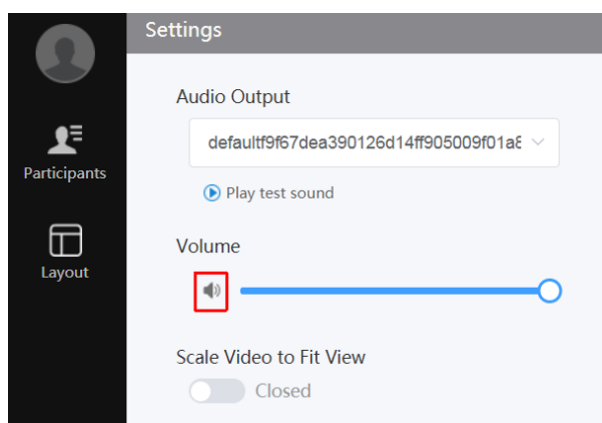
1. Click **Settings**.
2. Select the available device from the drop-down menu of the **Audio Output**.
3. Click **Play test sound**, and you can adjust the volume when the music is playing.

**Adjusting the Output Volume****Before you begin**

Go to the Conference Monitoring page.

**Procedure**

1. Click **Settings**.
2. In the **Volume** field, drag the adjuster to the desired value.  
The device volume you adjust is only applicable to the people who monitor the conference.
3. Click the icon below to mute the device.

**Changing the Display Language**

The supported languages are Simplified Chinese, Traditional Chinese, English, Russian, Polish, Spanish and Portuguese.

**Before you begin**

Go to the Conference Monitoring page.

**Procedure**

1. Click **Settings**.
2. Select the desired language from the drop-down menu of **Language Setting**.

**Configure the Video Images in Equal N×N****Before you begin**

Go to the Conference Monitoring page.

**Procedure**

1. Click **Layout**.
2. Select the desired value from the drop-down menu of **Equal N×N**.

The default value is 4x4.

3. Click **SAVE**.

## Setting the Video Carousel

If the number of participants exceeds the maximum number of video images per screen, you can enable the video carousel, and the system will switch among the video images of the participants automatically.

### Before you begin

Go to the Conference Monitoring page.

### Procedure

1. Click **Layout**.
2. Enable **Video carousel**.
3. Select **videos switch** or **Full screen switches**.
4. Click **SAVE**.


## Displaying a Participant in a Full Screen/Exiting the Full Screen

### Before you begin

Go to the Conference Monitoring page.

### Procedure

1. Click **Participants**.
2. On the right of the desired participant, click **Zoom In**.
3. Do one of the following:
  - Click **Participant's view**, and you can view the local video of this participant enlarged to a large window.
  - Click **Participant's video**, and you can view the MCU image applied to this participant enlarged to a large window.

The  appears beside the participant after you zoom the participant in.

4. If you want to toggle the full-screen mode, click **...**, and select **Switch to participant's video/Switch to participant's view**; if you want to exit the full-screen mode, click **Zoom Quit**.

## Scaling the Video Image

When you click an item such as **Settings** on the menu bar, the pop-up pane may cover some parts of the video image. Therefore, you can enable **Scale Video to Fit View** to get a better visual experience.

### Before you begin

Go to the Conference Monitoring page.

### Procedure

1. Click **Settings**.
2. Enable **Scale Video to Fit View**.

## Hiding/Showing the Conference Video

You can hide or display the conference video.


### Before you begin

Go to the Conference Monitoring page.

### About this task

By default, when participants are sharing content, the received content is displayed in a large window, and the main video window is reduced to a thumbnail in the bottom-left corner.

### Procedure

Click  in the top-right corner of the main video window or click **Remote video** in the bottom-left corner of the screen.

## Switching Between the Video Window and the Content Window

By default, when participants are sharing content, the received content is displayed in a large window, and the main video is reduced to a thumbnail in the bottom-left corner.

### Before you begin

Go to the Conference Monitoring page.

### About this task

To view the conference video more clearly, you can display the conference video in the large window.

### Procedure

Click the conference video displayed as a thumbnail.

The main video will be displayed in a large window, and the received content is displayed in a thumbnail in the bottom-left corner.

## Displaying the Conference Monitoring Page in a Full Screen/Exiting the Full Screen

You can display the Conference Monitoring page in a full screen or not.

### Before you begin

Go to the Conference Monitoring page.

### About this task

By default, the conference video is displayed in a window.

### Procedure

Do one of the following:

- Click **Full Screen/Exit Full Screen**.
- Double click the large window to toggle the full-screen mode.


## Deleting Conferences

You can delete the ongoing conference and the scheduled conference that can join in advance (refer to [Setting the Time for Joining Conference Beforehand](#)).

### About this task

If you delete an ongoing conference, the conference ends immediately.

### Procedure

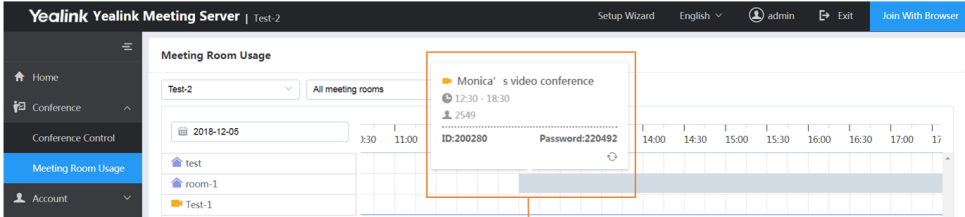
1. Click **Conference > Conference Control > Ongoing/Scheduled**.
2. On the right side of the desired conference, click .
3. If you want to delete the recurrence conference, click **Cancel occurrence/Cancel series**.
4. If you want to delete a single conference, click **OK**.

## Viewing the Usage of Meeting Rooms

You can view the details of the free entity meeting rooms and the occupied meeting rooms to know the usage of meeting rooms.

### Procedure

Click **Conference > Meeting Room Usage**.



The progress bar in gray means the conference room has been reserved and you cannot reserve it during this time. Hover your mouse over the progress bar, you can view the pop-up window, click the pop-up window and you can view the conference details.

## Managing Conference Statistics

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

- [Viewing the MCU Resource](#)
- [Viewing the Conference Statistics](#)
- [Viewing the Call History](#)

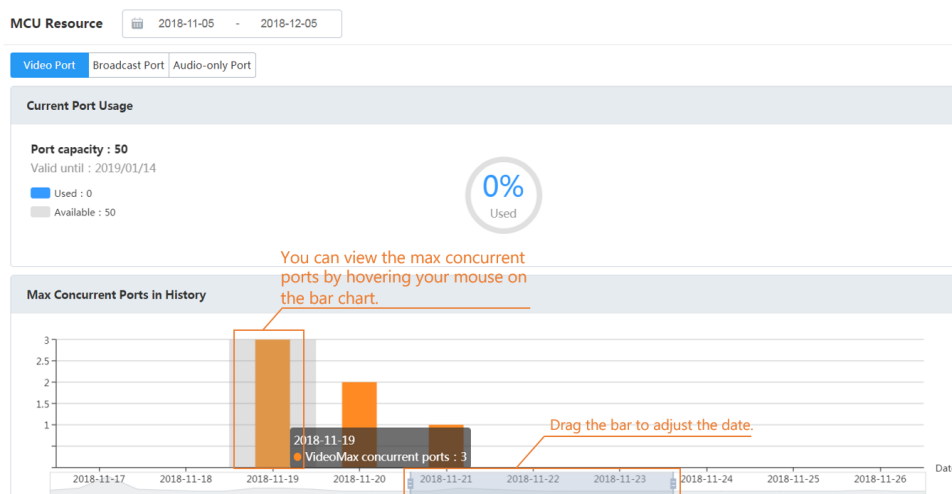


## Viewing the MCU Resource

You can view the maximum number of the concurrent ports, the usage of the video, the broadcast, and the audio-only ports.

### Procedure

Click **Statistics > MCU Resource**.

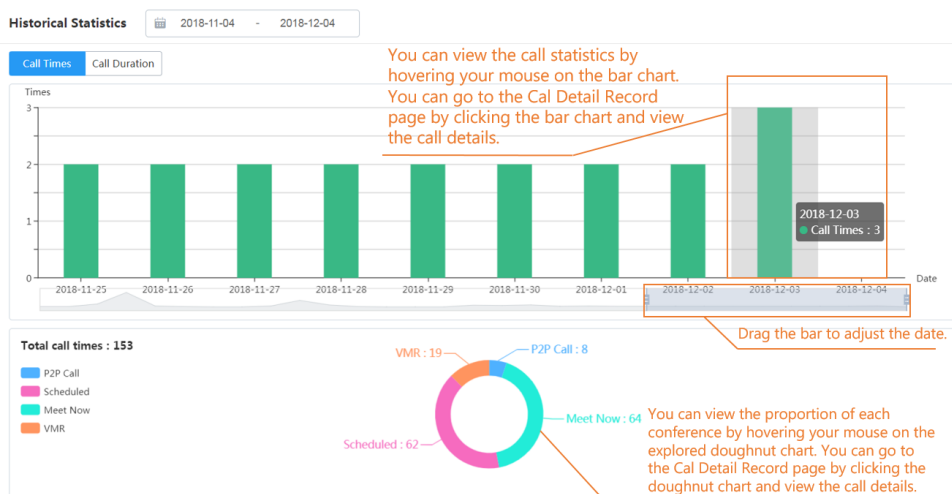


## Viewing the Conference Statistics

You can view the call duration and the times.

### Procedure

Click **Statistics > Historical Statistics**.



### Related tasks



[Viewing the Call History](#)

## Viewing the Call History

---

If you want to know the detailed information of the call or the conference, for example, the participants, you can view the call history.

### Procedure

1. Click **Statistics > CDR**.
2. Select the desired period.
3. Select **Video Conference** or **P2P**.
4. Do the following:
  - Click  on the right side of the desired conference to view the participant information.
  - Click  on the right side of the desired conference, to export the statistics to your computer to view the participant information.
  - If you want to view conferences or calls of the specified type in the specified period, click **Export** to export them to your computer.

### Related tasks

[Viewing the Conference Statistics](#)

## Managing Devices

---

You can manage YMS-registered devices on YMS, including viewing the device statistics, viewing the device details, adding groups for devices, adding/editing/pushing/deleting/exporting configuration, adding/editing/pushing/deleting/downloading configuration, rebooting devices, resetting devices to factory settings, capturing packets, exporting logs, managing T49 devices and so on.

You need to contact Yealink technical support engineers to enable these features except for managing the T49 devices.

- [Prerequisites for the Devices Automatically Connected to YMS](#)
- [Device Status](#)
- [Managing Devices by Groups \(Optional\)](#)
- [Pushing the Configuration](#)
- [Pushing Firmware](#)
- [Diagnosing Devices](#)
- [Managing T49 Devices](#)

## Prerequisites for the Devices Automatically Connected to YMS

---

YMS-registered devices can automatically be connected to the YMS device management platform. However, they should meet the prerequisites.

**Table 35: Prerequisites for the Devices Automatically Connected to YMS**

Prerequisites	
<b>YMS Version</b>	23.0.0.11 or later.  For YMS 1.X version, you need to upgrade it to YMS 2.X version first and then upgrade YMS 2.X to version 23.0.0.11.

Prerequisites	
Supported Device and Its Version	PVT980/PVT950: 1345.32.0.40 or later
	VC880/VC800/VC500: 63.32.0.40 or later
	VC200: 80.32.0.40 or later
	VP59: 91.332.0.19 or later

## Device Status

You can familiarize yourself with the following status when YMS-registered devices are connected to YMS.

- **Offline:** the device is disconnected from YMS. The reason might be the device being powered off, or being disconnected from the network, or others.
- **Registered:** the device is connected to YMS, and a YMS Account is registered on the device.
- **Unregistered:** the device is connected to YMS, but the YMS account is signed out.



**Note:** YMS will refresh the device status every 5 minutes.

## Managing Devices by Groups (Optional)

If you are used to managing the devices by groups, you can create groups.

### Procedure

1. Click **Device management** > **Group management**.
2. Add a group.

Add Group ×

\* Group name

Group Description

Save
Cancel

3. Go to the **Device management** page.

**Device management**

Firmware version/Account/Account name

Selected 9    Up: You can select the devices by setting the filter, such as the model or the group.

<input checked="" type="checkbox"/>	MAC地址	Model	Firmware version	Group	Device status	Account	IP	Operation
<input checked="" type="checkbox"/>	001565c06d62	VC800	63.4				10.81.47.51	
<input checked="" type="checkbox"/>	805ec060344e	VC800	63.4				10.81.41.8	
<input checked="" type="checkbox"/>	805ec0007b6d	VC800	63.4	* Select group			10.81.40.15	
<input checked="" type="checkbox"/>	805ec0602b23	VC800	63.4				10.81.32.27	
<input checked="" type="checkbox"/>	001565c06da8	VC800	63.4				10.81.6.68	

**Edit groups** ×

\* Select group

## Pushing the Configuration

### About this task

Before pushing the configuration, you need to know the device status first (*Device Status*):

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

### Procedure

1. Click **Device management** > **Configuration management**.
2. Add the configuration.

**Add Configuration**

\* Configuration name :

Description :

Note: You can set the parameters of the template by editing CFG text. Please follow the format "key=value" to edit, one line for each parameter. As follows:  
 static.lang.gui = Chinese\_5  
 features.hotline\_delay=8

3. Do one of the following:

- On the page of **Configuration management**, click **Push configurations** on the right side of the added configuration to go to the page of **Push configurations**.

**Push configurations** [Cancel](#)

Execution time:  
 Immediately  Timing 2019-08-26 20:22:44

Please select the device for pushing:  
 All devices  Customize device

You can select the devices by setting the filter, such as the model or the group.

<input checked="" type="checkbox"/>	MAC address	Model	Firmware version	Group	Device status	Account
<input checked="" type="checkbox"/>	001565c06d62	VC800	63.41.0.1	---	Registered	1303
<input checked="" type="checkbox"/>	805ec060344e	VC800	63.41.254.14	---	Unregistered	8551
<input checked="" type="checkbox"/>	805ec0007b6d	VC800	63.41.254.268	---	Offline	1051
<input checked="" type="checkbox"/>	805ec0602b23	VC800	63.41.251.167	---	Offline	2005
<input checked="" type="checkbox"/>	001565c06da8	VC800	63.41.254.81	---	Offline	2888
<input checked="" type="checkbox"/>	805ec0603c3f	VC800	63.40.0.35	---	Offline	8748
<input checked="" type="checkbox"/>	001565f2d11e	VC800	63.40.0.35	---	Offline	1305
<input checked="" type="checkbox"/>	805ec006d17b	VC800	63.40.0.35	---	Offline	8748

- Go to the **Device management** page.

**Device management**

Firmware version/Account/Account name

Selected 9    You can select the devices by setting the filter, such as the model or the group.

<input checked="" type="checkbox"/>	MAC地址	Model	Firmware version	Group	Device status	Account	IP	Operation
<input checked="" type="checkbox"/>	001565c06d62	VC800					10.81.47.51	<input type="button" value="⋮"/>
<input checked="" type="checkbox"/>	805ec060344e	VC800					10.81.41.8	<input type="button" value="⋮"/>
<input checked="" type="checkbox"/>	805ec0007b6d	VC800					10.81.40.15	<input type="button" value="⋮"/>
<input checked="" type="checkbox"/>	805ec0602b23	VC800					10.81.32.27	<input type="button" value="⋮"/>
<input checked="" type="checkbox"/>	001565c06da8	VC800					10.81.6.68	<input type="button" value="⋮"/>

**Update configuration file**

\* Configuration file:

## Pushing Firmware

You can push a firmware to upgrade an old firmware or downgrade a new firmware.

### About this task

Before pushing the firmware, you need to know the device status first (*Device Status*):

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


### Procedure

- Click **Device management** > **Firmware management**.
- Add the firmware.

**Add firmware**

\* Select file : Reupload

Rom file only, no more than 500 MB

 VP59-91.332.0.5.rom ✓

Firmware name :

Version :

Supported model :

Description :

Save Cancel

**3. Do one of the following:**

- On the page of **Firmware management**, click **Push firmware** on the right side of the added firmware to go to the page of **Push firmware**.

**Push firmware** [Cancel](#)

Attention: If the device is connected with any accessory and the accessory's firmware is not latest version, it will also be upgraded.

Execution time:

Immediately  Timing

Please the device for pushing:

All corresponding models  Customize device You can select the devices by setting the filter, such as the model or the group.

<input type="checkbox"/>	MAC address ⇅	Model ▾	Firmware version ⇅	Group ▾	Device status ▾	Account ⇅
<input type="checkbox"/>	001565abac59	VP59	91.332.125.3	---	Registered	2006
<input type="checkbox"/>	805ec0378bd5	VP59	91.332.0.5	---	Unregistered	3333
<input type="checkbox"/>	001565918530	VP59	91.332.0.10	---	Offline	2010
<input type="checkbox"/>	805ec03bc281	VP59	91.332.0.10	---	Offline	---
<input type="checkbox"/>	805ec03bb755	VP59	91.332.125.201	---	Offline	---
<input type="checkbox"/>	001565262635	VP59	91.332.125.252	---	Offline	2224
<input type="checkbox"/>	805ec0378ba7	VP59	91.332.0.10	---	Offline	7002
<input type="checkbox"/>	805ec0378bd7	VP59	91.332.0.10	---	Offline	---

OK Cancel

- Go to the **Device management** page.

**Device management**

Firmware version/Account/Account name

Selected 9

You can select the devices by setting the filter, such as the model or the group.

MAC地址	Model	Firmware version	Group	Device status	Account	IP	Operation
<input checked="" type="checkbox"/>	001565c06d62	VC800	63.41.0.1			1.47.51	<input type="button" value="⋮"/>
<input checked="" type="checkbox"/>	805ec060344e	VC800	63.41.254			1.41.8	<input type="button" value="⋮"/>
<input checked="" type="checkbox"/>	805ec0007b6d	VC800	63.41.254			1.40.15	<input type="button" value="⋮"/>
<input checked="" type="checkbox"/>	805ec0602b23	VC800	63.41.254			1.32.27	<input type="button" value="⋮"/>
<input checked="" type="checkbox"/>	001565c06da8	VC800	63.41.254			1.6.68	<input type="button" value="⋮"/>

**Update firmware**


\* Please select the firmware of VP59

Attention: If the device is connected with any accessory and the accessory's firmware is not latest version, it will also be upgraded.

## Diagnosing Devices

When problems occur to the devices, you can diagnose the device via YMS.

### Procedure

1. Click **Device management** > .
2. In the **Diagnosis tool** field, select the desired method, and click **OK**.

**Device details**

MAC address : 001565f4ce42      Firmware version : 63.41.254.79      Device model : VC500  
 Device status : Registered      Device account : 2555      Group : [?] --  
 IP : 10.81.6.72      Subnet Mask : 255.255.254.0      WIFI status : Close  
 IPv6 : Close      Bluetooth status : Close      VPN status : Close  
 Camera status : Enable      Most recent reporting time : 2019/08/26 18:18

**Diagnosis tool**

File Name	Size (Mb)	Modification time	Operation
Packet_001565f4ce42_20190826202501.pcap	0.13	2019/08/26 20:28	<input type="button" value="⬇"/> <input type="button" value="🗑"/>

\*The reported configuration includes: Wi-Fi, language, basic settings, and so on.

## Managing T49 Devices

You can upgrade the firmware, enable the device log, or export the device log.

- **Pushing Firmware**
  1. Click **Device management** > **Old device management** > **Device Upgrade**.
  2. Click **Add** to add firmware.

### Add Device Firmware

Select a file : [Reupload](#)

Only .rom format file is available

T49-51.25.0.30.rom ✔

Accessory firmware :

Please select the accessory firmware with the upgrade

[Save](#)

[Cancel](#)

3. Select the **Enable** check box and enable **Up to Date**.

Device Upgrade Device Log

Enable  [+ Add](#)

Selected 0 [Delete](#)

You can also click to update the firmware immediately.

File Name	Version	Model	Upload Time	Up to Date	Operation
<input type="checkbox"/> T49-51.25.0.25.rom	51.25.0.25	T49G	2019/08/12 16:12	<input type="checkbox"/>	
<input type="checkbox"/> T49-51.25.0.30.rom	51.25.0.30	T49G	2019/07/30 15:43	<input checked="" type="checkbox"/>	
<input type="checkbox"/> VP59-91.41.1.10.rom	91.41.1.10	VP59	2019/08/15 17:28	<input type="checkbox"/>	

Select all pages Total 3 10/page < 1 > Go to 1 Pages

**Results:** YMS will push the newest version to the device if the version of the device firmware is lower than the new one.

- **Enabling the Device Log**

After you enable the device log, the device will upload the log automatically.

1. Click **Device management > Old device management > Device Log**.
2. Select the **Enable** check box.

Device Upgrade Device Log

Enabled  Export log time: 2019-08-26 20:00 - 2019-08-26 21:00

Name	Account	Device Model	IP Address	Online/Offline	Operation
No data					

Total 0 10/page < > Go to 1 Pages

- **Exporting the Device Log**

1. Click **Device management > Old device management > Device Log**.
2. Select the time and click .

**Note:**

- Only the logs in the past 7 days will be saved and can be exported. Besides, you cannot select the start date and the end date across two different months.
- If the page prompts the file does not exist, it means that there is no device log during the time.



## Integrating YMS with Other Servers

---

- [Communicating with the PSTN](#)
- [Communicating with Skype for Business Server](#)
- [Communicating with Another YMS or Third-Party PBX \(Peer Trunk\)](#)
- [Communicating with Another YMS or Third-Party PBX \(Registration Trunk\)](#)
- [Setting Alibaba Cloud RTMP Live](#)
- [Enabling Conference Recording \(Third-Party Recording Server\)](#)

### Communicating with the PSTN

---

To communicate with the device in PSTN, for example, the mobile phone or the fixed-line, [Setting the PSTN Gateway Service](#) and [Adding a Call Routing Rule](#) need to be done. After the configuration, YMS users can call the phone number/fixed-line, invite them to join the conference. On the contrary, users can use their mobile phone or IP phone to go to the YMS IVR.

For more information about the configuration on YMS and third-party PSTN, refer to [Yealink SIP Trunk Deployment Guide](#).

- [Setting the PSTN Gateway Service](#)
- [PSTN Example](#)

#### Related concepts

[Common Regular Expressions and Replacement Strings](#)

### Setting the PSTN Gateway Service

#### Procedure

1. Click **Service > SIP Service > PSTN Gateway Service**.
2. Add a PSTN gateway service.
3. Configure the basic parameters.

Enabled :

\* Name :

\* Node :

\* Network :  Set these parameters of YMS on the PSTN gateway you want to connect to.

\* Port :  (Range : 1~65535)

\* Gateway address :  Set the parameters of the PSTN gateway you want to connect to.

\* Gateway port :  (Range : 1~65535)

\* Transport protocol :

4. Optional: Configure the security policy.

For adding a security group, see [Adding a Security Group](#)

**Enable security policy**  ON

Mode :  Whitelist  Blacklist

Security Group

Please select the security group

test

+ Add + Add Security Group

Allow the IP address in this group to call into.

Refuse the IP address in this group to call into.

5. Configure the outgoing call rule.

**Outgoing call rule**

Priority :	Callee regex match :	Callee regex replace string :
1	^(d{11})@	\$1@10.1.10.121
+ Add		

Matches 11-digit number. SIP account 3802 can call 13250789940 via PSTN gateway 10.1.10.121.

6. Configure the incoming call rule.

**Incoming call rule**

Priority :	Callee regex match :	Callee regex replace string :
1	+@	main_ivr@wc.cc
+ Add		

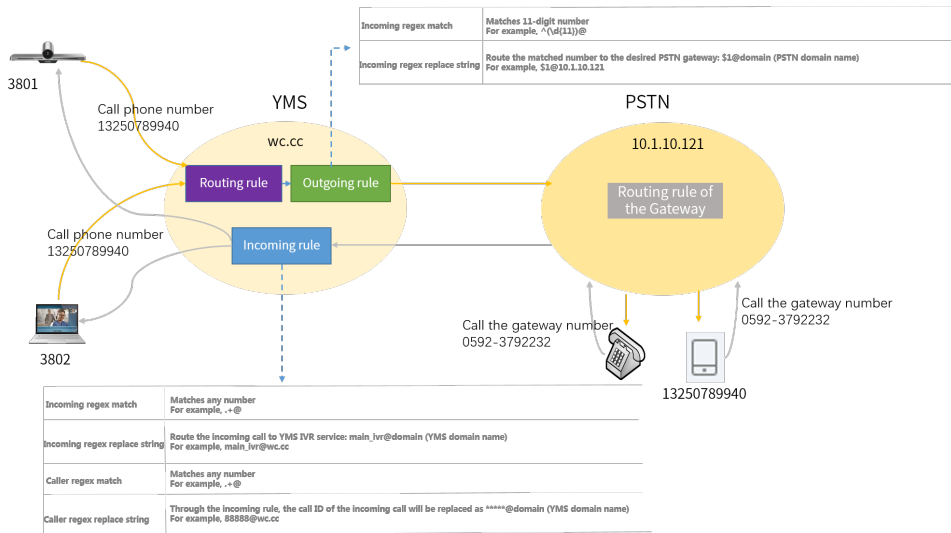
Mobile phone user 13250789940 can dial the PSTN number 0592-3792232 to go to YMS conference lobby whose domain name is wc.cc.

Priority :	Caller regex match :	Caller regex replace string :
1	+@	88888@wc.cc
+ Add		

Make the caller ID as 88888 rather than the mobile phone number.

7. Save the configuration.

**PSTN Example**



• **Situation**

- YMS users call PSTN users, for example, SIP account 3802 dials 13250789940 to call PSTN user.

- PSTN users call YMS users, for example, PSTN user 13250789940 dials 0592-3792232 to go to the conference lobby of YMS (SIP trunk IVR). You can make the caller ID as 88888 rather than the mobile phone number.
- **The configurations are as below:**
  - Enable the PSTN gateway service on server wc.cc
  - Set the outgoing call rule, the incoming call rule, and the call routing on server wc.cc

**Outgoing call rule**

Priority :  Callee regex match :  Callee regex replace string :  ✕

**Incoming call rule**

Priority :  Callee regex match :  Callee regex replace string :  ✕

Priority :  Caller regex match :  Caller regex replace string :  ✕

**Call Routing**

Search

Selected 0


<input type="checkbox"/>	Name ↕	Priority ↕	Destination match	Call Target/Out Location	Enabled	Operation
<input type="checkbox"/>	对等trunk	1	^555(d+)*@	Peer Trunk / 对等Trunk	<input type="radio"/>	<input type="button" value="✕"/>
<input type="checkbox"/>	rr	1	^030	Register Trunk / e	<input checked="" type="radio"/>	<input type="button" value="✕"/>
<input type="checkbox"/>	dd	1	^10086	H.323 GW / 150	<input type="radio"/>	<input type="button" value="✕"/>
<input type="checkbox"/>	PSTN	1	^(d{11})@	PSTN / PSTN	<input checked="" type="radio"/>	<input type="button" value="✕"/>
<input type="checkbox"/>	IP call 2	2	^conf	IP Call / IP直播	<input type="radio"/>	<input type="button" value="✕"/>
<input type="checkbox"/>	zhibo	3	^10086	IP Call / IP直播	<input type="radio"/>	<input type="button" value="✕"/>

Select all pages Total 6 page < 1 > Go to  Pages

- Configure the PSTN gateway. You can contact your service provider for details.

## Communicating with Skype for Business Server

YMS can communicate with the local Skype for Business (SfB) server, Microsoft Office 365, and SfB servers of other enterprises.

 **Note:** SfB 2016 and 2015 are supported by YMS.

For more information about the configuration and the usage of YMS and Skype for Business server, refer to [Yealink Meeting Server and Skype for Business Deployment Guide](#).

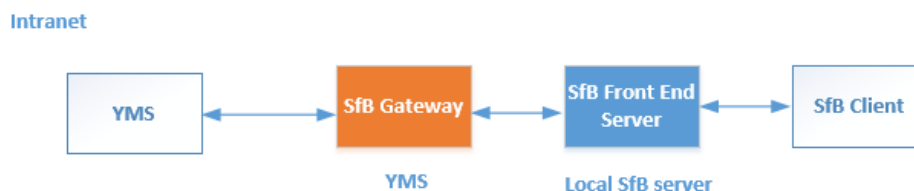
- [Communicating with the Local SfB Server](#)
- [Communicating with Microsoft Office 365](#)

- [Communicating with Other Enterprise SfB Servers](#)
- [Setting the SFB Gateway](#)
- [Setting the Sfb Gateway Media Service](#)

## Communicating with the Local SfB Server

To make the YMS and SfB in the intranet communicate with each other and the user in the intranet use both of them, you can deploy YMS to communicate with the SfB.

To communicate with the local SfB server, you need to do the following steps: [Setting the Local SfB Server](#) , [Importing the TLS Certificate](#) , [Setting the SFB Gateway](#) , [Setting the SfB Gateway Media Service](#) , and [Adding a Call Routing Rule](#) .



- [Setting the Local SfB Server](#)

### Setting the Local SfB Server

If you need your YMS to communicate with the local SfB server, you can follow the steps below to add YMS to the SfB server topology in the SfB front-end server.

#### About this task

Take the local environment as an example, you need to run the example command below to complete the configuration:

- If you use YMS cluster version and you plan to use the business node in YMS to connect to SfB, the FQDN of this node is *sfbl.5060.space* and the A record of this business node is added to the DNS server.
- The FQDN of the SfB Front-End Pool is *xiamenpool.xiamen.yealinksfb.com*, and the A record of this SfB pool is added to the DNS server.

#### Procedure

Run the command below to add YMS to the Front-End Pool generated by SfB server via powershell:

Note that only the accounts in the Front-End Pool can communicate with YMS.

For more information about the command, refer to <https://docs.microsoft.com/en-us/powershell/module/skype/?view=skype-ps>.

**Table 36:**

Procedure	Command	Syntax description
1. Get the Site ID of SfB Front-End Pool.	Get-CsSite	None

Procedure	Command	Syntax description
<p>2. Add YMS into the trusted application pool created by the SfB server.</p>	<pre>New-CsTrustedApplicationPool -Identity &lt;YMS DNS FQDN &gt; -ComputerFqdn &lt; YMS DNS FQDN &gt; -Registrar &lt;Front End Pool DNS FQDN&gt; -Site &lt; Site ID&gt; - RequiresReplication \$false -ThrottleAsServer \$true -TreatAsAuthenticated \$true</pre> <p><b>Example command:</b></p> <pre>New-CsTrustedApplicationPool -Identity sfb1.5060.space -ComputerFqdn sfb1.5060.space</pre> <pre>-Registrar xiamenpool.xiamen.yealinksfb.com -Site 5 -RequiresReplication \$false - ThrottleAsServer \$true -TreatAsAuthenticated \$true</pre>	<p><b>Syntax explanation:</b></p> <p><b>-Identity:</b> defines the DNS FQDN of the YMS group that belongs to the trusted application pool.</p> <p><b>-ComputerFqdn:</b> defines the DNS FQDN of the YMS which communicates with the SfB in the trusted application pool.</p> <p>The name of the trusted application pool should be consistent with the name of YMS, because when integrating SfB with YMS, there is only one YMS.</p> <p><b>-Registrar:</b> defines the DNS FQDN of the SfB Front-End Pool to which this trusted application pool belongs.</p> <p><b>-Site:</b> defines the SfB Site ID to which this trusted application pool belongs. Run command <b>Get-CsSite</b> to get the Site ID.</p> <p>Others are the same as the default value.</p> <p><b>Note:</b> When creating a trusted application pool (and a trusted application computer in the next step) in this way, SfB/Lync will issue a warning state: <b>"WARNING: Machine sfb1.5060.space from the topology you are publishing was not found in Active Directory and will result in errors during Enable-CsTopology as it tries to prepare Active Directory entries for the topology machines."</b> This warning can be safely ignored as YMS is non-domain-joined, and you should answer Yes to this warning.</p>

Procedure	Command	Syntax description
<p>3. Add other trusted applications to the trusted application pool.</p>	<p>New-CsTrustedApplication -ApplicationId &lt;Application ID&gt; -TrustedApplicationPoolFqdn &lt;YMS DNS FQDN&gt; -Port &lt;Available Port&gt;</p> <p><b>Example command:</b></p> <p>New-CsTrustedApplication -ApplicationId sfb1 -TrustedApplicationPoolFqdn sfb1.5060.space.space -Port 5067</p>	<p><b>Syntax explanation:</b></p> <p>-ApplicationId: defines a friendly identifier for the YMS devices. You can customize the name and it is unique.</p> <p>-TrustedApplicationPoolFqdn: defines the trusted application pool to which this YMS belongs.</p> <p>-Port: defines the source port on YMS that communicates with Sfb server. It can be any unoccupied port from 0 to 65535. The default port is 5067 in YMS, and we recommend that the Port you configure is consistent with the port in YMS.</p>
<p>4. View the trusted application to ensure that YMS is added to the trusted application pool.</p>	<p>Get-CsTrustedApplication</p>	<p>None</p>
<p>5. View information about whether or not there is the registrar to which you want to add static routing configuration. If there is no existing Identity that matches the desired registrar, run the next command.</p>	<p>Get-CsStaticRoutingConfiguration</p>	<p>None</p>
<p>6. Create a new static routing configuration for the desired registrar.</p>	<p>New-CsStaticRoutingConfiguration -Identity "Service:Registrar: &lt;Front End Pool DNS FQDN&gt;"</p> <p><b>Example command:</b></p> <p>New-CsStaticRoutingConfiguration -Identity "Service:Registrar:xiamenpool.xiamen.yealinksfb.com"</p>	<p><b>Syntax explanation:</b></p> <p>-Identity: defines the registrar to which we want to apply the static route object.</p>

Procedure	Command	Syntax description
7. Create the static SIP domain route, and associate this route with a trusted application.	<pre>\$newroute = New-CsStaticRoute -TLSSRoute - <b>Destination</b>&lt;YMS DNS FQDN&gt; -<b>Port</b> &lt;YMS Port&gt; -<b>MatchUri</b> &lt; YMS DNS FQDN&gt; - <b>UseDefaultCertificate</b> \$true</pre> <p><b>Example command:</b></p> <pre>\$newroute = New-CsStaticRoute -TLSSRoute -<b>Destination</b> "sfb1.5060.space" -<b>Port</b> 5067 -<b>MatchUri</b> "sfb1.5060.space" - <b>UseDefaultCertificate</b> \$true</pre>	<p><b>Syntax explanation:</b></p> <p><b>-Destination:</b> defines the YMS DNS FQDN where SfB should send SIP requests matching the domain specified in <b>-MatchUri</b>.</p> <p><b>-Port:</b> defines the source port on YMS that communicates with SfB server. It can be any unoccupied port from 0 to 65535. The default port is 5067 in YMS, and we recommend that the Port you configure is consistent with the port in YMS.</p> <p><b>-MatchUri:</b> defines the matched YMS DNS FQDN.</p>
8. Apply your required static route to your registrars' static routing configuration.	<pre>Set-CsStaticRoutingConfiguration -<b>Identity</b> "Service:Registrar: &lt;Front End Pool DNS FQDN&gt;" -Route @{Add=\$newroute}</pre> <p><b>Example command:</b></p> <pre>Set-CsStaticRoutingConfiguration -<b>Identity</b> "Service:Registrar:xiamenpool.xiamen.yealink.sfb.com" - -Route @{Add=\$newroute}</pre>	<p><b>Syntax explanation:</b></p> <p><b>-Identity:</b> defines the registrar to which we want to apply the static route object.</p> <p>Others are the same as the default value.</p>
9. View all routes in your static routing configuration to ensure that your required static route is added successfully.	<pre>Get-CsStaticRoutingConfiguration   Select-Object -ExpandProperty Route</pre>	None
10. Enable the new topology.	<pre>Enable-CsTopology</pre>	None

## Communicating with Microsoft Office 365

To communicate with Microsoft Office 365, you need to do the following: [Setting Microsoft Office 365](#) , [Importing the TLS Certificate](#) , [Setting the SFB Gateway](#) , [Setting the Sfb Gateway Media Service](#) , and [Adding a Call Routing Rule](#) .

Note that you need to enable the federation on Microsoft Office 365.

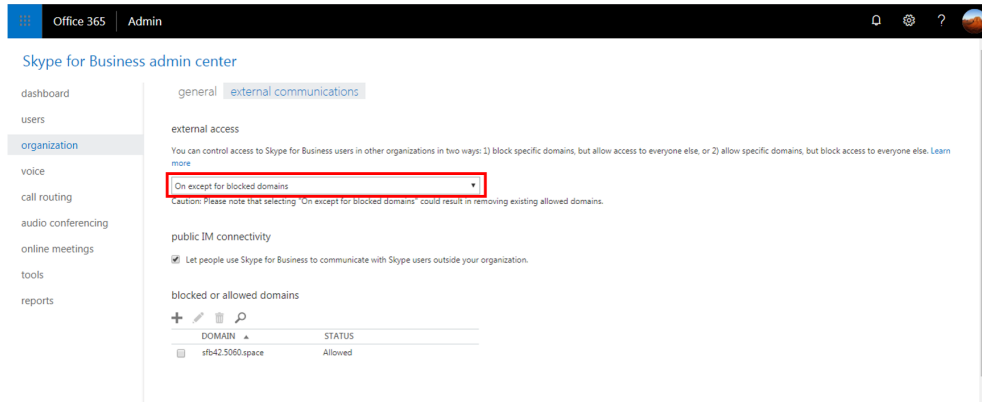
- [Setting Microsoft Office 365](#)

### Setting Microsoft Office 365

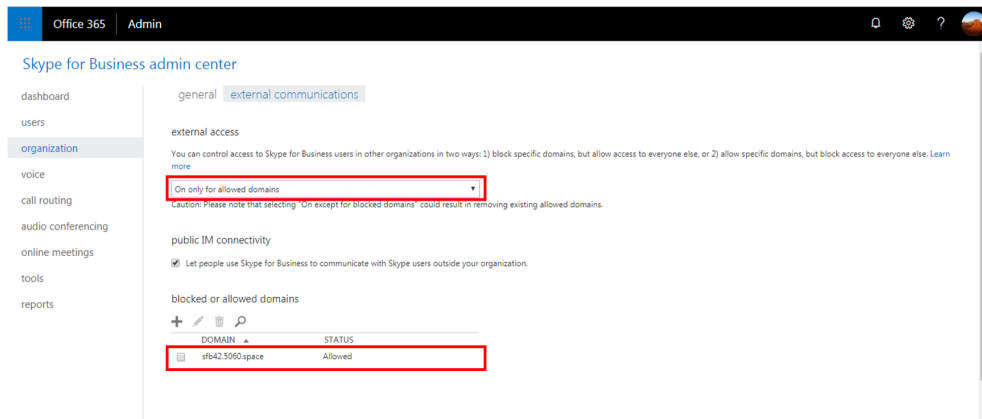
#### Procedure

1. Make sure that the SRV record and the A record of YMS and SfB are configured on the public DNS server.

2. If you add a domain name in Office 365, and use the suffix of the added domain name to build a federation with YMS, you need to add CNAME record and SRV record to the DNS server which the added domain belongs to.
3. If you use the suffix onmicrosoft.com of Office 365 or use the suffix of the added domain name to build a federation with YMS, you can do one of the following to check whether the external access is allowed:
  - If you use the legacy portal of Office 365 and want to create the federation between Office365 and all the external YMSs, you need to select **On except for blocked domains** in the **External access** field on Office 365.

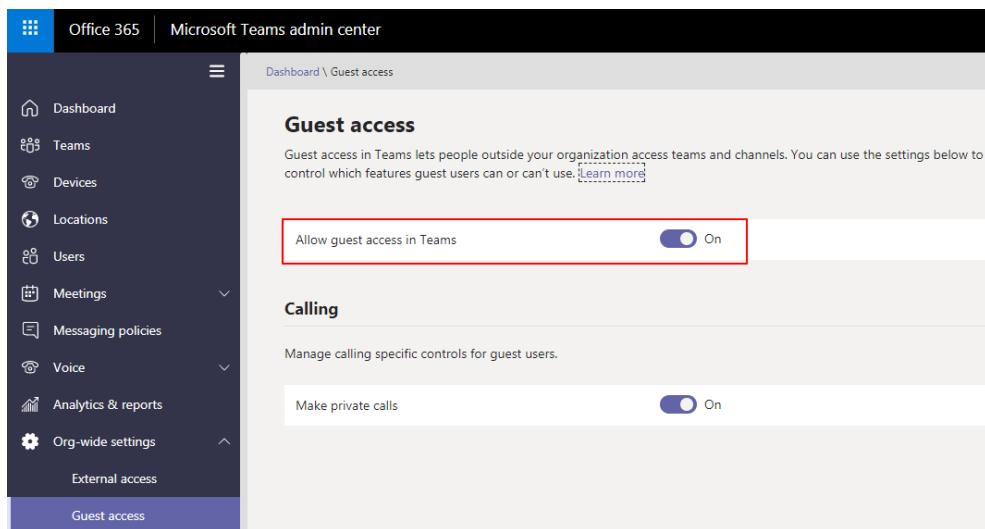
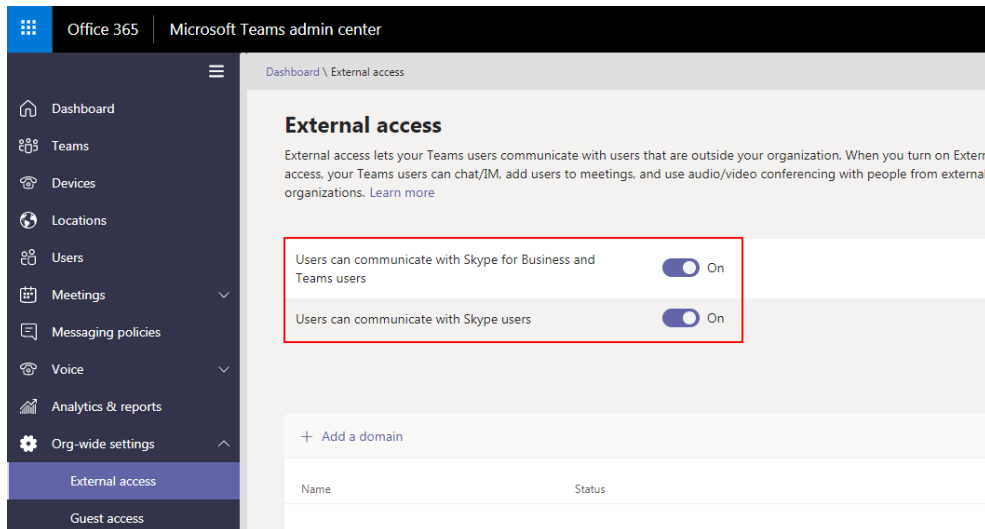


- If you use the legacy portal of Office 365 and want to create the federation between Office 365 and one YMS, you need to select **On only for allowed domains** in the **External access** field on Office 365. Besides, the DNS FQDN of YMS is added to the allowed domain.

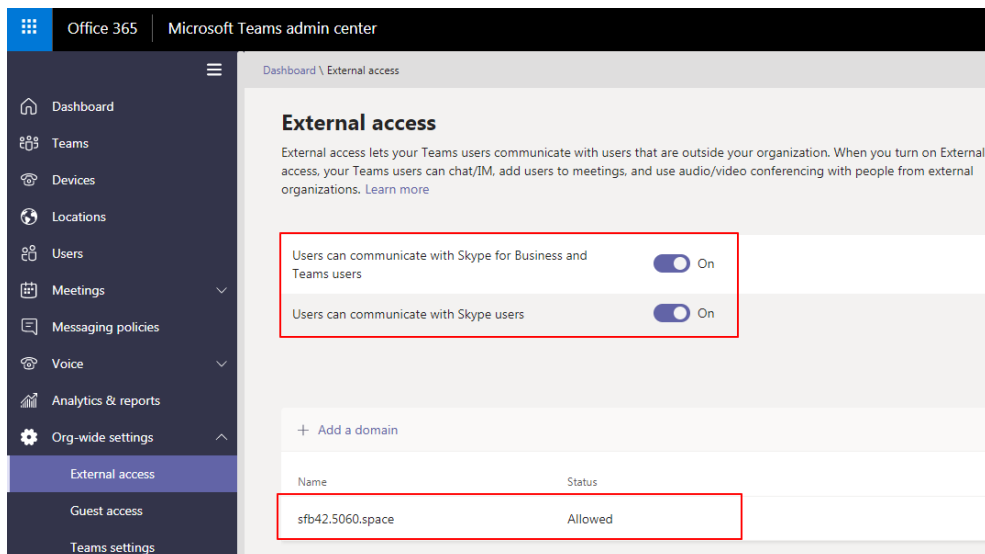


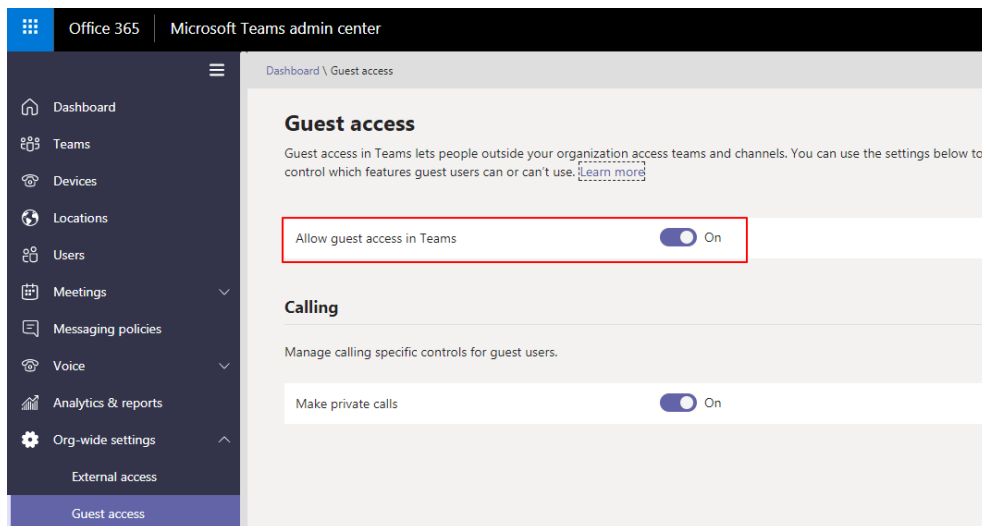
- If you use the new Office 365 and want to build the federation between Office 365 and all the external YMSs, you should turn on the switches displayed as below:





- If you use the new Office 365 and want to build the federation between Office 365 and one YMS, you should turn on the switches displayed as below, and make sure that the DNSFQDN of YMS is added to the allowed domain.



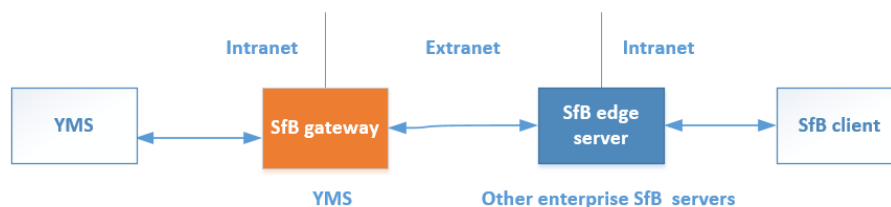


## Communicating with Other Enterprise SfB Servers

If the YMS device needs to communicate with the SfB device via the public network, you can configure the YMS to communicate with other enterprise SfB servers.

To communicate with the other enterprise SfB servers, you need to do the following: [Configuring Other Enterprise SfB Servers](#) , [Importing the TLS Certificate](#) , [Setting the SfB Gateway](#) , [Setting the SfB Gateway Media Service](#) , and [Adding a Call Routing Rule](#) .

YMS communicates with the edge servers of other enterprise SfBs via the SfB gateway. Note that edge servers of other enterprise SfBs should enable the federation.



- [Configuring Other Enterprise SfB Servers](#)

### Configuring Other Enterprise SfB Servers

#### Procedure

1. Make sure that other enterprise SfB servers have edge servers, and the IP address of the public network is configured on these edge servers or the IP addresses of these edge server are mapped to the public network by NAT. Do one of the following:
  - Verify the public DNS FQDN of the SfB edge server on the Command Prompt, for example, ping sip.yealinksfb.com. If the verification fails, you need to check the DNS A record of the SfB edge server.

```

Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping sip.yealinksfb.com

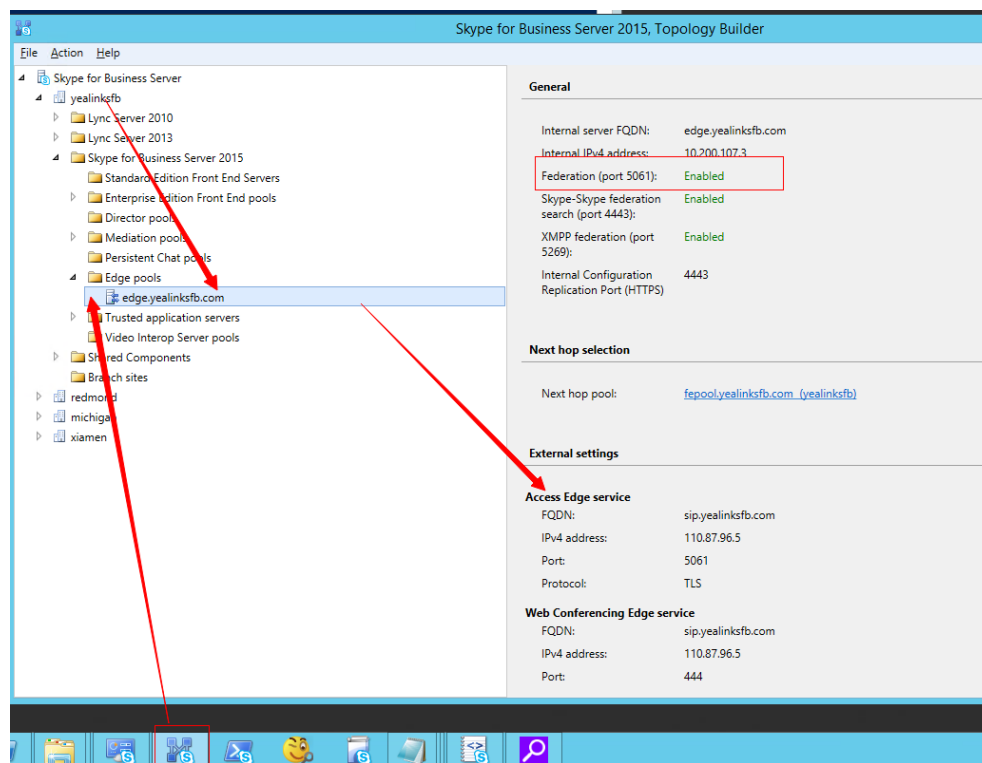
Pinging sip.yealinksfb.com [110.87.96.5] with 32 bytes of data:
Reply from 110.87.96.5: bytes=32 time<1ms TTL=128
Reply from 110.87.96.5: bytes=32 time<1ms TTL=128
Reply from 110.87.96.5: bytes=32 time<1ms TTL=128
Reply from 110.87.96.5: bytes=32 time<1ms TTL=128

Ping statistics for 110.87.96.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>_

```

- View the information of the SfB edge server in the Front End topology. The information includes whether or not the federation is enabled on the SfB edge server.

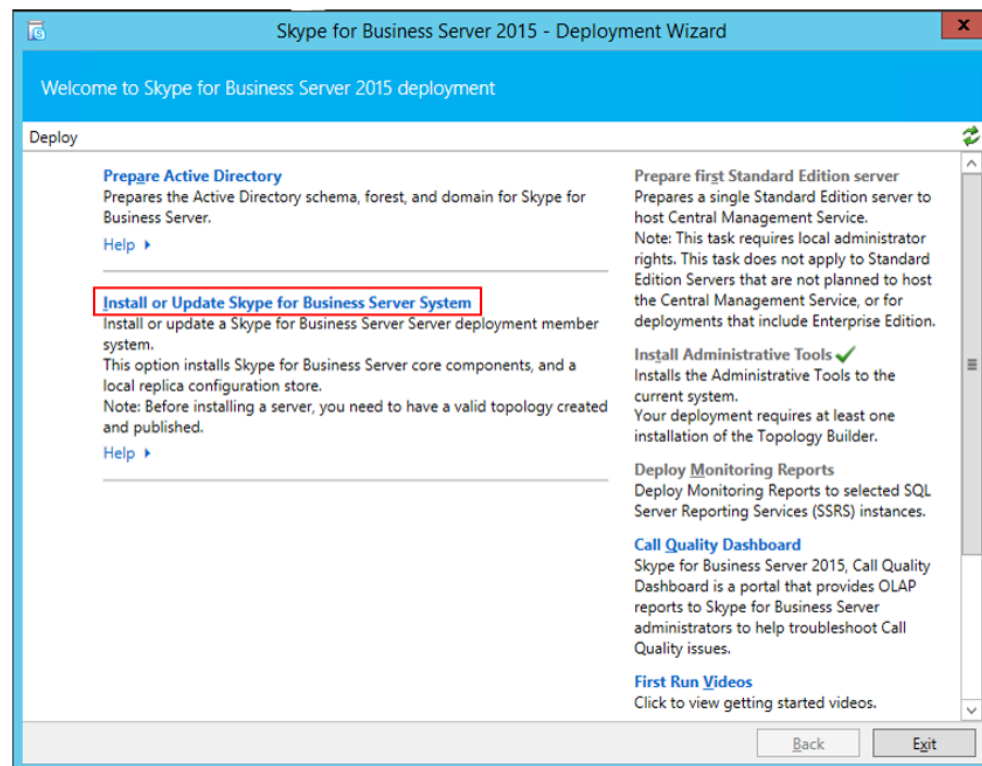


2. Make sure that the SRV record and the A record of YMS and SfB are configured on the public DNS server.

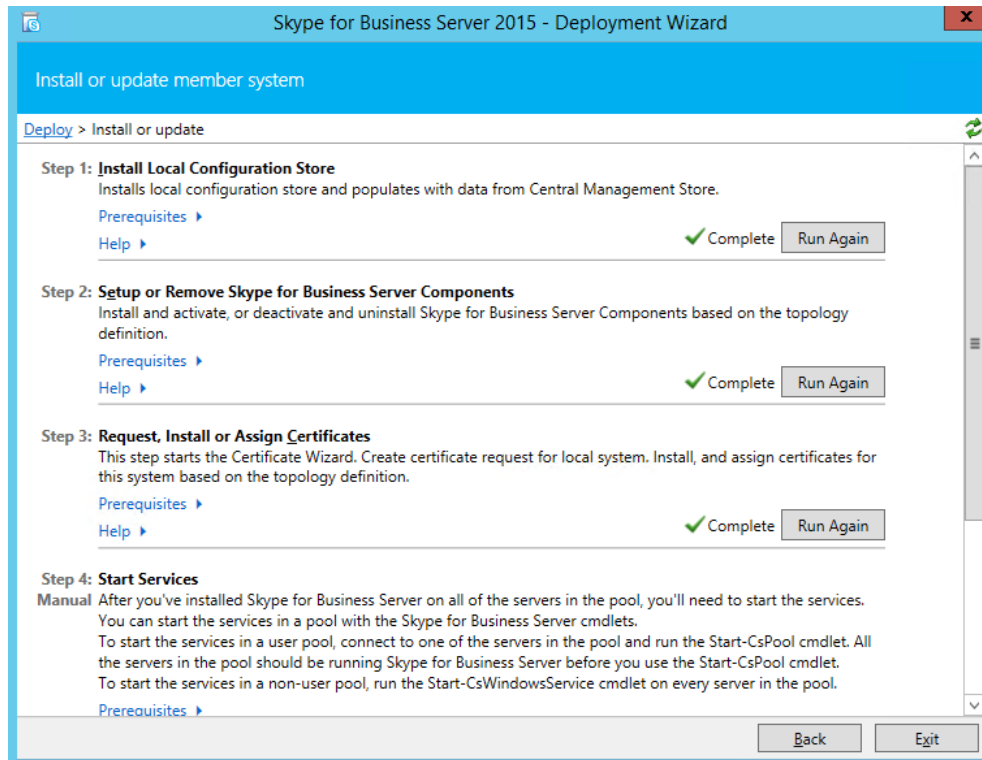
- Log into the public DNS server where the SfB edge server is located to view the SRV record and the A record. The host record must be `_sipfederationtls_tcp` in the SRV record.

<input type="checkbox"/>	A	sip	默认	110.87.96.5
<input type="checkbox"/>	A	sipexternal	默认	110.87.96.5
<input type="checkbox"/>	SRV	_sip_tls	默认	0 100 5061 sip.yealinksfb.com
<input type="checkbox"/>	SRV	_sipfederationtls_tcp	默认	0 100 5061 sip.yealinksfb.com
<input type="checkbox"/>	SRV	_sip_tcp	默认	0 0 5060 sip.yealinksfb.com

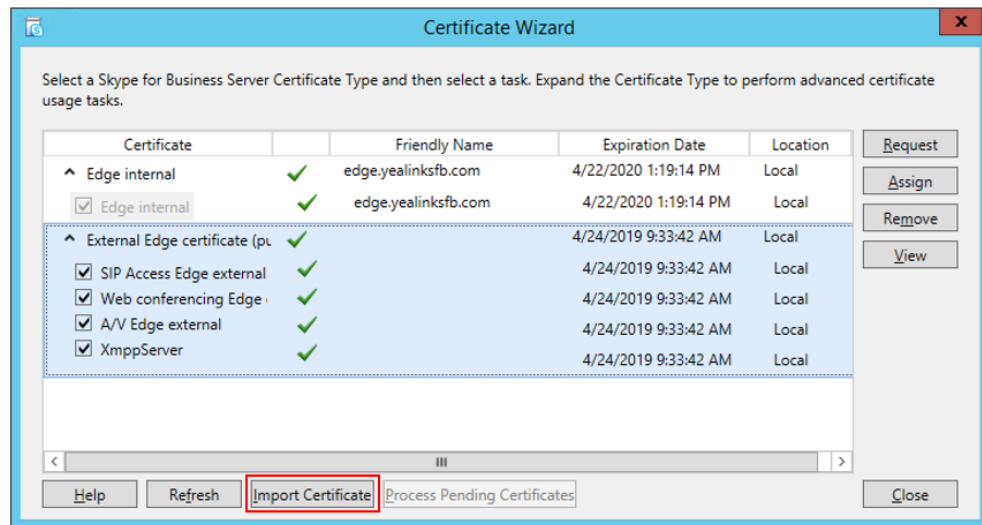
- Log into the public DNS server where YMS is located to view the SRV record and the A record. The host record must be `_sipfederationtls_tcp` in the SRV record.
3. Check if you purchase the certificate of the SfB edge server from a trusted third-party organization. The procedure of importing the certificate is described as below:
    - a) Go to the Deployment Wizard of the Lync Server, and click **Install or Update Skype for Business Server System**.



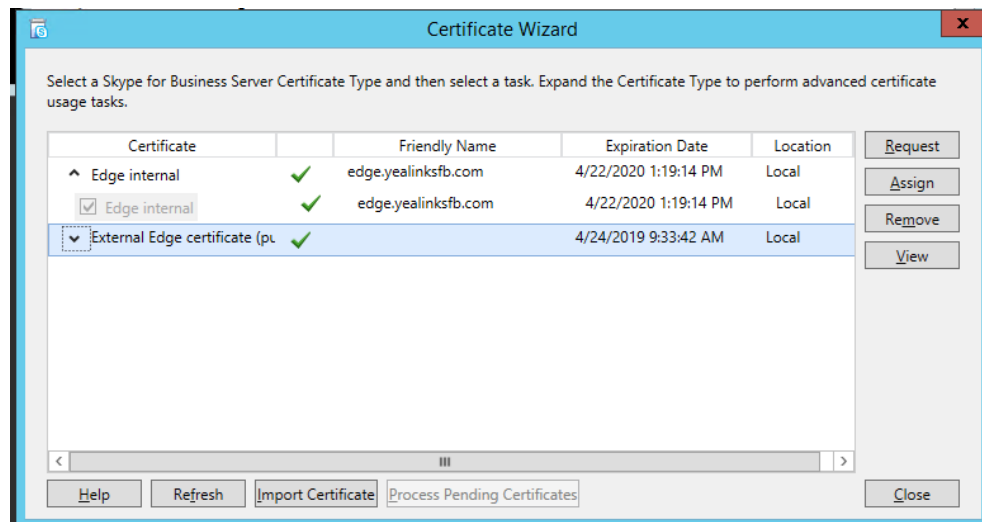
- b) Click **Run Again**.



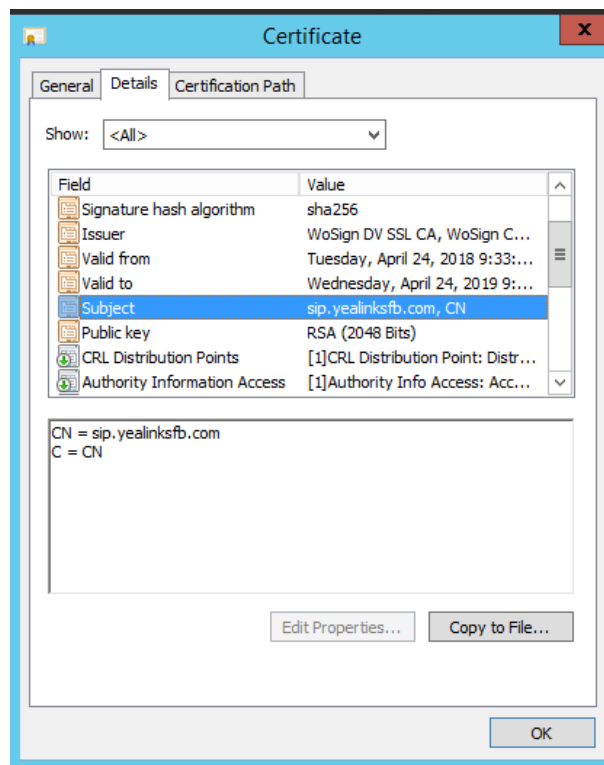
c) Click **Import Certificate** and import the external edge certificate.



After importing, the page is shown as below:

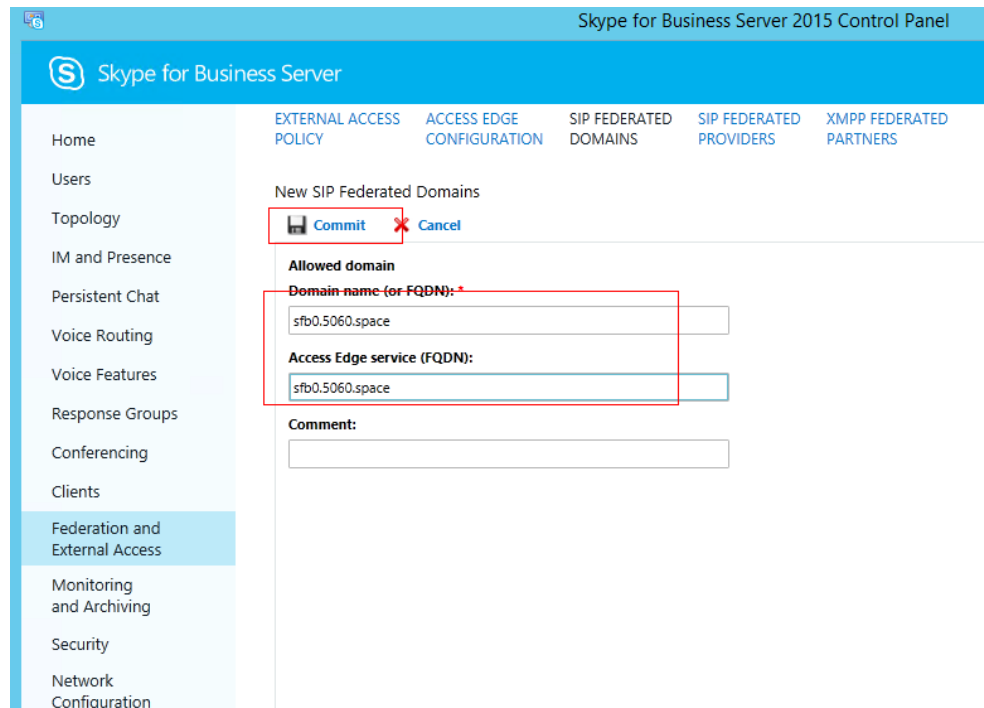
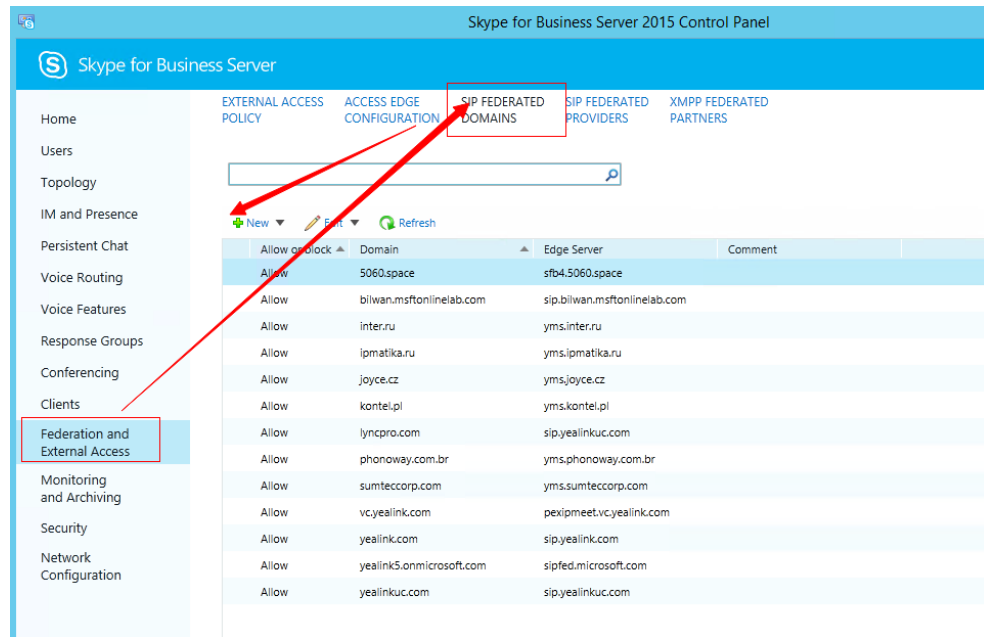


- d) Select the imported edge server certificate, click **View**, and make sure that the user name (commonName attribute) or the user optional name (altNames attribute) contain the FQDN name of the edge server.



#### 4. Configure the federation information on the SfB and YMS.

- a) Open the Control Panel in the SfB Front End, click **Federation and External Access**, and add the YMS FQDN that connects to the SfB business node to the **SIP FEDERATION DOMAINS** field.



## Setting the SFB Gateway

To route calls correctly to the specified Sfb server, you need to add a Sfb gateway on YMS, providing the destination gateway for the call routing.

### Before you begin

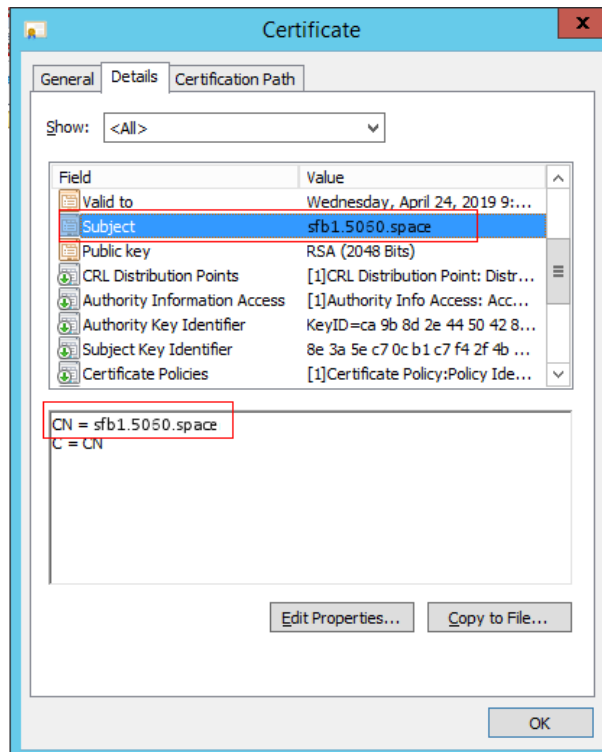
Make the Sfb server trust this YMS by [Importing the TLS Certificate](#) on this YMS.

The methods of obtaining the certification are described as follows:

- If it is the local Sfb server, you can use a certificate issued by a public CA, or a certificate issued by the organization's internal CA (trusted by Sfb and YMS).
- If it is Microsoft office 365 or other enterprise Sfb servers, you can use the certificate issued by a public CA.

The certificate should meet the following:

- The Subject name (commonName attribute) or the Subject Alternative Name (altNames attribute) of the certificate should contain the DNS FQDN name of YMS service node.



- The certificate should contain the public key and the private key.

```
-----BEGIN CERTIFICATE-----
MIIEczCCA1ugAwIBAgIJALSy12RyrkNWMA0GCSqGSIb3DQEBBQUAME8xetzARBgoJ
kiaJk/IsZAEZFgNjb20xGjAYBgokiaJk/IsZAEZFgpp5ZWFsaW5rc2ZiMRwwGgYD
VQDExN5ZWFSaW5rc2ZiLUFELUNBLUNBMB4XDTE3MTIyODAyMTIOMlcoXDTI3MTIy
NjAyMTIOMlownGZAxZAJBgNVBAYTAkNOMQ8wDQYDVQQIEwZGdWppYW4xZDZANBgNV
BAcTB1hpYW11bjEQMA4GA1UEChMHVWVhbG1uay5jb20xH2AdBgkqhkiG9w0BCQEW
EwZGdWppYW11bjEQMA4GA1UECjE5b20xH2AdBgkqhkiG9w0BCQEWZGdWppYW11bjEQ
eWVhbG1uay5jb20xGjAYBgokiaJk/IsZAEZFgpp5ZWFsaW5rc2ZiMRwwGgYD
ddIJ9Rh/Ykx7kksD4bxK+qz50LLcIwY/qPI7ZcPUD0kf+zdz07/AQQkjza/cZgF
36R3oUBwrgJRRUZhdYHxRYr/+wOCHRmcCkPKKLSmpKezjxTzd/x3Eq1MyM4jD8j
TbTbRLjt3dZumZ03a5gBzja2wnFwexQ7Pmb6e4EnViW7PNfDfrtr1sQECNUCDBC
bo+7LIPDPp/trpYDB8U4fNuVHjko455jwTz3/wdsTwbosDISX46nywn01K8QpEB
9Q1fKglA6/Tzp5yNhoT62x0szADdOVZ6EBh0dZc8fduNiS8rIrVj+8Bfj14VktG2
e0JubaQcxHtZQ7k3AgMBAAGjggEOMIIBCjAMBGNVHRMEBTADAQH/MIHNBGNVHRE
gcUwgcKCFnBleG1wMm11ZXQueWVhbG1uay5jb20xH2AdBgkqhkiG9w0BCQEWZGdW
U0ZCMS41MDYwLnNwYWN1gg9TRkIyLjUwNjAuc3BhY2WCD1NGQjMuNTA2MC5zcGFj
ZYIPU0ZCNC41MDYwLnNwYWN1gg9TRkI1LjUwNjAuc3BhY2WCD1NGQjYuNTA2MC5z
cGFjZYIPU0ZCNCy41MDYwLnNwYWN1gg9TRkI4LjUwNjAuc3BhY2WCD1NGQjkuNTA2
MC5zcGFjZTAdBgNVHQ4EFgQUxXmjM3vh1JEGQX2WpMFTpNEJZoowCwYDVR0PBAQD
AgXgMA0GCSqGSIb3DQEBBQUAA4IBAQBtp42PO5TXqPNvEqn104QcEBXbukKmErOq
CqxksUVyudOQ/5qqyd6x9K1M/6BmAS2Fi/1463PaqiQEZZAbDH0UyAvisOyUDDW
WYEAya2vIe2tvE/NW7TFysWgHPWcvjLN91wtLNDVjJkb7r4Et7//TnRc5oHL5ok9
En43cfZ3inev1HgFhne3C6iHVip5X4T7rZ05j9G51QYp9Jw4GwiCT2syP2D010u/
Yf6h/yIwnYLE3s4MFwqkD4fRjh8p+aCjabhJxUPWvk7PCctmaceWUg1VRDIgZB4L
xsZPAeywK+qgvrYfAQFTB2OpAxVBXHuBsw0/6oPmtvJso50R+Qdt
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAnqYXcnXSCSFUYf2JMe5JLA+G8Svqs+dCy3CMGP6jy02XD1Hd
JH/s83d0/wEEJi82v3GYBd+kd6FAcK6iUUVGYXch4cUWK//sDgh65nApCjyi0pqs
```

**Procedure**

1. Click **Service > SIP Service > Skype for Business**.
2. Add a SfB gateway service.



## 3. Set the parameters.

**Table 37: Basic Parameters**

Parameter	Description
<b>Enabled</b>	Enable or disable the SfB gateway server. <b>Default:</b> enabled.
<b>Name</b>	Specify the name of SfB gateway.
<b>Node</b>	Specify the node used by this SfB gateway.
<b>Network</b>	Specify the IP address of this node.
<b>Transport protocol</b>	Only TLS is available if communicating with SfB.
<b>FQDN</b>	Specify the name of YMS. Example: sfb1.5060.space <b>Method:</b> add this domain name on DNS server which the A record of YMS is added to.
<b>Port</b>	Specify the source port on YMS to communicate with SfB server. <b>Note:</b> the value can be any integer from 0 to 65535. This port must be consistent with the port configured in SfB server and cannot be occupied. <b>Default:</b> 5067.  If the SfB enables the federation, this port should be 5061. First of all, change the registration port to another port, and make this port as 5061, otherwise, the port will be closed by the firewall.
<b>Domain</b>	Specify the domain name of SfB server. For example, xiamen.yealinksfb.com.
<b>Port</b>	Specify the source port of the SfB server to communicate with YMS. <b>Default:</b> 5061.
<b>Federation</b>	Enable or disable the federation. <b>Default:</b> disabled.  According to different SfB servers, you can enable or disable the federation in one of the following scenarios: <ul style="list-style-type: none"> <li>• If the SfB server is the local SfB server, you can disable the federation.</li> <li>• If the SfB server is Microsoft Office 365 or other enterprise SfB servers, you can enable the federation.</li> </ul>
<b>Outbound proxy</b>	Enable or disable it to allow the SfB server to send requests to the outbound proxy server. <b>Default:</b> disabled.
<b>Proxy address</b>	Specify the IP address or the domain name of this outbound proxy server.
<b>Proxy port</b>	Specify the port of this outbound proxy server. <b>Note:</b> the value can be any integer from 0 to 65535.

Parameter	Description
<b>Support video</b>	If you enable this, you can place video calls to the remote that supports video calls.  <b>Default:</b> enabled.

4. Configure the security policy.

For adding a security group, see [Adding a Security Group](#)

Enable security policy:  ON

Mode:  Whitelist  Blacklist

Security Group: Please select the security group

test

+ Add + Add Security Group

Allow the IP address in this group to call into.

Refuse the IP address in this group to call into.

5. Configure the outgoing call rule.

Outgoing call rule

Priority: 1 Callee regex match: ^888(d+}@ Callee regex replace string: yS1@xiamen.yealinksfb.com

Priority: 1 Caller regex match: (+)@ Caller regex replace string: \$1@sfb1.5060.space

Priority: 1 Sfb conference regex match: ^666(d+}@ Sfb conference regex replace string: \$1@xiamen.yealinksfb.com

Account 3802 registered in the local YMS can dial 888751 to call Sfb account yl751@xiamen.yealinksfb.com.

Make the caller ID displayed in the remote call or conference as 3802@sfb1.5060.space rather than 3802.

Account 3802 registered in the local YMS can dial 66671920 to join Sfb conference 71920@xiamen.yealinksfb.com.

6. Configure the incoming call rule.

Incoming call rule

Priority: 1 Callee regex match: (+)@ Callee regex replace string: \$1@10.86.0.220.xip.io

Priority: 1 Caller regex match: y|(d+)@ Caller regex replace string: 888\$1@10.86.0.220.xip.io

Priority: 1 Sfb conference regex match: y|(d+)@ Sfb conference regex replace string: 666\$1@10.86.0.220.xip.io

Sfb account yl751@xiamen.yealinksfb.com can dial 3802 to call the account 3802 registered in the local YMS (10.86.0.220.xip.io).

Make the caller ID displayed in the local call as 888751@10.86.0.220.xip.io rather than yl751@xiamen.yealinksfb.com.

Make the caller ID displayed in the local conference as 666751@10.86.0.220.xip.io rather than yl751@xiamen.yealinksfb.com.

7. In the **SfB certificate** field, select the desired certificate to make the SfB server trust this YMS.

8. Save the configuration.

**Related concepts**

[Common Regular Expressions and Replacement Strings](#)

## Setting the SfB Gateway Media Service

If you want to communicate with the SfB server, you need to configure the SfB gateway media service.

### Procedure

1. Click **Service** > **MCU Service** > **SfB Gateway Media Service**.
2. Add a SfB gateway media service.
3. Set the parameters.

\* Enabled :  ON

\* Name :

\* Node :

\* External media port :  ~

\* All local networks :  10.83.1.150

4. Save the configuration.

## Communicating with Another YMS or Third-Party PBX (Peer Trunk)

To route calls between accounts registered in two different servers (for example, CUCM accounts and YMS accounts), [Setting the Peer Trunk Service](#) and [Adding a Call Routing Rule](#) need to be done.

- [Setting the Peer Trunk Service](#)
- [Peer Trunk Example](#)

## Setting the Peer Trunk Service

### Procedure

1. Click **Service** > **SIP Service** > **Peer Trunk Service**.
2. Add a peer trunk service.
3. Set the parameters.

Enabled :  ON

\* Name :

\* Node :

\* Network :

\* Port :  (Range : 1~65535)

\* Transport protocol :

Outbound proxy :  ON

\* Proxy address :

\* Proxy port :  (Range : 1~65535)

Set these parameters of YMS on the server you want to connect to.

If the domain name of the server that you want to connect to cannot be solved, enable outbound proxy, and set the parameters of the server.

4. Enable **Media Bypass** to improve the server performance and to support a larger number of participants in the conference. Note that the third-party devices have lower compatibility.

If **Support video** is enabled, **Media Bypass** is recommended to be enabled.

If **Media Bypass** is enabled, Media bypass service should be enabled too. For more information, refer to [Configuring the Media Bypass Service](#).

5. Optional: Configure the security policy.

For adding a security group, see [Adding a Security Group](#)

Enable security policy  ON

Mode :  Whitelist  Blacklist

Security Group

Please select the security group

test

+ Add + Add Security Group

Allow the IP address in this group to call into.

Refuse the IP address in this group to call into.

6. Configure the outgoing call rule.

Outgoing call rule

Priority :	Callee regex match :	Callee regex replace string :
1	^666(d+)	\$1@10.83.1.221.xip.io
+ Add		

Account 3802 registered in YMS (wc.cc) can dial 6664802 to call account 4802 registered in YMS (10.83.1.221.xip.io).

Priority :	Caller regex match :	Caller regex replace string :
1	(.+)	777\$1@wc.cc
+ Add		

Make the caller ID as 7773802@wc.cc rather than 3802 so the callee can redial quickly.

7. Configure the incoming call rule.

Incoming call rule

Priority :	Callee regex match :	Callee regex replace string :
1	(.+)	\$1@wc.cc
+ Add		

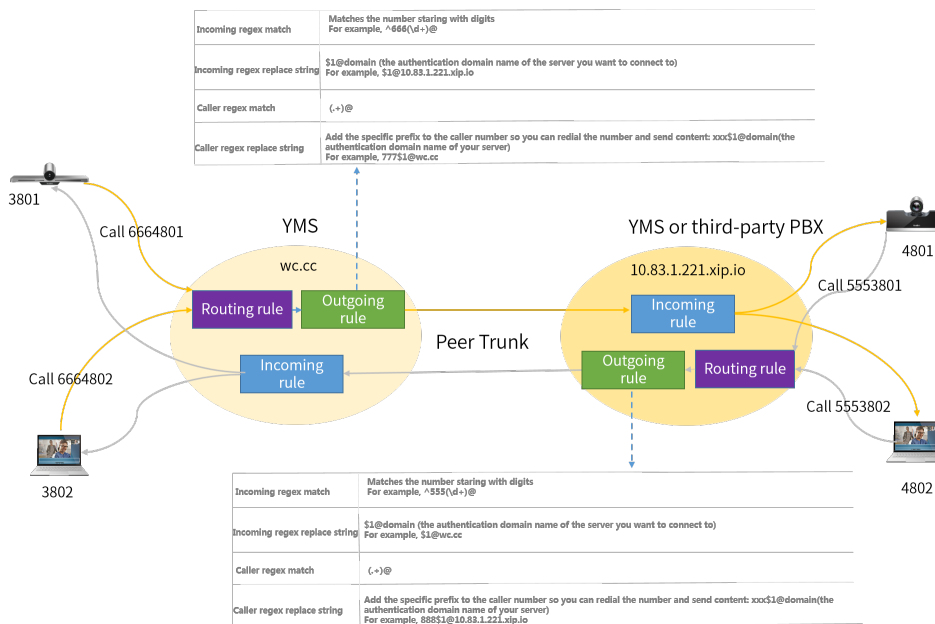
Account 4802 registered in YMS (10.83.1.221.xip.io) can dial 3802 to call account 3802 registered in YMS (wc.cc).

8. Save the configuration.

**Related concepts**

[Common Regular Expressions and Replacement Strings](#)

## Peer Trunk Example



- **Situation**

- YMS SIP account 3802 can dial 6664802 to call another YMS SIP account 4802. You can make the caller ID as 7773802 rather than 3802, and the callee can redial 7773802 to call 3802.
- YMS SIP account 4802 can dial 5553802 to call YMS SIP account 3802. You can make the caller ID as 8884802 rather than 4802, and the callee can redial 8884802 to call 4802.
- YMS SIP account 4802 can dial 555+Conference ID to join the conference held by YMS SIP account 3802, and the caller ID is displayed as 8884802@10.83.1.221.xip.io.

- **The configurations are as below:**

- Enable the peer trunk service on both servers
- Set the outgoing call rule and the call routing on server wc.cc

**Outgoing call rule**

Priority :	Callee regex match :	Callee regex replace string :
<input type="text" value="1"/>	<input text"="" type="text" value="\$1@10.83.1.221.xip.io"/>	
<input type="button" value="+ Add"/>		
Priority :	Caller regex match :	Caller regex replace string :
<input type="text" value="1"/>	<input type="text" value="(.)"/>	<input type="text" value="777\$1@wc.cc"/>
<input type="button" value="+ Add"/>		

Call Routing + Add

Search

Selected 0 Delete

<input type="checkbox"/>	Name	Priority	Destination match	Call Target/Out Location	Enabled	Operation
<input type="checkbox"/>	对等trunk	1	^555(d+)	Peer Trunk / 对等Trunk	<input type="checkbox"/>	<a href="#">✎</a>
<input type="checkbox"/>	rr	1	^030	Register Trunk / e	<input checked="" type="checkbox"/>	<a href="#">✎</a>
<input type="checkbox"/>	dd	1	^10086	H.323 GW / 150	<input type="checkbox"/>	<a href="#">✎</a>
<input type="checkbox"/>	Peer trunk	1	^666(d+)	Peer Trunk / 对等Trunk	<input checked="" type="checkbox"/>	<a href="#">✎</a>
<input type="checkbox"/>	IP call 2	2	^conf	IP Call / IP直拨	<input type="checkbox"/>	<a href="#">✎</a>
<input type="checkbox"/>	zhibo	3	^10086	IP Call / IP直拨	<input type="checkbox"/>	<a href="#">✎</a>

Select all pages Total 6 | 10page < 1 > Go to 1 Pages

- Set the outgoing call rule and the call routing on server 10.86.1.221.xip.io

#### Outgoing call rule

Priority : Callee regex match : Callee regex replace string :

1 ^555(d+)\$ \$1@wc.cc ✕

+ Add

---

Priority : Caller regex match : Caller regex replace string :

1 (.+)\$ 888\$1@10.83.1.221.xip.ir ✕

+ Add

Call Routing + Add

Search

Selected 0 Delete

<input type="checkbox"/>	Name	Priority	Destination match	Call Target/Out Location	Enabled	Operation
<input type="checkbox"/>	peer_trunk	1	^555(d+)	Peer Trunk / 对等Trunk	<input checked="" type="checkbox"/>	<a href="#">✎</a>

## Communicating with Another YMS or Third-Party PBX (Registration Trunk)

To communicate with the third-party PBX, [Configuring the REG Trunk Service](#) and [Adding a Call Routing Rule](#) need to be done. For example, if you want to communicate with BSFT or 3CX server, you need to register a BSFT or 3CX account on YMS.

YMS accounts can call third-party accounts directly, while third-party accounts can only call into YMS conferences but cannot place P2P calls to YMS account. Besides, the P2P call can only be transmitted by third-party accounts registered in YMS.

- [Configuring the REG Trunk Service](#)
- [Registration Trunk Example](#)

## Configuring the REG Trunk Service

### Procedure

1. Click **Service** > **SIP Service** > **REG Trunk Service**.
2. Add a REG trunk service.
3. Set the parameter.

Enabled :

\* Name :

\* Node :

\* Network :

\* Port :  (Range : 1-65535)

\* Transport protocol :

Outbound proxy :

\* Proxy address :

\* Proxy port :  (Range : 1-65535)

Display name :

\* URL :

\* Auth name :

\* Auth domain :

\* Password :

\* Expires :  (Range : 30-3600)

Set these parameters of YMS on the server you want to connect to.

If the domain name of the server that you want to connect to cannot be solved, enable outbound proxy, and set the parameters of the server.

The account provided by the server you want to connect to. With this account, you can take your YMS as an endpoint and register YMS on the server.

4. Enable **Media Bypass** to improve the server performance and to support a larger number of participants in the conference. Note that the third-party devices have lower compatibility.

If **Support video** is enabled, **Media Bypass** is recommended to be enabled.

If **Media Bypass** is enabled, Media bypass service should be enabled too. For more information, refer to [Configuring the Media Bypass Service](#).

5. Configure the outgoing call rule.

Outgoing call rule

Priority :	Callee regex match :	Callee regex replace string :
<input type="text" value="1"/>	<input type="text" value="^777(d+)@"/>	<input type="text" value="\$1@10.86.0.103.xip.io"/>
<input type="button" value="+ Add"/>		
Priority :	Caller regex match :	Caller regex replace string :
<input type="text" value="1"/>	<input type="text" value="(d+)@"/>	<input type="text" value="030@10.86.0.103.xip.io"/>
<input type="button" value="+ Add"/>		

Account 3802 registered in YMS (10.86.0.104.xip.io) can dial 7774802 to call account 4802 registered in YMS (10.86.0.103.xip.io).

Make the caller ID as 030@10.86.0.103.xip.io rather than 3802 so the callee can redial quickly.

6. Configure the incoming call rule.

Incoming call rule

Priority :	Callee regex match :	Callee regex replace string :
<input type="text" value="1"/>	<input type="text" value="^030"/>	<input type="text" value="main_jvr@10.86.0.104.xip.io"/>
<input type="button" value="+ Add"/>		

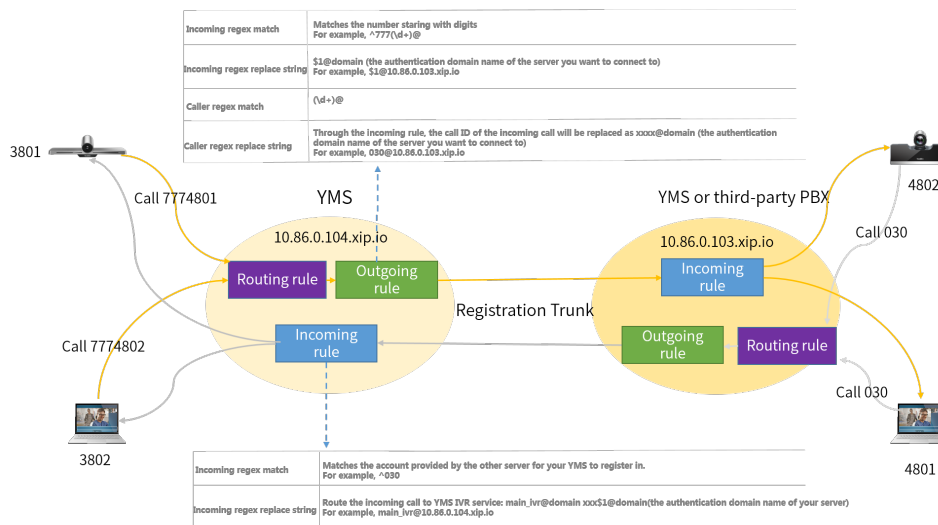
Account 4802 registered in YMS (10.86.0.103.xip.io) can dial 0301 to go to the conference lobby in YMS (10.86.0.104.xip.io).

7. Save the configuration.

**Related concepts**

[Common Regular Expressions and Replacement Strings](#)

## Registration Trunk Example



- Situation**
  - YMS SIP account 3802 can dial 7774802 to call another YMS SIP account 4802.
  - YMS SIP account 4802 can dial 030 to go to the conference lobby of another YMS (SIP trunk IVR). YMS SIP account 4802 can dial the extension number or join the conference according to the prompts.
- The configurations are as below:**
  - Enable the registration services on both servers
  - Enable the third party registration service on server 10.86.0.103.xip.io (the outbound proxy of the registration service on server 10.86.0.104.xip.io directs to this node).
  - Set the outgoing call rule, the incoming call rule, and the call routing on server 10.86.0.104.xip.io

### Outgoing call rule

Priority :	Caller regex match :	Callee regex replace string :
<input type="text" value="1"/>	<input text"="" type="text" value="\$1@10.86.0.103.xip.io"/>	
<input type="button" value="+ Add"/>		

Priority :	Caller regex match :	Caller regex replace string :
<input type="text" value="1"/>	<input text"="" type="text" value="030@10.86.0.103.xip.io"/>	
<input type="button" value="+ Add"/>		

### Incoming call rule

Priority :	Callee regex match :	Callee regex replace string :
<input type="text" value="1"/>	<input type="text" value="^030"/>	<input type="text" value="main_ivr@10.86.0.104.xip.io"/>
<input type="button" value="+ Add"/>		



Call Routing + Add

Search

Selected 0 Delete

<input type="checkbox"/>	Name	Priority	Destination match	Call Target/Out Location	Enabled	Operation
<input type="checkbox"/>	peer_trunk	1	^555(d+)-@	Peer Trunk / 对等Trunk	<input type="radio"/>	<a href="#">✎</a>
<input type="checkbox"/>	rr	1	^030	Register Trunk / e	<input checked="" type="radio"/>	<a href="#">✎</a>
<input type="checkbox"/>	dd	1	^10086	H.323 GW / 150	<input type="radio"/>	<a href="#">✎</a>
<input type="checkbox"/>	777	1	^777	Register Trunk / e	<input checked="" type="radio"/>	<a href="#">✎</a>
<input type="checkbox"/>	IP call 2	2	^conf	IP Call / IP直播	<input type="radio"/>	<a href="#">✎</a>
<input type="checkbox"/>	zhibo	3	^10086	IP Call / IP直播	<input type="radio"/>	<a href="#">✎</a>

Select all pages Total 6 10page < 1 > Go to 1 Pages

- Set the call routing on server 10.86.0.33.xip.io

Call Routing + Add

Search

Selected 0 Delete

<input type="checkbox"/>	Name	Priority	Destination match	Call Target/Out Location	Enabled	Operation
<input type="checkbox"/>	peer_trunk	1	^555(d+)-@	Peer Trunk / 对等Trunk	<input type="radio"/>	<a href="#">✎</a>
<input type="checkbox"/>	rr	1	^030	Register Trunk / e	<input checked="" type="radio"/>	<a href="#">✎</a>

## Setting Alibaba Cloud RTMP Live

Some activities, for example lectures or training, have large audiences but limited interaction between the lecturers and the audience. Moreover, the cost is high, and it takes many video port resources if it is held by the general video conferences. In this situation, the audience who do not need to join the activity can choose to watch the webcast.



**Note:** The number of participants that can concurrently watch the webcast depends on the authorized license.

You can follow the steps below to set the RTMP media service. For more information, refer to [RTMP Configuration Guide](#)

1. [Configuring the RTMP Media Service](#)

2. [Configuring the RTMP Live](#)

3. For scheduled conferences, when users schedule conferences, enable **RTMP live**. For more information, refer to [Yealink Meeting Server User Guide](#).

4. For VMR, refer to [Setting the RTMP Live for VMRs](#) to enable **RTMP live**.

4. The conference moderator goes to the Conference Control page and starts the webcast. For more information, refer to [Yealink Meeting Server User Guide](#).

If you want to use RTMP media service, make sure that the network is available and check the following:

- The server can access the external network.
- If your company has limitation to the web surfing, make sure that the server has the video privilege.

You can also stream the conference to YouTube so users can watch the webcast. For more information, refer to [Yealink Meeting Server Streaming Guide](#).

- [Configuring the RTMP Media Service](#)
- [Configuring the RTMP Live](#)
- [Setting the RTMP Live for VMRs](#)

## Configuring the RTMP Media Service

### Procedure

1. Click **Service > MCU Service > RTMP Media Service > Add**.
2. Set the parameters.

\* Enabled :  ON

\* Name :

\* Node :

\* External media port :  --

\* All local networks :  10.83.1.150

### Related tasks

[Configuring the RTMP Live](#)

## Configuring the RTMP Live

### Before you begin

- Obtain the information about the ApsaraVideo Live of Alibaba Cloud.
- [Configuring the RTMP Media Service](#) .

### About this task

For more information about RTMP Live, refer to <http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>.

### Procedure

1. Click **Call Configuration > Call Control Policy**.
2. Enable **Alibaba Cloud RTMP live**.
3. Set the parameters.

**Table 38: RTMP live parameters**

Parameter	Description
<b>Organizer Logo</b>	Specify the logo displayed on the Webcast page.
<b>Domain</b>	Specify the domain name of the server.
<b>Application name</b>	Specify the application name in the authentication URL.
<b>Live domain</b>	Specify the domain name.
<b>Edge Ingest</b>	Specify the streaming method. <b>Note:</b> if your domain name for watching is added after February 21, 2019, you cannot use the Live Center Ingest method.
<b>Enable authentication</b>	Enable or disable the authentication. <b>Default:</b> disabled.

Parameter	Description
Authentication key	Specify the authentication password.

4. Click **Save**.
5. Operate according to the prompts, and click **OK**.

#### Related tasks

[Configuring the RTMP Media Service](#)

## Setting the RTMP Live for VMRs

### Procedure


Click **Meeting Room > Virtual Meeting Room** and do one of the following:

RTMP live : ?  ON

Definition : HD(720P) ▼

Layout : 1+N ▼

Details :

- If you want to add a VMR, click **Add Meeting Room**.  
In the **Permission setting** field, set the parameters.
- If you want to edit a VMR, click .  
In the **Permission setting** field, set the parameters.

**Table 39: RTMP live parameters**

Parameter	Description
<b>RTMP Live</b>	Enable or disable the RTMP live. If it is enabled, the users can watch the webcast of the conference. <b>Default:</b> disabled.
<b>Definition</b>	It refers to the video resolution that the MCU sends to a live streaming platform. The supported video resolution is as below: <ul style="list-style-type: none"> <li>• 1080P(1080P)</li> <li>• HD(720P)</li> </ul> <b>Default:</b> 720P.

Parameter	Description
Layout	<p>Configure the video layout displayed in the webcast.</p> <p>The supported layouts are as below:</p> <ul style="list-style-type: none"> <li>• <b>1+N</b>: the video layout of the webcast is displayed in 1+N format with the voice-activated feature enabled. If no participants share content, the current speaker is displayed in a large video image. Otherwise, the shared content is displayed in the large video image. Up to 1+N participants are displayed in a single row of live thumbnails at the bottom, that is, the video images in the row are switched automatically.</li> <li>• <b>Picture in picture</b>: the video layout of the webcast is displayed in Picture in picture format. If no participants share content, the current speaker is displayed in a large video image. Otherwise, the shared content is displayed in the large video image and the video image of the current speaker is reduced to a thumbnail at the bottom-right corner.</li> <li>• <b>Selected speaker</b>: the video layout of the webcast is displayed in Selected speaker format. If no participants share content, the current speaker is displayed in a large video image. Otherwise, the shared content is displayed in the large video image.</li> </ul>
Event details	It refers to the text displayed on the Live page.

## Enabling Conference Recording (Third-Party Recording Server)

You can enable this feature and configure the third-party recording server to record conferences.

### About this task



**Note:** If you want to use the recording service of YMS, you can refer to [Yealink Recording Service](#) .

Before you configure the third-party recording server, make sure Yealink technical support engineers have deployed the third-party recording server. If the recording server is deployed, you need to obtain the corresponding information of the recording server from the Yealink technical support engineers.

### Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Recording** and set the parameters.

Recording : ?

ON 

RSS address :	<input type="text" value="10.10.10.10"/>
Port :	<input type="text" value="80"/>
HTTP port :	<input type="text" value="81"/>
RPC port :	<input type="text" value="6000"/>
RPC username :	<input type="text" value="user"/>
RPC password :	<input type="text" value="pass"/>

3. Save the configuration.

## System Maintenance

---

- [Making Backups and Restoring the Server](#)
- [Rebooting the System](#)
- [Resetting to the Factory](#)
- [Viewing Operation Logs](#)
- [Exporting System Logs](#)
- [Using Tools](#)

### Making Backups and Restoring the Server

---

When there is sufficient space for backups, you can make backups for the server data, including the user accounts and the conference information.

- [Setting the Auto Backup](#)
- [Creating a Backup Manually](#)
- [Downloading a Backup](#)
- [Restoring the Backup](#)

### Setting the Auto Backup

#### Procedure

1. Click **Maintenance > Backup/Restore > Setting**.
2. Configure the parameter and save it.

×

### Automatic Backup Setting

Auto backup :  ON

Cycle :  Monthly  Weekly  Daily

Date :

Max backup number :   
When the backups are more than the max, the oldest files will be covered automatically.

## Creating a Backup Manually

### Procedure

1. Click **Maintenance > Backup/Restore > Add.**
2. Enter the file name and save the configuration.


×

### Add Backup

File name :

## Downloading a Backup

### Procedure

1. Click **Maintenance > Backup/Restore.**
2. Click  on the right side of the desired file.

Backup/Restore Setting Upload Add

Search

Selected 0 Delete

<input type="checkbox"/>	File Name	File Size(KB)	Build Time	Operation
<input type="checkbox"/>	Backup_190902_181212.tar.gz	804.6	2019/09/02 18:12	<span>Download</span> <span>Refresh</span>
<input type="checkbox"/>	Backup_190712_133704.tar.gz	184.5	2019/07/12 13:37	<span>Download</span> <span>Refresh</span>

Select all pages Total 2 10/page < 1 > Go to 1 Pages

## Restoring the Backup

If the server is powered off during the restoring, after powered on, it will return to the status before being restored.

- [Restoring a backup by Selecting a Backup Directly](#)
- [Restoring the Server by Uploading a Backup](#)


### Restoring a backup by Selecting a Backup Directly

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

#### Before you begin

[Setting the Auto Backup](#) or [Creating a Backup Manually](#)

#### Procedure

1. Click **Maintenance** > **Backup/Restore**.
2. Click  on the right side of the corresponding file, and confirm to restore the server.

Backup/Restore Setting Upload Add

Search

Selected 0 Delete

<input type="checkbox"/>	File Name	File Size(KB)	Build Time	Operation
<input type="checkbox"/>	AutoBackup_20191015_120000.tar.gz	1010.2	2019/10/15 12:00	<span>Download</span> <span>Refresh</span>
<input type="checkbox"/>	AutoBackup_20191014_120000.tar.gz	1007.9	2019/10/14 12:00	<span>Download</span> <span>Refresh</span>
<input type="checkbox"/>	AutoBackup_20191013_120000.tar.gz	1008.0	2019/10/13 12:00	<span>Download</span> <span>Refresh</span>
<input type="checkbox"/>	Backup_190902_181212.tar.gz	804.6	2019/09/02 18:12	<span>Download</span> <span>Refresh</span>
<input type="checkbox"/>	Backup_190712_133704.tar.gz	184.5	2019/07/12 13:37	<span>Download</span> <span>Refresh</span>

Select all pages Total 5 10/page < 1 > Go to 1 Pages

### Restoring the Server by Uploading a Backup

When an exception occurs to the server or the data is lost because of an accidental operation, you can restore the data by the backup file to keep the server working normally.

#### Before you begin

[Downloading a Backup](#)

#### Procedure

1. Click **Maintenance** > **Backup/Restore** > **Upload**.
2. Click **Upload**, and select the desired file.

×

## Upload Local Backup

Restore file : 📁 Upload

Only .tar or .gz format file is available

OK
Cancel

- If you succeed in uploading, click **OK**, and the server will be restored immediately.

## Rebooting the System

---

When you fail to upgrade the server, for example, the server stuck on a certain page, you can choose to reboot the system.

### Procedure

- Click **Maintenance > System Restart**.
- Select a node and reboot the node.

**System Restart**

Select the node : Default(10.83.1.150) ▾

Restart

## Resetting to the Factory

---

In some situations, you might need to clear up the entire user data, the system settings, the call records, the logs, and the recording files to solve the problem that occurred to the YMS.

### Procedure

- Click **Maintenance > Restore to factory setting**.
- Select the data type, and reset the server to the factory.

**Restore to factory setting**

Please select the data type to be cleared:

- User Data** (User data includes: accounts, meeting rooms, scheduled meetings' data )
- System configurations** (System configurations include: all server configurations, backups, device firmware)
- CDR** (Call detail records include: conference records, P2P call records)
- Logs** ( Logs include: server, endpoints, operation and recording logs )
- Recording files** ( Recording files include: All recording files )

Restore to Factory Settings



## Viewing Operation Logs

The operation log keeps a record of the changes, including the visit record and the configuration record.

### Procedure

Click **Maintenance > Operation Log > Operation Log**.

Operation Log					
2019-09-25	-	2019-09-25	Search	Advanced Search	Export Log Delete
Name	IP Address	Operation Module	Operation	Operation Time	Result
admin	10.82.24.2	Login module	Log In	2019/09/25 17:13	Operation Successful
admin	10.87.1.16	Conference module	Conference control	2019/09/25 16:49	Operation Successful
admin	10.87.1.16	Conference module	Conference control	2019/09/25 16:39	Operation Successful



**Tip:** You can also click **Export Log** in the top right corner to view the log.

## Exporting System Logs

You can view the system log to find out the reason when a problem occurs to the server. For example, someone removes the cable from the server, or the server is restarted because of being powered off.

### Procedure

1. Click **Maintenance > Operation Log > System Log**.
2. Select the time, the module, and the node to export the log.

Operation Log **System Log** Recording log

Please select the desired time to export logs :

-

Please select the module that need to export server logs

Signalling
  Media
  Web
  System

Please select the node that need to export server logs

Nodes ( 3 )	Selected nodes ( 1 )
<input checked="" type="checkbox"/> Default(10.83.1.150) <input type="checkbox"/> Default(10.83.1.151) <input type="checkbox"/> Default(10.83.1.152)	Default(10.83.1.150)
<input type="button" value="Select All"/>	<input type="button" value="Cancel"/>

3. Click **Export Syslog**.

## Using Tools

---

Ping and packetcapture are available on YMS to test the network.

- [Pinging the Network](#)
- [Capturing Packets](#)

### Pinging the Network

You can ping the network to test the network performance from the node to the destination.

#### Procedure

1. Click **Maintenance > Tools > Ping**.
2. Select one node, enter the IP/domain name of the destination, and select the number of requests.
3. Click **Start**.

Ping
Packetcapture

Select node :

IP/Domain name

Number of requests :

Output of ping:

### Capturing Packets

You can capture packets to analyze the network traffic sent or received by the nodes.

#### About this task

If you encounter problems when using YMS, Yealink technical support engineers will solve the problem with the packets you captured.

#### Procedure

1. Click **Maintenance > Tools > Packetcapture**.
2. Select the desired node.
3. Enter the file name.  
Only 64 characters are allowed, and the file name can only be made up of characters, numbers, \_ and \$.
4. Select the desired network adapter.

5. Click **Packetcapture settings**, and set the file size and the total size.
6. Click **Capture now** or **Schedule capture**.

Ping **Packetcapture**

Select node :

File Name :

Packetcapture ethernet :

Packet Filter String :

Filter strings mainly include three types: type, direction and protocol

1. Type : mainly includes host, net, port;  
For example: host 210.45.114.211 indicates a host with IP address 210.45.114.211; net 210.11.0.0 indicates a network address with IP address 210.11.0.0; port 21 indicates a port with port number to be 21.

2. Direction: mainly includes src, dst, dst or src, dst and src;  
For example: src 210.45.114.211 indicates that the source IP address of the packet is 210.45.114.211.

3. Protocol: mainly includes ether, ip, ip6, arp, rarp, tcp, udp, etc.

The above three types of filter strings can be combined with the logical operators: not, and, or to establish complex filter strings.

( Tips : Packetcapture will consume server

06 20:07 Packetcapture success

File Name : 20190806\_200732.pcap

## Troubleshooting

---

- [Users Do Not Receive Emails](#)
- [Failing to Connect to SMTP](#)
- [Users Fail to register an Account](#)
- [Failing to Activate a License Online](#)
- [Failing to Activate a License Offline](#)
- [Loading the Organizational Structure Slowly](#)
- [The Configuration of Access WebRTC Authentication Is Invalid](#)

### Users Do Not Receive Emails

---

**Situation:**

When you send the account information to users by email, but users do not receive any emails.

**Cause:**

- [Configuring the SMTP Mailbox](#) is not configured or you do not add the email address when adding user accounts.
- The emails may be in the spam folders.
- The emails may be intercepted by the back-end server.

**Solution:****Procedure**

1. [Configuring the SMTP Mailbox](#) .
2. Remind users to check the spam folders.
3. Contact the enterprise IT staff to check the back-end server.

## Failing to Connect to SMTP

---

**Situation:**

When setting the SMTP, it prompts failing to connect to SMTP server.

**Cause:**

- The connection between YMS and SMTP server cannot work.
- The setting of SMTP is incorrect.
- If you enable the secure connection, YMS might fail to verify SMTP server.

**Solution:****Procedure**

1. [Pinging the Network](#) to make sure that the connection to SMTP server can work.
2. Contact your IT staff to make sure the setting of SMTP is correct.
3. If the SMTP server uses a self-signed certificate, you need [Importing the Trusted CA Certificate](#) .

## Users Fail to register an Account

---

**Situation:**

Users fail to register an account.

**Cause:**

- Users may enter the wrong registration information.
- The user IP address is set as an abnormal IP address.
- Users can not access YMS due to the network problem.

**Solution:****Procedure**

1. Check the registration information.
2. Check whether or not the user IP address is set as an abnormal IP address. If it is, you can [Deleting the Abnormal IP](#) .

## Failing to Activate a License Online

---

### Situation:


Click **Refresh**, and the prompt “Unable to connect to License Server due to network problem” is popped up.

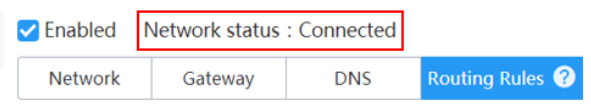
### Cause:

- Network configuration error.
- Other YMSs use the license; or the CPU, the network adapter or the motherboard on YMS is changed, which causes the mismatch between the license and the YMS hardware information.

### Solution:

#### Procedure

1. Check whether or not the network cable of the YMS physical machine is connected.
  - a) Click **System Settings > Node Management**.
  - b) Click  on the right side of desired node to view the network status.



2. If you use a Linux console, run the command "ping license.yealink.com".
  - If it fails, there is a problem with the DNS or the gateway route configured on the network.
  - If it succeeds but takes a long time, the reason may be the DNS configuration problem or the poor network.
3. Make sure that the server license is not used by other YMSs, or the CPU, the network adapter or the motherboard on YMS is not changed. If the above remedy cannot work, you can contact Yealink to get the license again.

### Related tasks

[Activating a License Online](#)

## Failing to Activate a License Offline

---

### Situation:

Import the authority file obtained from Yealink, but the page prompts “Certificate import failed”.

### Cause:

- Authority file error.
- Other YMSs use the license; or the CPU, the network adapter or the motherboard on YMS is changed, which causes the mismatch between the license and the YMS hardware information.

### Solution:

#### Procedure

1. Contact Yealink to confirm whether or not the authority file can match the serial number associated with your YMS.

2. Make sure that the server license is not used by other YMSs, or the CPU, the network adapter or the motherboard on YMS is not changed. If the above remedy cannot work, you can contact Yealink to get the license again.

**Related tasks**

[Activating a License Offline](#)

## Loading the Organizational Structure Slowly

---

**Situation:**

If you use the stand-alone version, wherever there is the organizational structure, when the number of the staff reaches 25,000, the speed of loading the data may become slower.

**Cause:**

A large amount of data.

**Solution:****Procedure**

Contact Yealink technical support engineers to modify the contact push mechanism.

## The Configuration of Access WebRTC Authentication Is Invalid

---

**Condition**

You have enabled the feature of internal network access WebRTC authentication, but when users join a conference via the browser, users are not required to enter the login information of YMS account.

**Cause**

The server fails to identify whether the IP address is an internal one or an external one.

**Remedy****Procedure**

1. Check whether you enable **Public IP** for the IP address used by the user to join the conference.
2. If you do enable it, do one of the following:
  - Change the IP address used by the user to join the conference to the internal one.
  - Enable the feature of **External network access WebRTC authentication**.