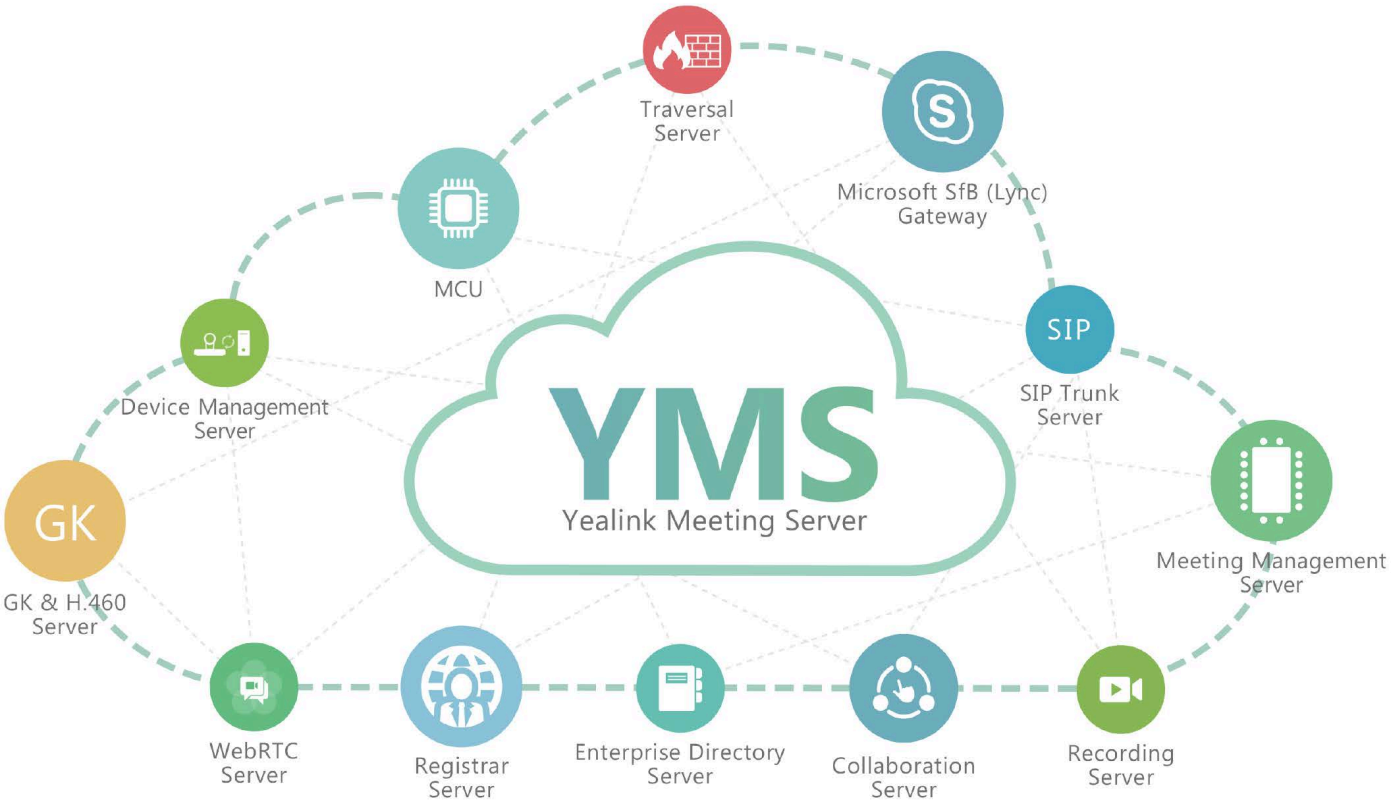
Yealink



Yealink Meeting Server Administrator Guide

Version 26.0.0.15 | April 2021

Contents

About This Guide 8

Targeted Audiences 8
Related Documents 8
Basic Concepts 8
Icon Introduction 9
In This Guide 9
Summary of Changes 10
Changes for Release 26, Guide Version 26.0.0.15 10
Changes for Release 26, Guide Version 26.0.0.10 10
Changes for Release 25, Guide Version 25.0.0.10 10
Changes for Release 24, Guide Version 24.0.0.20 11
Changes for Release 24, Guide Version 24.0.0.10 11
Changes for Release 23, Guide Version 23.0.0.11 11
Changes for Release 22, Guide Version 22.0.0.10 12
Changes for Release 21, Guide Version 21.0.0.5 12

Introduction of Yealink Meeting Server 13

Specifications 13
Distributed Architecture 15
Benefits of YMS Distributed Architecture 15
Components of YMS Distributed Architecture 16
Handling the Signaling and the Media 16
Browser Requirement 17
Port Requirements of the Router 17
Port Requirements of the Internal Service 17
Port Requirements for the External Service 18
Port Requirements for the External Service 18
Port Consumption 20

Installing and Deploying YMS 21

The Process of Installing and Deploying YMS 22
Good to Know about the Hardware 22
Basic Requirements of the Hardware 23
Calculating Method for the Concurrent Capacity 24
Recommended Hardware 24
Network Requirements 25
Checking the Version of CentOS 25
Viewing the Version of CentOS 26
Upgrading CentOS Online 26
Installing CentOS by Using a USB Flash Drive 26
Configuring the Node IP 26
Upgrading YMS 1.X to YMS 2.X 26
Making a Backup on YMS 1.4 27
Uninstalling YMS 1.4 29
Installing YMS 2.X 30
Migrating the Data on YMS 30
Installing YMS 2.X 30

Installing Stand-Alone YMS....30
Installing Cluster YMS....31
Expanding the Stand-Alone YMS....33
Upgrading YMS 2.X....34
Upgrading YMS 2.X via the Command....34
Upgrading YMS 2.X via the Web Interface....35
Uninstalling YMS 2.X....36

Getting Started....36
Logging into YMS....36
Setting the Setup Wizard....37
System Settings....38
Setting the Primary Domain Name....39
Editing the Login Password....39
Configuring SNTP....40
Configuring the SMTP Mailbox....41
Setting the Node....42
Service Settings....61
Setting the Registration Service....61
Setting the Traversal Service....62
Setting the Interactive Media Service....63
Activating a License....63
Importing the Device Certificate to the Server....64
Activating a License Online....64
Activating a License Offline....64
Disassociating the License....65
Creating Accounts....65
Creating Meeting Rooms....67
Managing Conferences....69
The Checklist for the Configurations and the Common Features....69

System Setting....70
Basic Operations....71
Introduction of the Home Page....71
Changing the Display Language for the Website....72
Editing the Registered Email....72
Setting the Session Timeout....72
Enabling Forced Https Authentication....73
Adding a Sub Admin Account....74
Customizing the Theme....76
Setting the Password Policy....82
Logging out of YMS....82
Setting the Web Service Address....82
Setting the Log Service Address....83
Setting the Web Access Port....84
Enabling the NTP Service....84
Setting the Time Zone....84
Importing the Trusted CA Certificate....85
Importing the HTTPS Certificate....86
Importing the TLS Certificate....87
Configuring the Port....87
Setting the Data Space....88
Allocating the Number Resource....88
Setting the IP Property....90

Setting the Intelligent Security Strategy....90
Adding a Security Group....92
Deleting the Abnormal IP....92
Applying for the Accesskey....93
Adding the User-Agent Blacklist....93
Adding the User-Agent Compatible List....94
Configuring the Email Template....94
Setting SIP Trunk IVR....95
Setting the Audio IVR....96
Setting IVR language....97

Managing Services....97
Configuring the Redirection Service....98
Broadcasting Interactive Conference....98
Configure the Broadcast Media Service....99
Enabling Broadcasting Interactive for Scheduled Conferences....99
Enabling Broadcasting Interactive for VMR....100
Yealink Recording Service....100
Enabling the Recording Service....101
Enabling Auto Recording....102
Managing the Recording Settings....102
Enabling the Recording Privileges for User Accounts....107
Enabling the Recording Privileges for VMRs....108
Managing the Recording Files....109
Managing the Sharing Link....112
Viewing the Recording Log....112
Managing Screenshot Files....113
Configuring the Media Bypass Service....114
Yealink Live Service....114
Enabling Live Service....115
Configuring YMS System RTMP Live....115
Setting the RTMP Live for VMRs....116
Collaboration Service....117
Setting the Collaboration Service....118
Managing Collaboration Files....118
Configuring the Third-Party Registration Service....119
Configuring the RTSP Gateway Service....121
Face Recognition Service....122
Installation of the Face Recognition Service....122
Enabling the Face Recognition Service....123
Registering Faces....124
Registering Faces (Quick Registration for External Users)....125
Configuring the GK Service....125
Setting the GK Service....125
Enable GK Registration for Accounts....127
H.323 Gateway....127
Setting H.323 Gateway....127
H.323 Gateway Example....129
H.323 Gateway Example (Taking H.323 Gateway as an Endpoint)....130
Setting the IP Call....131
Setting the IP Call Service....131
IP Call Example....133
Call Routing....134
Process of Call Routing....135
Regular Expressions....136

Adding a Call Routing Rule....138
Setting the Call Routing Rule for Rejecting....140
Add a Number Filter....141

Managing Accounts....142
User Account, Room System Account and Other Accounts....142
Managing Accounts by Group (Optional)....143
Parameters of User Account and Room System Account....144
Add a User Account....145
Importing a Batch of Accounts....148
LDAP....149
Configuring the LDAP....149
Adding an LDAP Account....152
Setting the Auto Synchronization....153
Enabling Logging into YMS via AD Account with Priority....154
Synchronizing LDAP Accounts....154

Managing Meeting Rooms....154
Entity Meeting Room and the Virtual Meeting Room....155
Managing Meeting Rooms by Groups (Optional)....155
Adding Entity Meeting Rooms....156
Adding a VMR....157
Discussion Mode and Training Mode....159
Sending Emails to VMR Participants....160

Managing Conferences....161
Call Settings....161
Setting the Video and Content Resolution....162
Setting the Call Bandwidth....163
Configuring the Max Video Parties per Conference....163
Configuring the Max Audio-Only Parties per Conference....164
Setting the Time for Joining Conference Beforehand....164
Enabling Auto Dialing....164
Enabling Audio Redialing....165
Enabling Mute Participants upon Entry....165
Setting the Audio Prompt When Participants Join or Leave Conferences....166
Displaying the Native Video....167
Ending the Video Conference Beforehand....167
Setting the Last Participant Backstop Timeout....168
Setting the Auto End Conference Without Moderator....168
Enabling Content Only....169
Setting the Join with APP Awakened by Browser....169
Enabling Receiving Ringtone Receipt....170
Enabling External/Internal Network Access WebRTC Authentication....170
Enabling the Roll Call....170
Setting the App Push Address....171
Setting the QoS....171
Enabling Password for Meet Now Conferences....171
Setting the Default Layout....172
Displaying the Participant Name....173
Displaying Participant Status....174
Displaying the Participant Quantity....174
Displaying the Audio-Only Participant....175

Displaying the Speaker Reminder....175
Setting the Codec....175
Controlling Conferences....176
Monitoring the Conference....177
Going to the Conference Monitoring Page....177
Selecting an Audio Output Device....178
Adjusting the Output Volume....178
Changing the Display Language....178
Configure the Video Images in Equal N×N....179
Setting the Video Carousel....179
Displaying a Participant in a Full Screen/Exiting the Full Screen....179
Scaling the Video Image....180
Hiding/Showing the Conference Video....180
Switching Between the Video Window and the Content Window....180
Displaying the Conference Monitoring Page in a Full Screen/Exiting the Full Screen....180
Deleting Conferences....181
Viewing the Usage of Meeting Rooms....181

Managing Conference Statistics....181
Viewing the MCU Resource....182
Viewing the Conference Statistics....182
Viewing the Call History....183

Managing Devices....183
Prerequisites for the Devices Automatically Connected to YMS....184
Device Status....184
Managing Devices by Groups (Optional)....184
Pushing the Configuration....185
Pushing Firmware....187
Diagnosing Devices....188
Managing T49 Devices....190
Viewing the Statistics of the Executed Tasks....191

Integrating YMS with Other Servers....191
Communicating with the PSTN....192
Setting the PSTN Gateway Service....192
PSTN Example....193
Communicating with Skype for Business Server....194
Communicating with the Local SfB Server....195
Communicating with Microsoft Office 365....198
Communicating with Other Enterprise SfB Servers....202
Setting the SFB Gateway....208
Setting the SfB Gateway Media Service....212
Communicating with Another YMS or Third-Party PBX (Peer Trunk)....212
Setting the Peer Trunk Service....212
Peer Trunk Example....214
Communicating with Another YMS or Third-Party PBX (Registration Trunk)....216
Configuring the REG Trunk Service....216
Registration Trunk Example....217
Setting Alibaba Cloud RTMP Live....218
Configuring the RTMP Media Service....219
Configuring the RTMP Live....219
Setting the RTMP Live for VMRs....220

Enabling Conference Recording (Third-Party Recording Server)..... 221

Immersive TelePresence..... 222

Adding TelePrence Accounts..... 222
Adding TelePresence Meeting Rooms..... 223
Introduction of the TelePresence Recording..... 226
Controlling Conferences..... 227
Going to the Conference Control page..... 228
Muting/Unmuting Participants..... 228
Turning on/off the Video Image..... 228
Removing Participants..... 229
Viewing Call Statistics..... 229
Switching the Roles Between the Moderators and Guests..... 230
Controlling the Remote Camera..... 230
Blocking/Unblocking Audio..... 230
Editing the Site Name..... 231
Inviting Contacts..... 232
Inviting Other Participants..... 232
Inviting Participants by Email..... 232
Sharing the Conference Information..... 232
Searching for Participants..... 233
Moving Participants to the Lobby..... 233
Recording Conferences..... 234
Setting Smart Check-in..... 234
Pausing/Stopping the Recording..... 235
Leaving/Ending a Conference..... 235
Conference Settings..... 235

System Maintenance..... 236

Making Backups and Restoring the Server..... 236
Setting the Auto Backup..... 237
Creating a Backup Manually..... 237
Downloading a Backup..... 237
Restoring the Backup..... 238
Rebooting the System..... 239
Resetting to the Factory..... 239
Viewing Operation Logs..... 240
Exporting System Logs..... 240
Using Tools..... 241
Pinging the Network..... 241
Capturing Packets..... 242

Troubleshooting..... 243

Users Do Not Receive Emails..... 243
Failing to Connect to SMTP..... 244
Users Fail to register an Account..... 244
Failing to Activate a License Online..... 245
Failing to Activate a License Offline..... 245
Loading the Organizational Structure Slowly..... 246
The Configuration of Access WebRTC Authentication Is Invalid..... 246

About This Guide

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

This guide is available to YMS1000, YMS 2000 and YMS3000.

- Targeted Audiences
- Related Documents
- Basic Concepts
- Icon Introduction
- In This Guide
- 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
	TelePresence account, TelePresence meeting room
	Other account
	Video meeting room
	VMR

In This Guide

This guide contains those chapters.

- Chapter 1 Introduction of Yealink Meeting Server
- Chapter 2 Installing and Deploying YMS
- Chapter 3 Getting Started
- Chapter 4 System Setting
- Chapter 5 Managing Services
- Chapter 7 Managing Accounts
- Chapter 10 Managing Meeting Rooms
- Chapter 11 Managing Conferences
- Chapter 12 Managing Conference Statistics
- Chapter 13 Managing Devices
- Chapter 14 Integrating YMS with Other Servers
- Chapter 15 System Maintenance
- Chapter 16 Troubleshooting

Summary of Changes

- Changes for Release 26, Guide Version 26.0.0.15
- Changes for Release 26, Guide Version 26.0.0.10
- Changes for Release 25, Guide Version 25.0.0.10
- Changes for Release 24, Guide Version 24.0.0.20
- Changes for Release 24, Guide Version 24.0.0.10
- 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 26, Guide Version 26.0.0.15

The following section(s) are new for this version:

- Registering Faces (Quick Registration for External Users)
- Enabling Auto Recording

Major updates have occurred to the following section(s):

- Customizing the Theme
- Face Recognition Service
- Adding TelePresence Meeting Rooms

Changes for Release 26, Guide Version 26.0.0.10

The following section(s) are new for this version:

- Ending the Video Conference Beforehand

Major updates have occurred to the following section(s):

- Adding a VMR
- Setting the RTMP Live for VMRs
- Making Backups for Recording Files
- Registering Faces

Changes for Release 25, Guide Version 25.0.0.10

The following section(s) are new for this version:

- Displaying the Speaker Reminder
- Controlling Conferences

Major updates have occurred to the following section(s):

- Customizing the Theme
- Setting the Time Zone
- Adding a VMR
- Parameters of the Recording Template
- Adding a Call Routing Rule
- Pushing the Configuration
- Pushing Firmware
- Resetting to the Factory

Changes for Release 24, Guide Version 24.0.0.20

The following sections are new for this version:

- Sharing Recording Files
- Setting the Codec
- Managing Screenshot Files

Major updates have occurred to the following sections:

- Specifications
- Port Consumption
- Adding a VMR
- Setting the Data Space
- LDAP
- Yealink Recording Service
- Managing the Recording Files
- Yealink Live Service
- Setting Alibaba Cloud RTMP Live

Changes for Release 24, Guide Version 24.0.0.10

The following sections are new for this version:

- Setting the Web Access Port
- Enabling the NTP Service
- Configuring the RTSP Gateway Service
- Face Recognition Service
- Enabling Password for Meet Now Conferences
- Viewing the Statistics of the Executed Tasks
- Immersive TelePresence

Major updates have occurred to the following sections:

- Port Consumption
- Basic Requirements of the Hardware
- Setting the Audio IVR
- Parameters of the Recording Template
- Configuring the LDAP
- Adding a VMR
- Displaying the Participant Name
- Viewing the MCU Resource
- Viewing the Conference Statistics

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
- Port Consumption

Specifications

The specifications are as below:

Features	YMS3000	YMS2000	YMS1000
All-in-One	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		
Conference Capability	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
Broadcasting Interactive Conference	Up to 1,500 parties from External Server		
Additional Audio Calls	40		
Communication Protocols	ITU-T H.323/H.239, IETF SIP/BFCP, RTMP, RDP, RTSP		
Resolution	4K, 1080P, 720P, 360P, 4CIF, CIF		
Video Codecs	H.265, H.264 High Profile, H.264, H.263+, H.263, VP8		
Audio Codecs	Yealink ARES, G.722.1C, G.722.1, G.722, G.711(μ/A), G.729, G.729A, G.729AB, G.728, AAC-LC		
Distributed Architecture	Server Cluster Management & Multi-host Hot Standby		

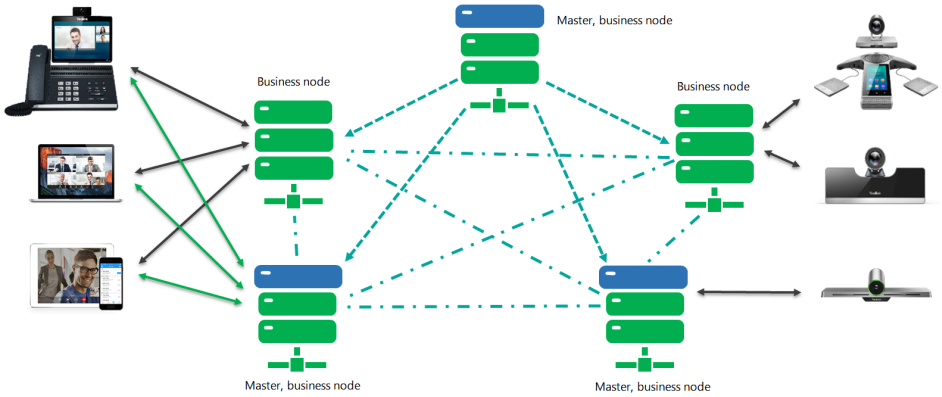
Features	YMS3000	YMS2000	YMS1000
Server Federation	Server Federation Management & Multi-server Cascading		
Expansion	MCU Stack Technology, Cascading Video Conference		
Flexible Layouts	Equal NxN (N=2, 3, 4, 5, 6, 7), onePlusN (N=0, 4, 7, 9, 12, 16, 20), twoPlusN (N=8), Overlay and Selected Speaker		
Recording	Supports 5-way full HD(1080P30) recording with dual stream	Recording, VOD(Video on Demand) and Management	
Face recognition service	Identify the participant through the external server		
Other Functions	RTMP Live, Audio IVR, Display Native Video and Content, Display audio parties, Chat in Conference		
Bandwidth Dynamic Adaptive Adjustment	Anti 30% video and70% audio packet loss, QoS		
Security Protocols	TLS, SRTP, HTTPS, SSH, H.235, AES-256bit		
Firewall Traversal	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.		
Multiple Conferencing Methods	P2P Call, Meet Now, Ad Hoc, Scheduled Conferencing, VMR		
Multiple Conference Modes	Training Mode, Discussion Mode and Lecturer View		
Integration with Yealink VC Endpoints	Sync Conference Information, Conference Reminder, One-touch Conference Access, Apply for Speaking		
Conference Control	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		
Personal Layout	Voice Activated Speaker, Video Carousel, Customized Layout and Application Parties		
User Account	Organizational Structure and up to 100,000accounts		
Enterprise Directory	Synchronize directory to the device		
LDAP	Synchronize directory from Microsoft AD Server		
Third-party Device Registration	SIP/H.323		
Traversal Features	ICE/TURN/STUN/NAT/H.460		
Web Management	Friendly Web UI and Setup wizard		
Customization	Web & Logo, Email Template, Audio IVR and SIP Trunk IVR		

Features	YMS3000	YMS2000	YMS1000
System Status Monitoring	Web-based real-time dashboard & data update on capacity and system information		
Resource Statistics Management	Graphic display and statistics & analysis of conferences, MCU resources and CDR		
System Maintenance Management	Remote Upgrade, Backup/Restore, Reboot/Factory Reset and Syslog, Network Ping, Packet Capture, SNMP		
System Security Management	Blacklist, Whitelist and Intelligent Security Strategy		
Device Remote Management	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 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.

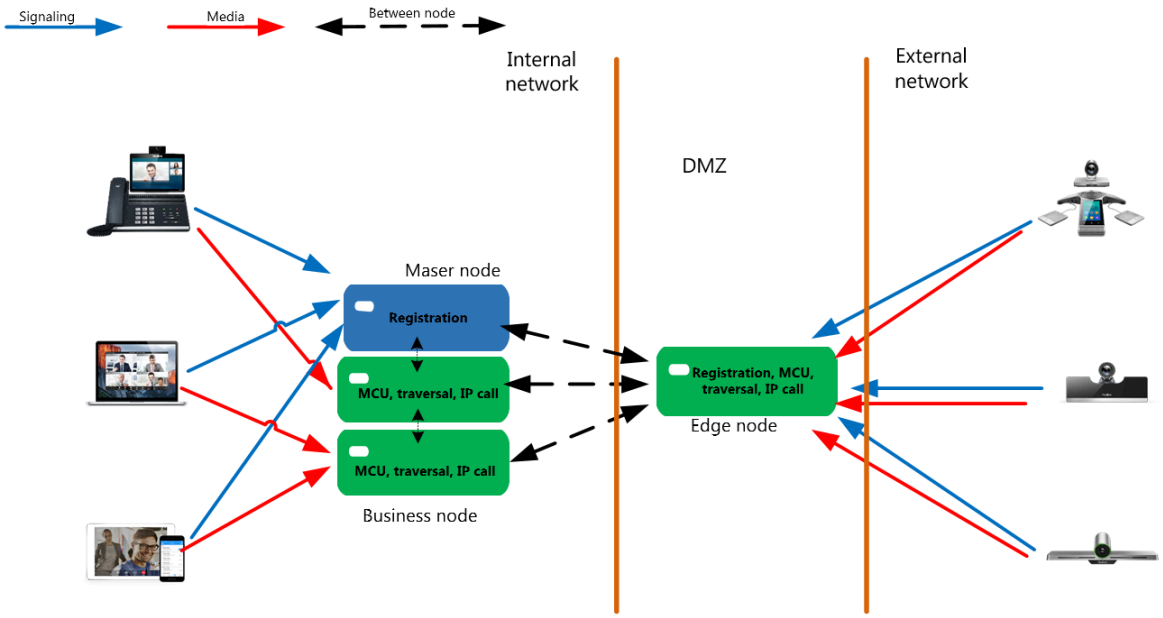
Business node: those nodes mainly provide services, for example, SIP service, H.323 service, and MCU service. You can configure and add business nodes via the web interface. You can also enable and disable these services via the web interface. Especially for the MCU service that calls for higher hardware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

Port	Protocol	Description
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	It is used by YMS for collating the device log
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	

Module	Port	Protocol	Description
	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
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
61000-62999		UDP	RTSP gateway service
IVR port	10000-10999	UDP	IVR
BFCP/FECC port	11000-12999	UDP	BFCP/FECC
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
Face recognition service port	65100-65499	UDP	Face recognition service

Port Consumption

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

Table 5: Port Consumption

No.	Situation		Video ports (License)	Other ports (License)	Compared to the resource consumed by a single HD 720p call	Compared to the resource consumed by a single HD 720p call
					720P	1080P
1	Broadcasting interactive conference	When no participant joins the conference	N/A	N/A	N/A	N/A
		When a broadcasting participant joins the conference	2	1 broadcast port	1/23	2/23
		When an interactive participant joins the conference	1	N/A	1	2
2	Alibaba Cloud RTMP Live	Enable Alibaba Cloud RTMP live	2	N/A	2	3
		When one participant watches the webcast	N/A	1 live port	N/A	N/A
3	Yealink RTMP live	Enable Yealink RTMP live	2	N/A	2	3
		When one participant watches the webcast	N/A	1 live port	N/A	N/A
4	Each time you stream the conference to the live streaming platform by RTMP		1	N/A	1	2
5	Each time you record the conference		1	1 recording port	1	2

No.	Situation	Video ports (License)	Other ports (License)	Compared to the resource consumed by a single HD 720p call	Compared to the resource consumed by a single HD 720p call
				720P	1080P
6	Each time you invite a media stream from other servers by RTSP	1	1 RTSP port	1	2
7	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)	1	N/A	Bypass disabled: 3; Bypass enabled: 1	Bypass disabled: 6; Bypass enabled: 2
8	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)	1	N/A	Bypass disabled: 3; Bypass enabled: 1	Bypass disabled: 6; Bypass enabled: 2
9	Establish a SfB call	1	N/A	3 (Bypass not supported)	6 (Bypass not supported)
10	A YMS user joins a SfB conference	1	N/A	3 (Bypass not supported)	6 (Bypass not supported)
11	A Lync user joins a YMS conference	1	N/A	3 (Bypass not supported)	6 (Bypass not supported)
12	Invite a user to join the conference via IP call (IVR/URL/IP)	1	N/A	Bypass disabled: 3; Bypass enabled: 1	Bypass disabled: 6; Bypass enabled: 2
13	An H.323 user joins the conference	1	N/A	Bypass disabled: 3; Bypass enabled: 1	Bypass disabled: 6; Bypass enabled: 2
14	An H.323 user calls a SIP user or a SIP user calls an H.323 user	1	N/A	3 (Bypass not supported)	6 (Bypass not supported)

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	√		√	√	√	Good to Know about the Hardware
Making a Backup on YMS 1.4	√					Making a Backup on YMS 1.4
Uninstalling YMS 1.X	√					Uninstalling YMS 1.4
Checking the Version of CentOS	√		√	√	√	Checking the Version of CentOS
Configure the Node IP	√	√	√	√	√	Configuring the Node IP
Installing YMS 2.X	√		√	√	√	Installing YMS 2.X
Migrating the data on YMS	√					Migrating the Data on YMS
Activating a License	√	√	√	√	√	Activating a License
The network of YMS 2.X and the basic configuration	√	√	√	√	√	Getting Started
The Checklist for the Configurations and the Common Features	√	√	√	√	√	The Checklist for the Configurations and the Common Features

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 you install YMS, your hardware should meet the following requirements.

Table 6: Basic Requirements of the Hardware

Item	Requirement
CPU	E5-2600 V3/V4 with frequency as 2.3GHz
RAM	• 32G • The memory frequency should be 2133MHz at least • For the physical machine, 2 GB RAM for one core, using multi-channel memory architecture and multi-memory with small capacity • For the virtual machine, 1 GB RAM for one core. For the host machine, you can use multi-channel memory architecture and multi-memory with small capacity **Note:** • Each E5 CPU should be assigned with 4 channels of 8G RAM. The RAM frequency of E5 V3 and E5 V4 should be 2133MHz and 2400MHz respectively. • Each Silver/Gold CPU should be assigned with 6 channels of 8G RAM. The RAM frequency of the Silver and Gold CPU should be 2400MHz and 2666MHz respectively.
Network	1 Gbps NIC or switches
Disk	**Stand-alone deployment:** The total disk space should be 500G at least, and the details are as below: • /home: 300GB • /usr/local: 150GB • /var: 50GB **Cluster deployment:** The disk space for each master node should be 500G at least, and the details are as below: • /home: 300GB • /usr/local: 150GB • /var: 50GB The disk space for each business node should be 200G at least, and the details are as below: • /home: 50G • /usr/local: 100GB • /var: 50G **Note:** When the first time you install YMS, the system will automatically check your hardware. If your hardware cannot meet the requirement, you cannot install YMS.

Calculating Method for the Concurrent Capacity

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

  Concurrent capacity of 720p = total number of cores * frequency * 1.2

  Concurrent capacity of 1080p = total number of cores * frequency * 0.6
- **For the virtual machine, you can refer to the following:**

  Concurrent capacity of 720p = total number of Vcores * frequency * 0.6

  Concurrent capacity of 1080p = total number of Vcores * frequency * 0.3

Recommended Hardware

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

CPU Model	Frenquency	Total Number of Vcores	RAM	Concurrent Capacity (Video + Content sharing + 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:

- The number of VCPU is the number you assign to the VMware rather than the number of the whole CPU.
- 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.

- If you use Intel E5 to install CentOS and then install YMS 2.0, you can refer to the following recommendations.

CPU Model	Frenquency	Total Number of CPUs	Total Number of Cores	RAM	Concurrent Capacity (Video + Content sharing + 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

Note: Each E5 CPU should be assigned with 4 channels of 8G RAM. The RAM frenquency of E5 V3 and E5 V4 should be 2133MHz and 2400MHz respectively.

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

CPU Model	Frenquency	Total Number of CPUs	Total Number of Cores	RAM	Concurrent Capacity (Video + Content sharing + 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

Note: Each Silver / Gold CPU should be assigned with 6 channels of 8G RAM. The RAM frenquency of the Silver and Gold CPU should be 2400MHz and 2666MHz respectively.

Network Requirements

Table 7: Network Requirements

Item		Requirements
Bandwidth	1080P60fps (1920x1080)	4M
	1080P60fps (1920x1080) video 1080P30fps (1920x1080) content	6M
	1080P30fps (1920x1080)	1.7Mb
	1080P30fps (1920x1080) Video + content	3.4Mb
	720P30fps (1280x720)	700Kb
	720P30fps (1280x720) Video + 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

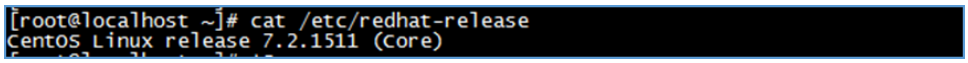
If the YMS cannot access the external network, we recommend that you use CentOS 7.5 or later. If it can access the external network, you can use CentOS 7.0 or later.

- 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*.



Upgrading CentOS Online

Before you begin

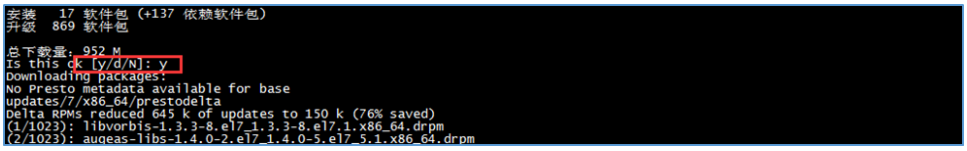
The server can access the external network.

Procedure

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

2. Run the command *yum update* to update the yum package.

   The whole upgrading process might take a long time. Please wait.



   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

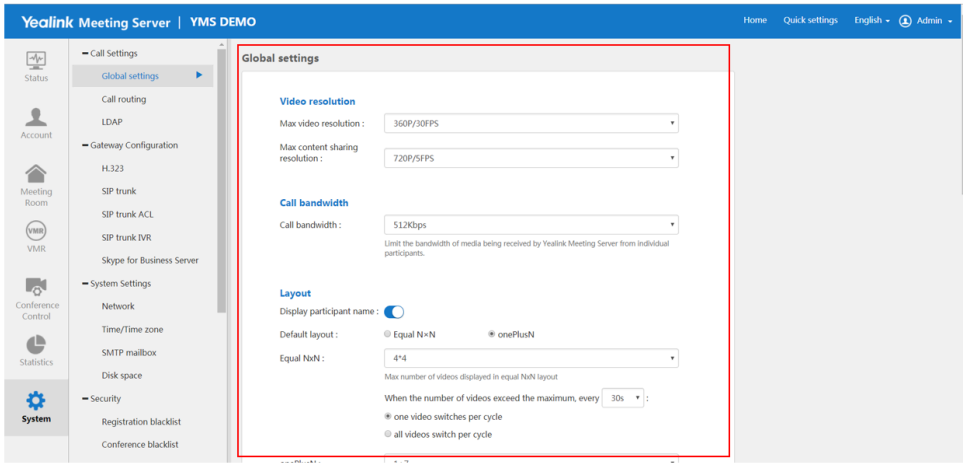
- Saving the Data by Screenshot
- Exporting All Call Statistics
- Making a Backup for the System Data

Saving the Data by Screenshot

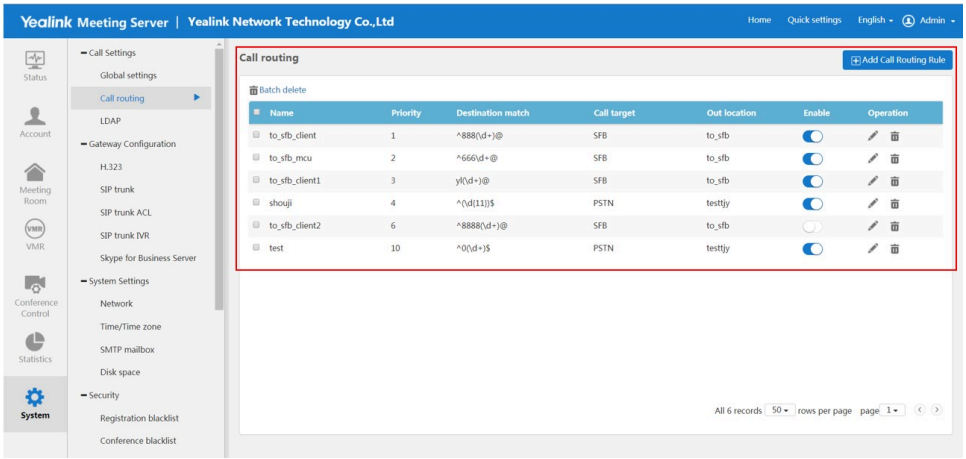
From Version 2.X, the structure of YMS has changed. Therefore, the data migration is not available. You can save the following configuration by taking screenshots.

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

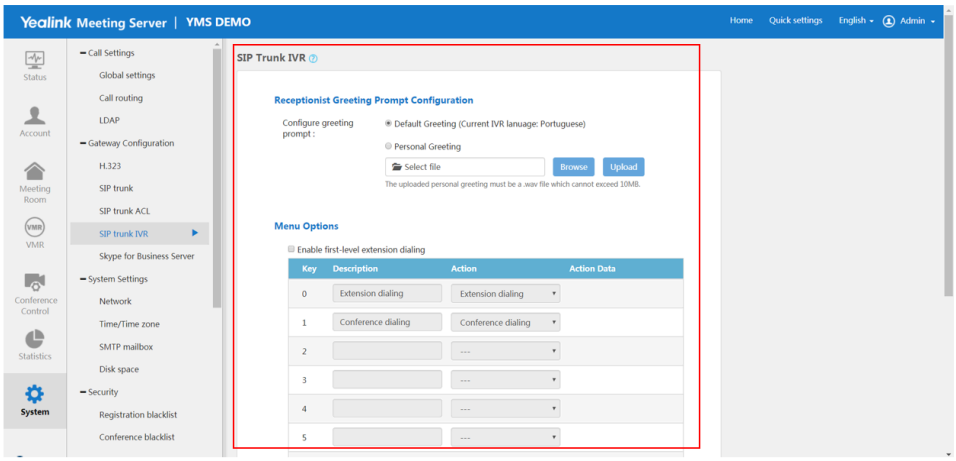
- Click **System**->**Call Settings**->**Global settings**, and take screenshots of the entire configuration.



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



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



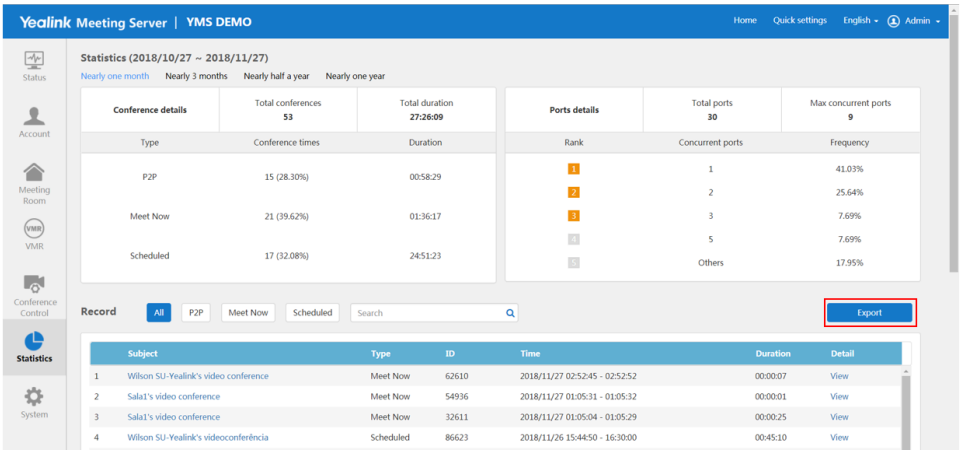
Exporting All Call Statistics

About this task

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

Procedure

Click **Statistics** > **Export**.



Making a Backup for the System Data

About this task

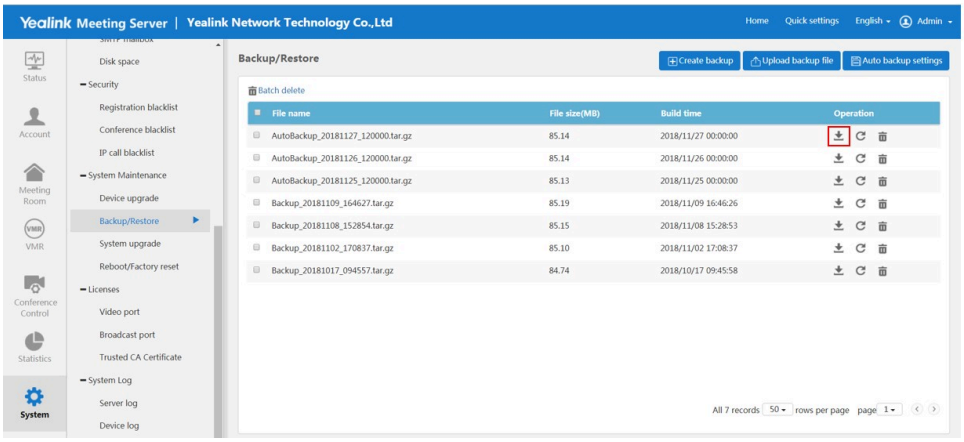
Log into YMS 1.X, and do the following:

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

Procedure

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

2. Click [redacted] on the right side of the created backup to download it to your computer.



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
Installing Stand-Alone YMS	A single YMS but with all services.
Installing Cluster YMS	Multiple YMSs, including the following node types: • **Master node**: it provides all the YMS services. • **Sub-master node**: if you want to realize the disaster recovery for all features, it must contain 2 sub-master nodes. • **Business node**: you can assign the desired service, mainly the MCU service, to each business node according to the enterprise deployment need.

- 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:

     ```
     wget address    # It is the address for downloading the installation package (you can obtain the address from Yealink technical support engineers) to #
     ```

- **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 desired installation 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.el7        libtommath.x86_64 0:0.42.0-6.el7
     sshpass.x86_64 0:1.06-2.el7

   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:

     ```
     wget address    # It is the address for downloading the installation package (you can obtain the address from Yealink technical support engineers) to #
     ```

- **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 desired installation package on the pop-up window.

Unzipping the Installation Package

Procedure

Run the following command:

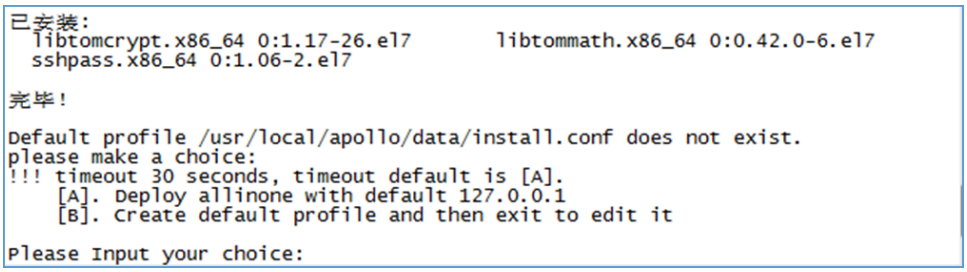
```
cd /usr/local                    #go to the directory where the installation package is in#
tar xzf YMS_x.x.x.x.tar.gz       # unzip the installation package (change x.x.x.x to the version you want to install)#
cd apollo_install                # go to the installation directory#
tar xzf install.tar.gz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

Run the Installation Command

Procedure

1. Run the following command:

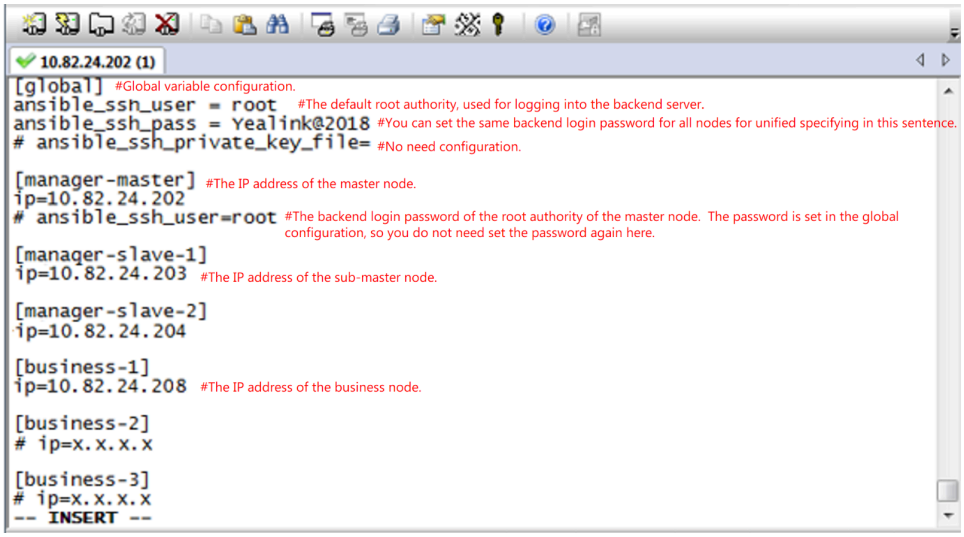
```
./install.sh
```



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.



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

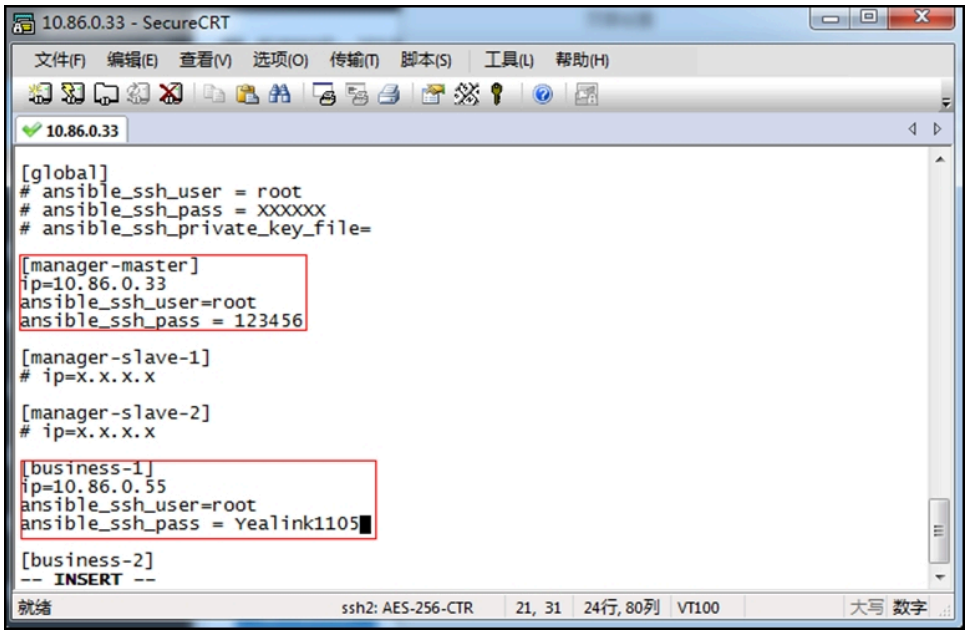
- The network among all the nodes can be accessed. All the nodes can access the external network.
- YMS is not installed in all the nodes.

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.



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.

Uninstalling YMS 2.X

About this task

Note: Generally, you do not need to uninstall YMS 2.X. If you need to uninstall it, 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 *apollo-uninstall* to uninstall the script.
   For the cluster deployment, you need to run the uninstalling command on every node.
3. 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

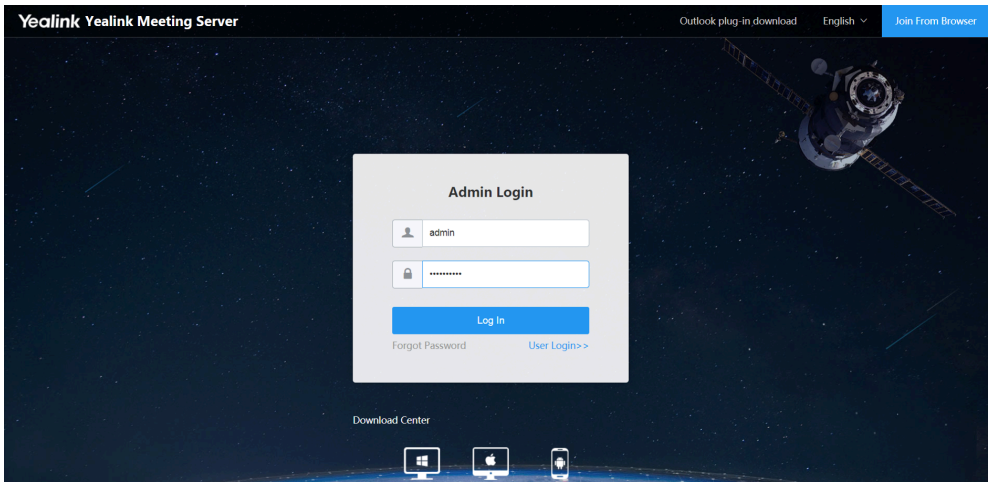
Logging into YMS

Procedure

1. 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.

2. Click **Admin Login**, enter the username and the password to log in.

   By default, the username is admin and the password is 123456yl. If it is the first time you log into YMS, you are required to change the password.



Setting the Setup Wizard

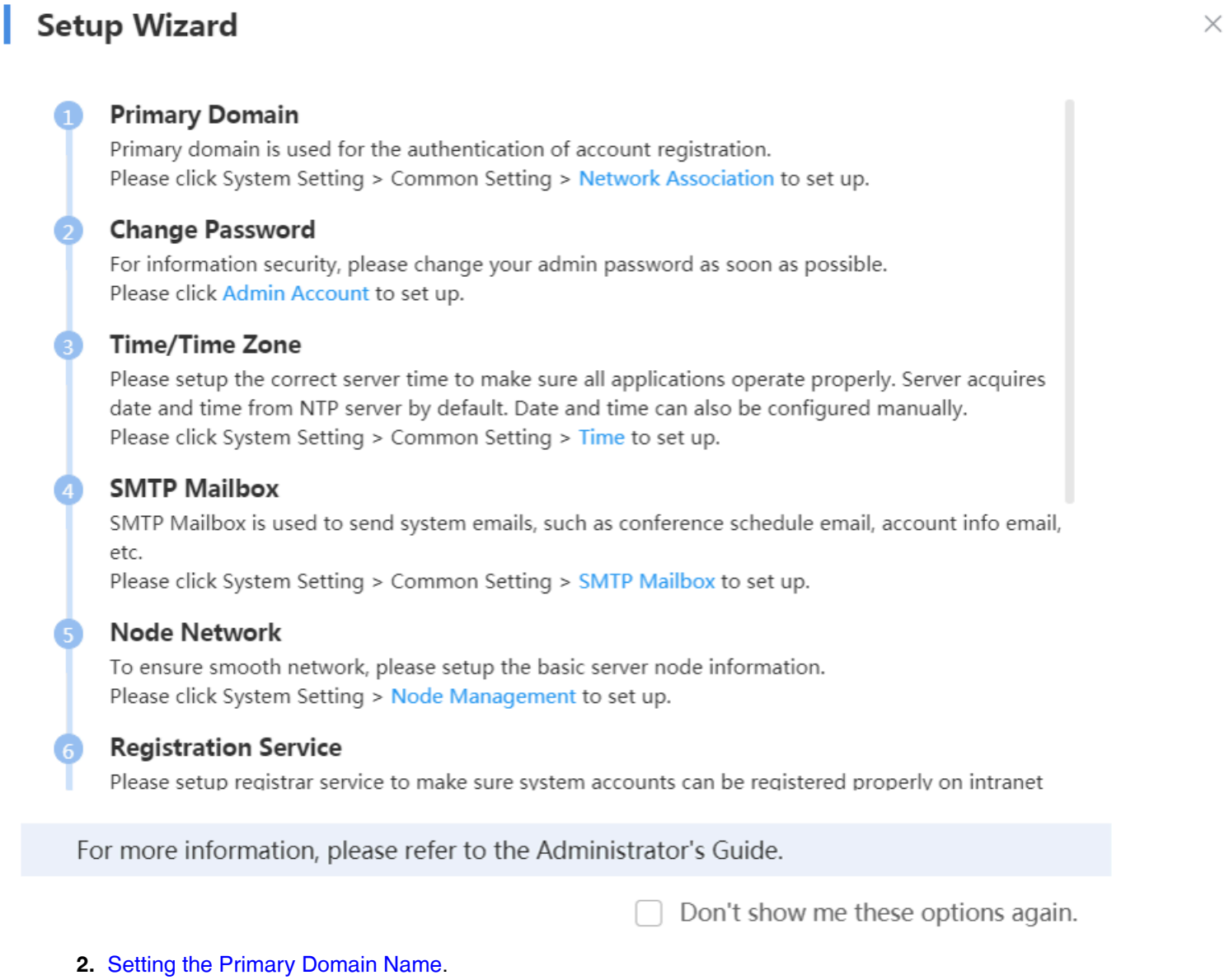
To meet the necessary call and conference need, you can configure the server according to the setup wizard.

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.



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

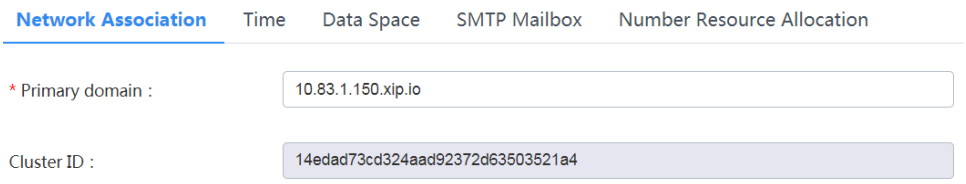
Setting the Primary Domain Name

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.

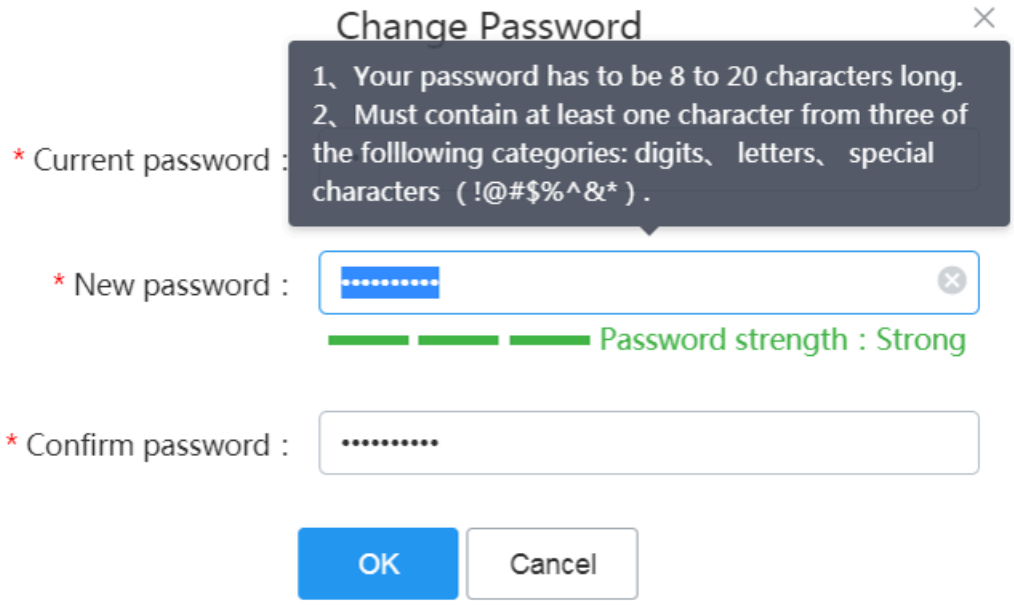


Editing the Login Password

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.



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.

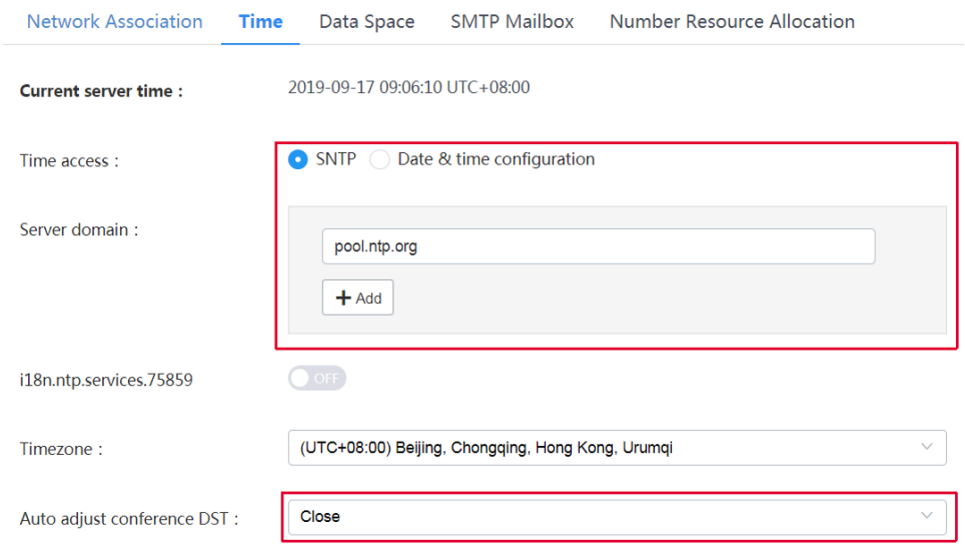


Table 8: Time parameter

Parameter	Description
Time access	Select the desired method to obtain the system time. • **SNTP** • **Date & time configuration** **Default**: SNTP.
Server domain	If you select **SNTP**, configure the SNTP server. **Note**: the first server address is the primary server by default, and its default value is pool.ntp.org.
NTP Service	
Date & time	If you select **Date & time configuration**, configure the time and date manually.

Parameter	Description
Auto adjust conference DST	Configure the DST type. • **Enabled**—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. • **Close**—DST is disabled. **Default**: disabled.

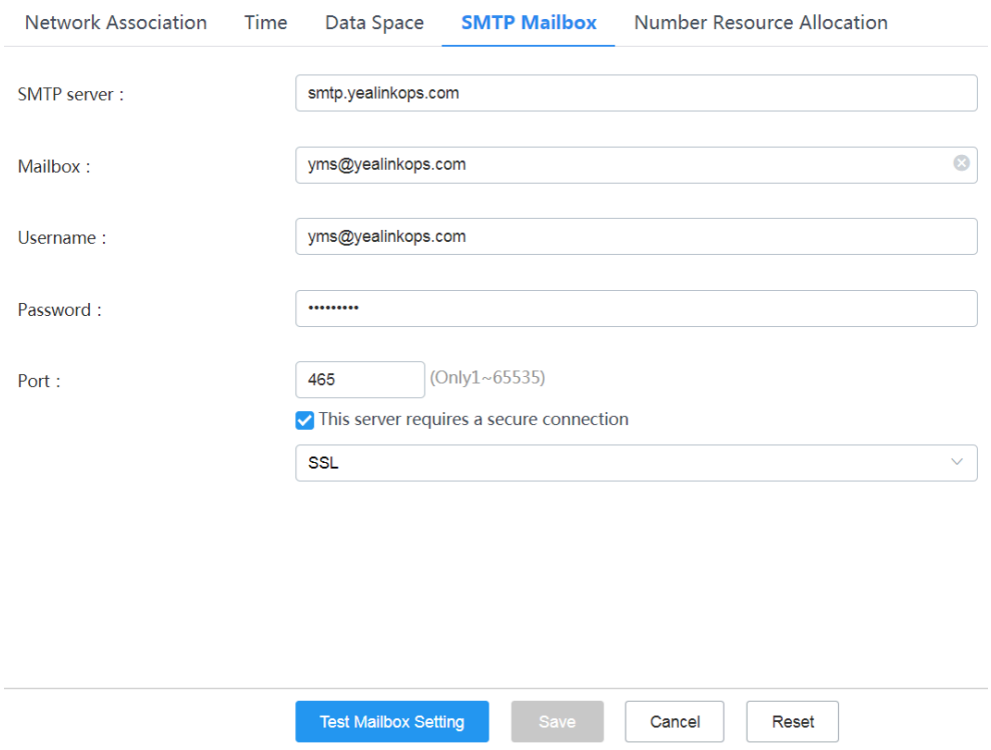
3. Save the configuration and the system reboots.

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.



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.

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.

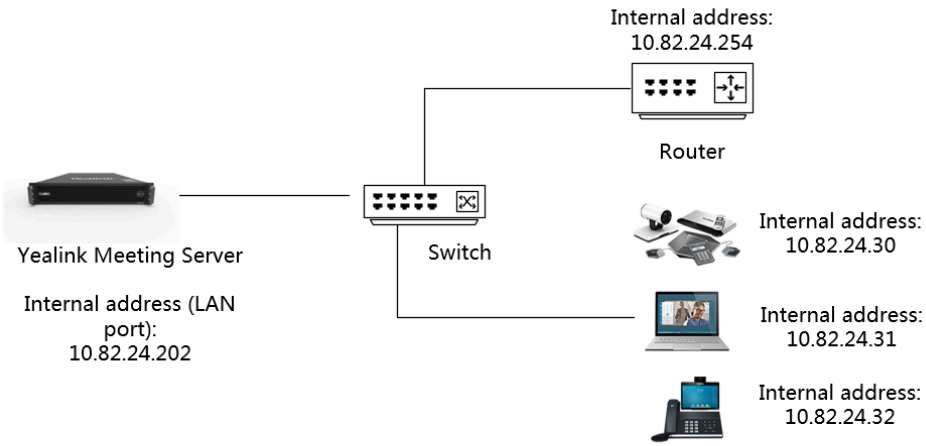
Go to the page of Address Port Mapping:

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)

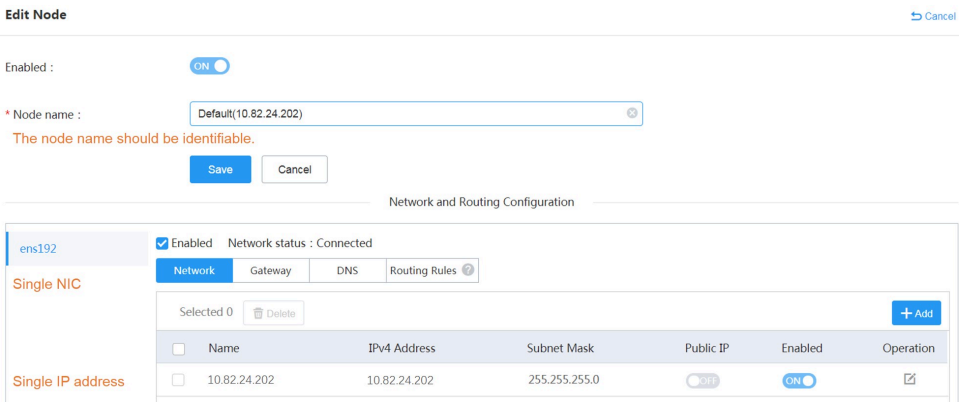
Internal Deployment with One-IP NIC

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.

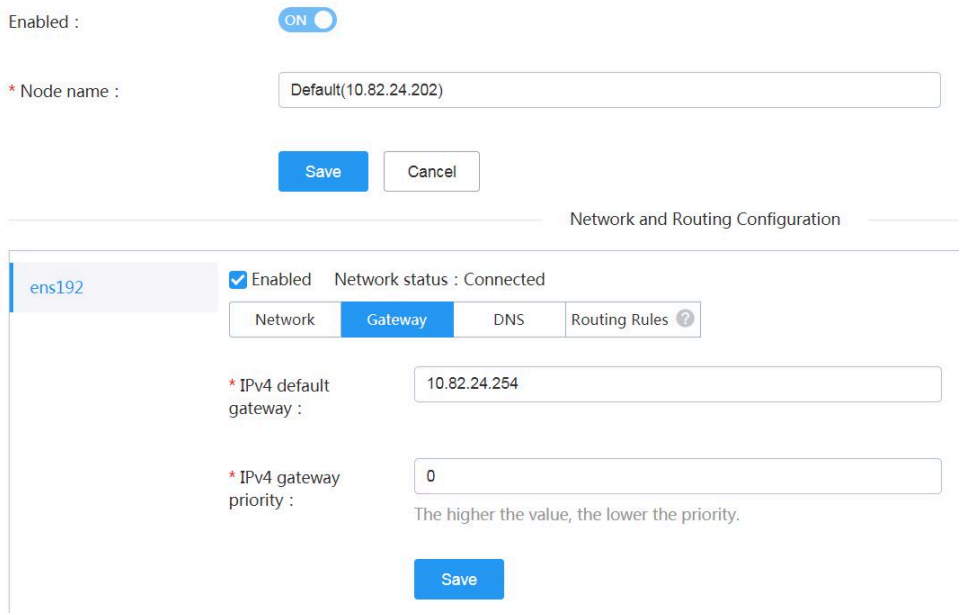


Go to the page of Node Management, and check the following configuration:

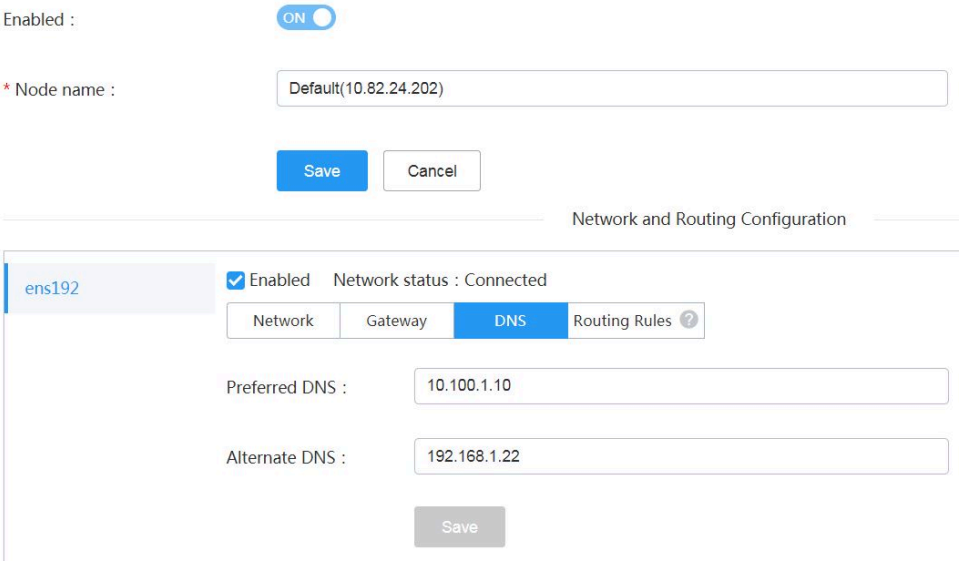
- **Network**



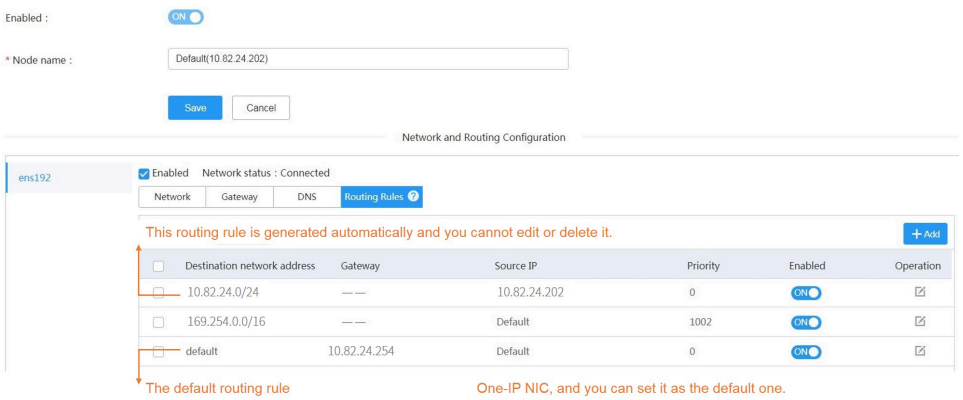
- **Gateway**



- **DNS**

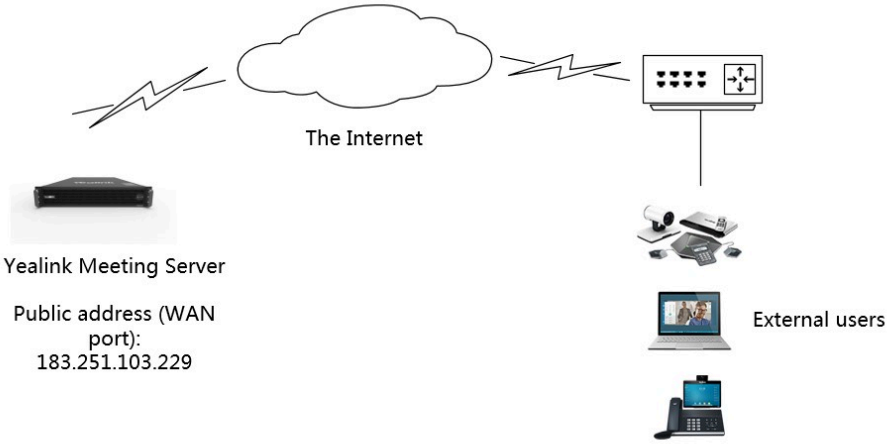


- **Routing Rules**



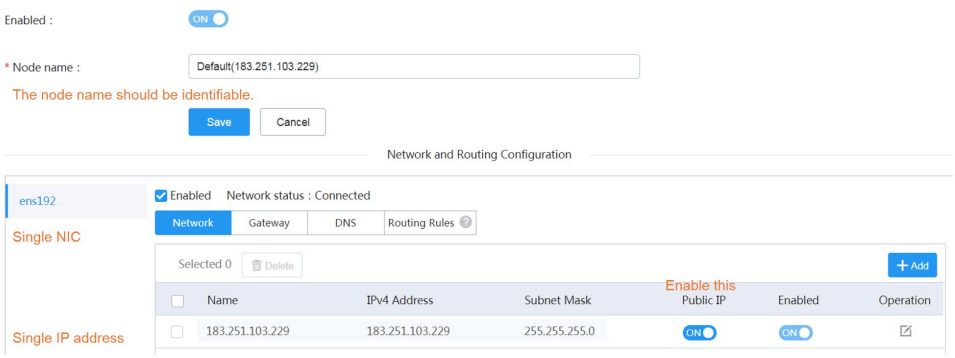
External Deployment with One-IP NIC

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.

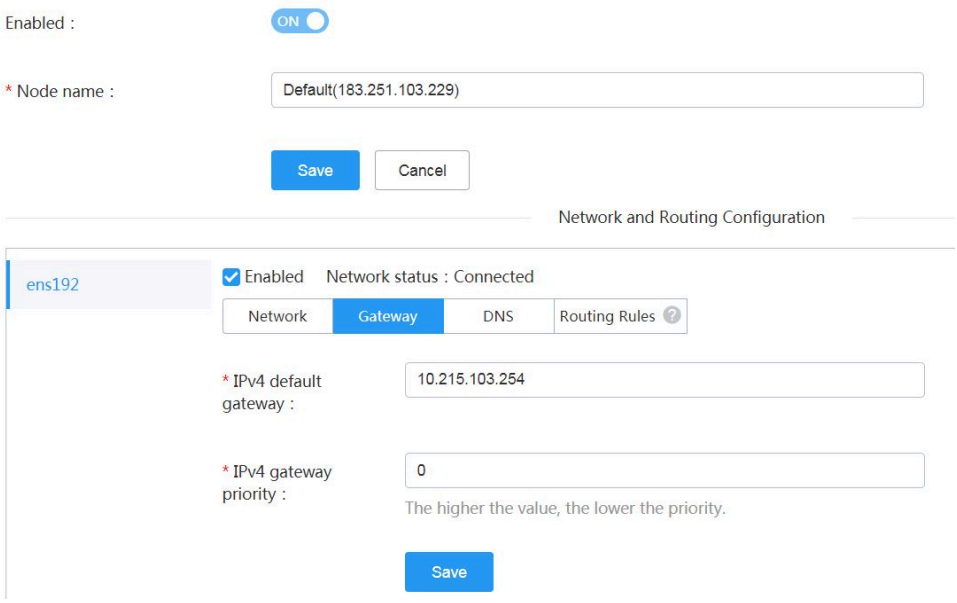


Go to the page of Node Management, and check the following configuration:

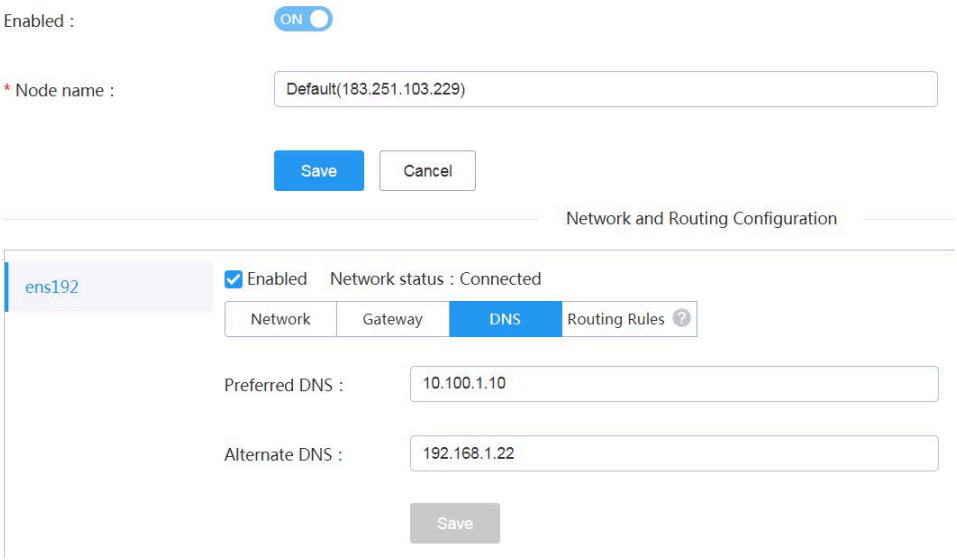
- **Network**



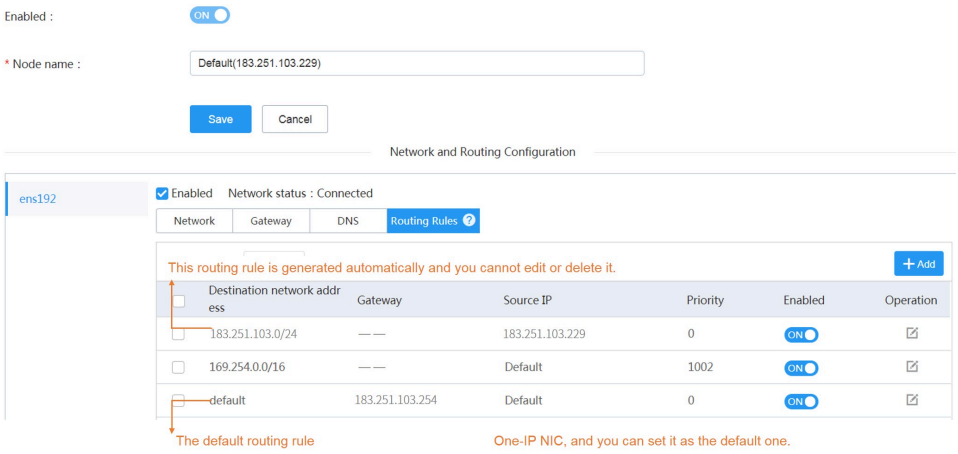
- **Gateway**


Enabled :
ON
* Node name :
Default(183.251.103.229)
Save
Cancel
Network and Routing Configuration
ens192
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
* IPv4 default gateway :
10.215.103.254
* IPv4 gateway priority :
0
The higher the value, the lower the priority.
Save

- **DNS**


Enabled :
ON
* Node name :
Default(183.251.103.229)
Save
Cancel
Network and Routing Configuration
ens192
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
Preferred DNS :
10.100.1.10
Alternate DNS :
192.168.1.22
Save

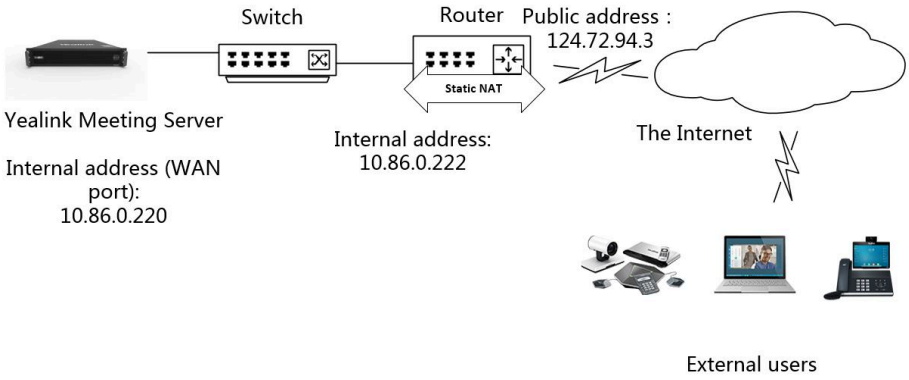
- **Routing Rules**



External Deployment with One-IP NIC (with NAT)

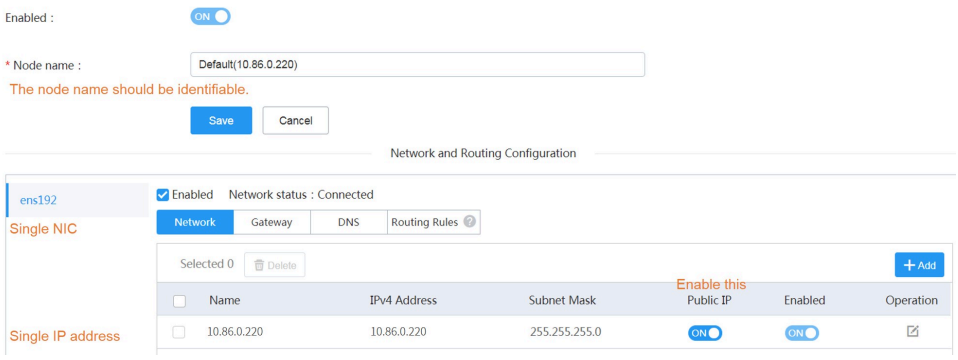
To secure YMS and the internal network, you can deploy YMS in the internal network and map the address by static NAT on the router and YMS. Therefore, users in the external network can access YMS.

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

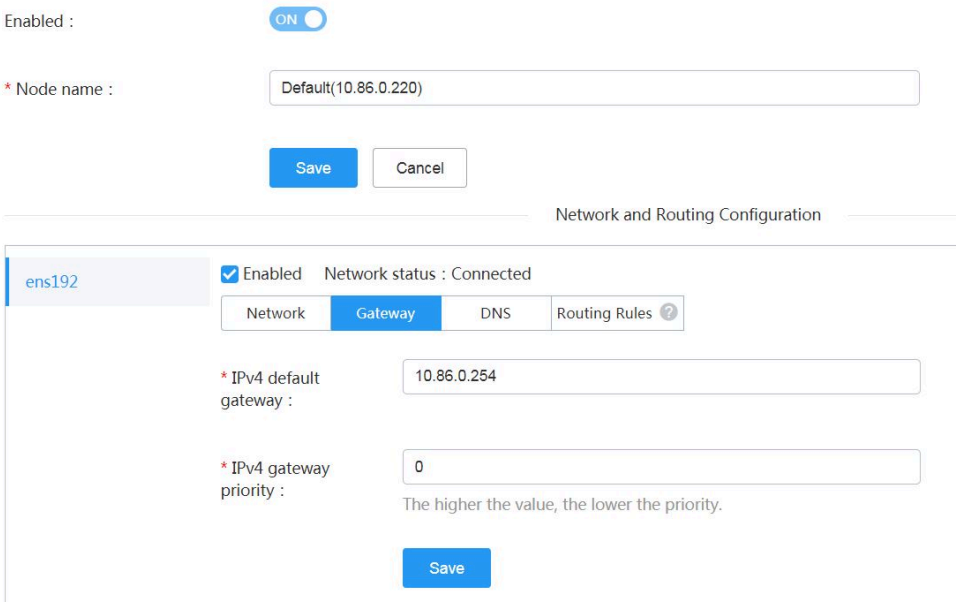


Go to the page of Node Management, and check the following configuration:

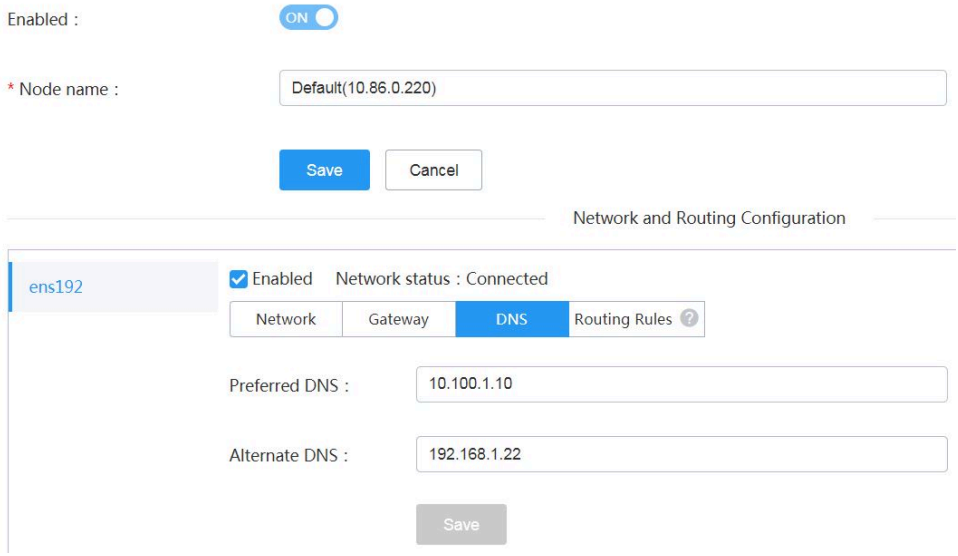
- **Open the external service port in Port Requirements of the Router.**
- **Network**



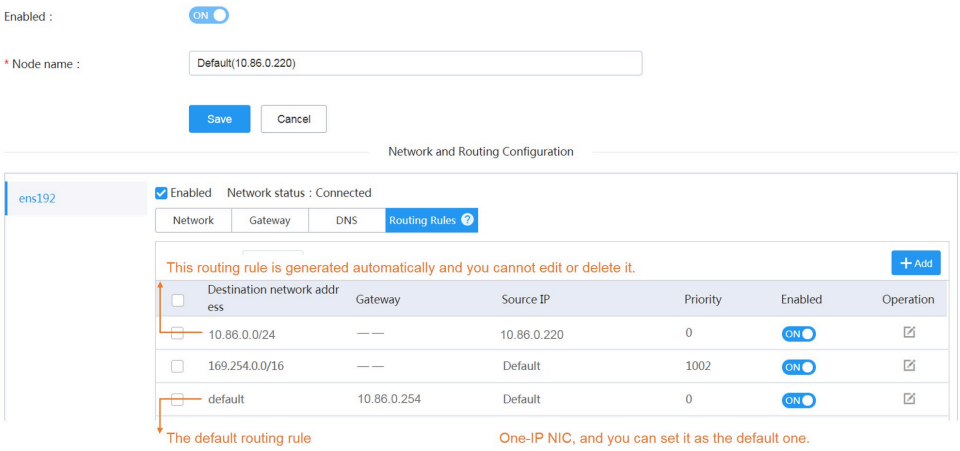
- **Gateway**


Enabled :
ON
* Node name :
Default(10.86.0.220)
Save
Cancel
Network and Routing Configuration
ens192
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
* IPv4 default gateway :
10.86.0.254
* IPv4 gateway priority :
0
The higher the value, the lower the priority.
Save

- **DNS**


Enabled :
ON
* Node name :
Default(10.86.0.220)
Save
Cancel
Network and Routing Configuration
ens192
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
Preferred DNS :
10.100.1.10
Alternate DNS :
192.168.1.22
Save

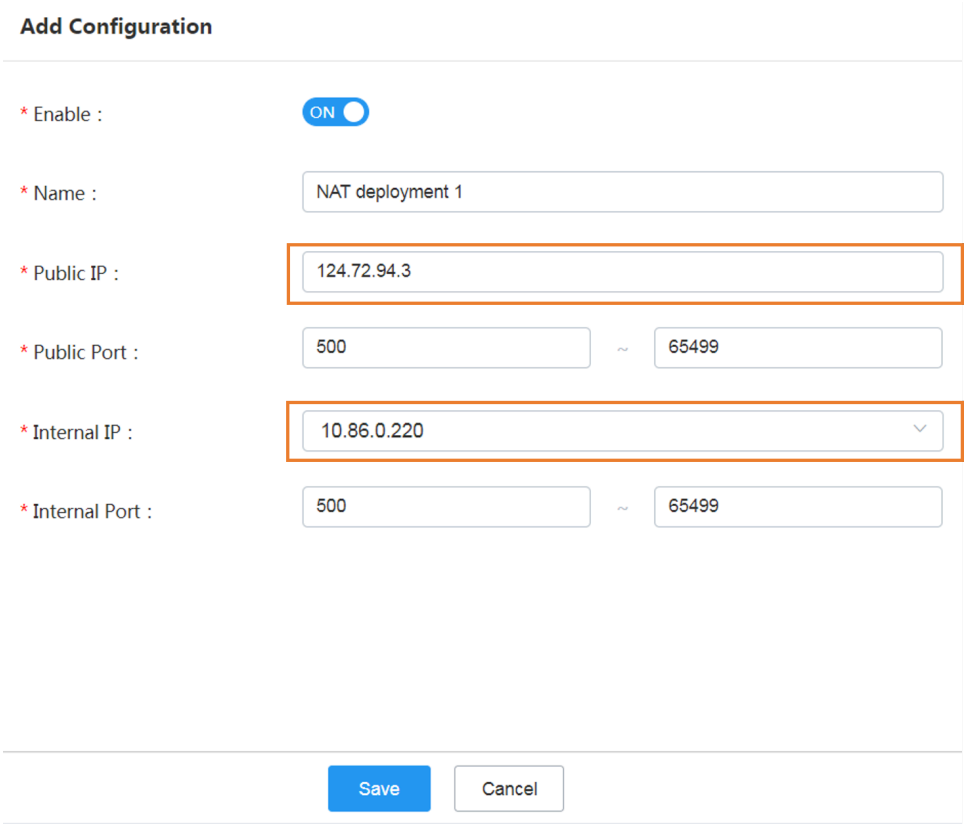
- **Routing Rules**



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

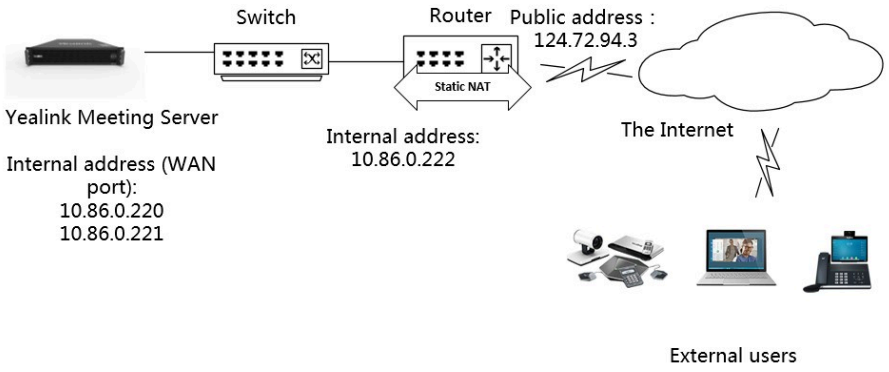
- **Address Port Mapping**

  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.



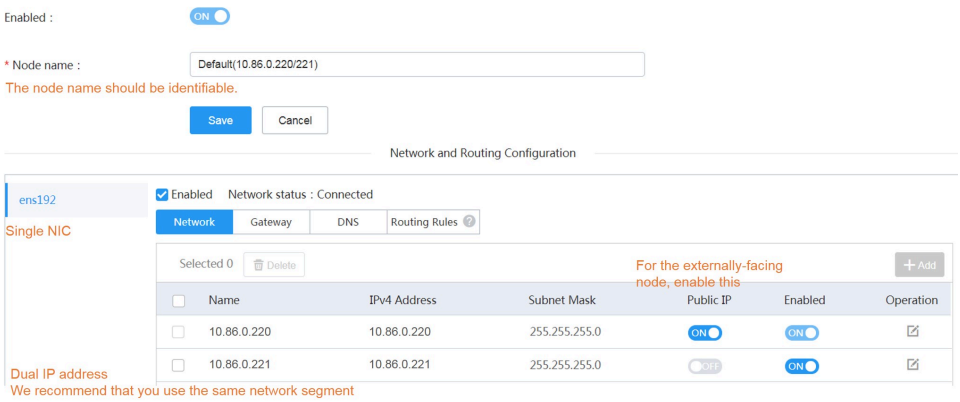
Internal and External Deployment with Dual-IP NIC (with NAT)

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.

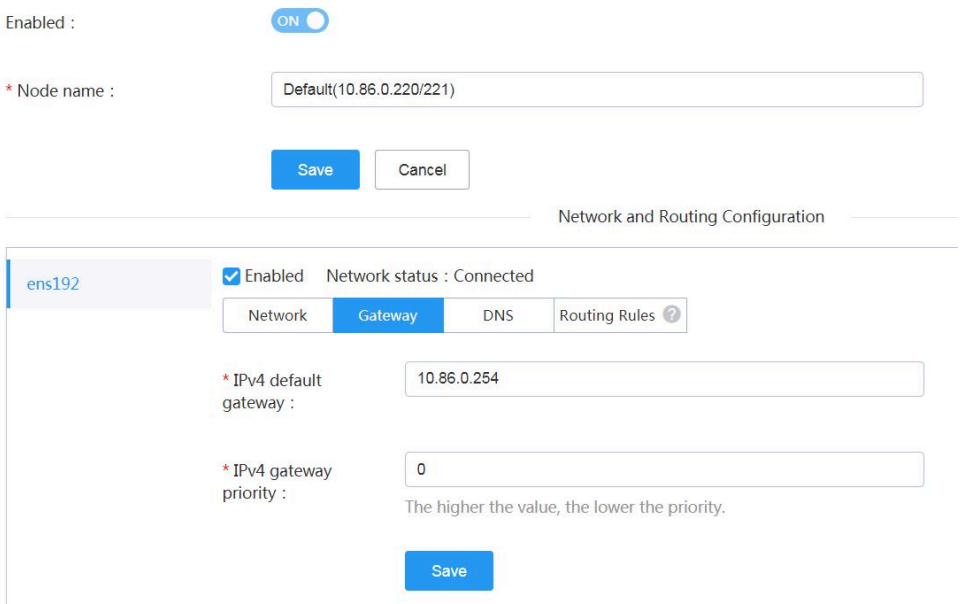


Go to the page of Node Management, and check the following configuration:

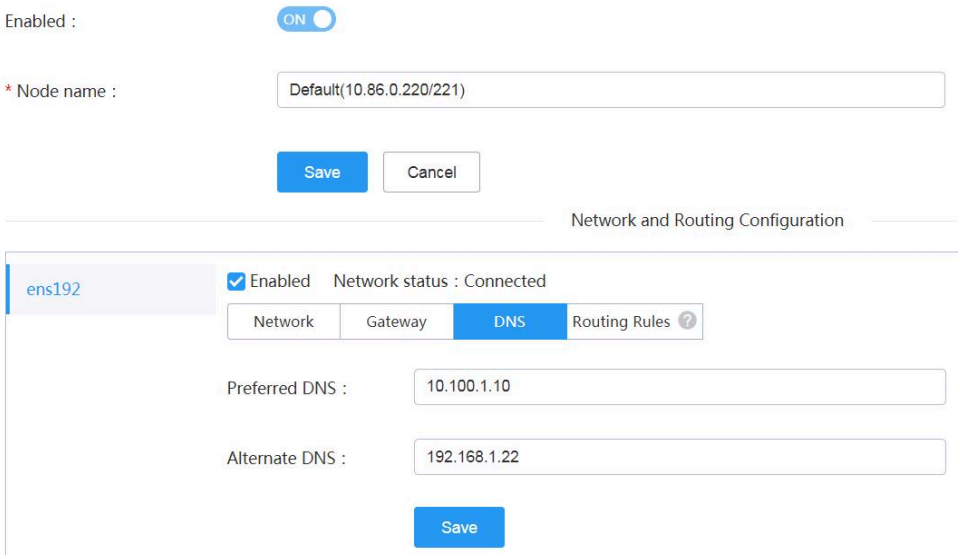
- **Open the external service port in Port Requirements of the Router.**
- **Network**



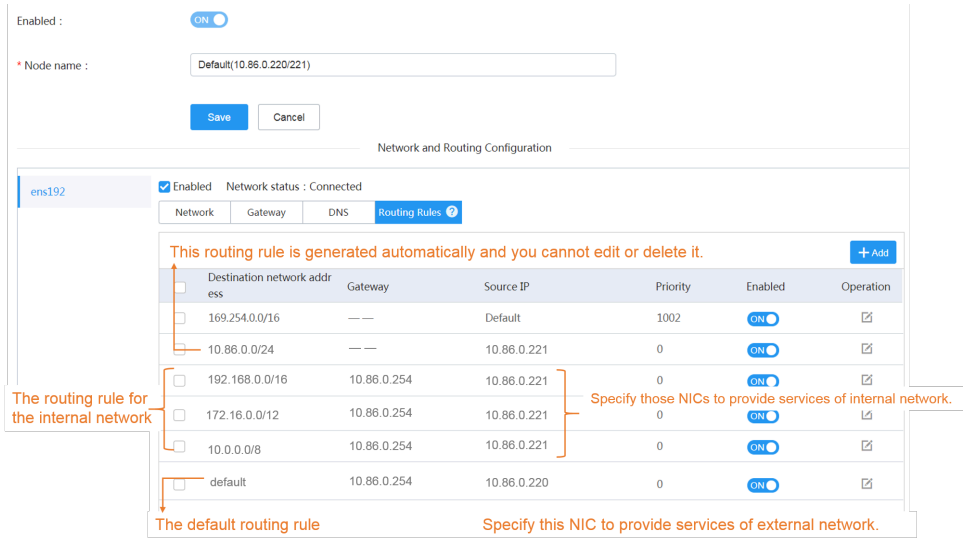
- **Gateway**



- **DNS**



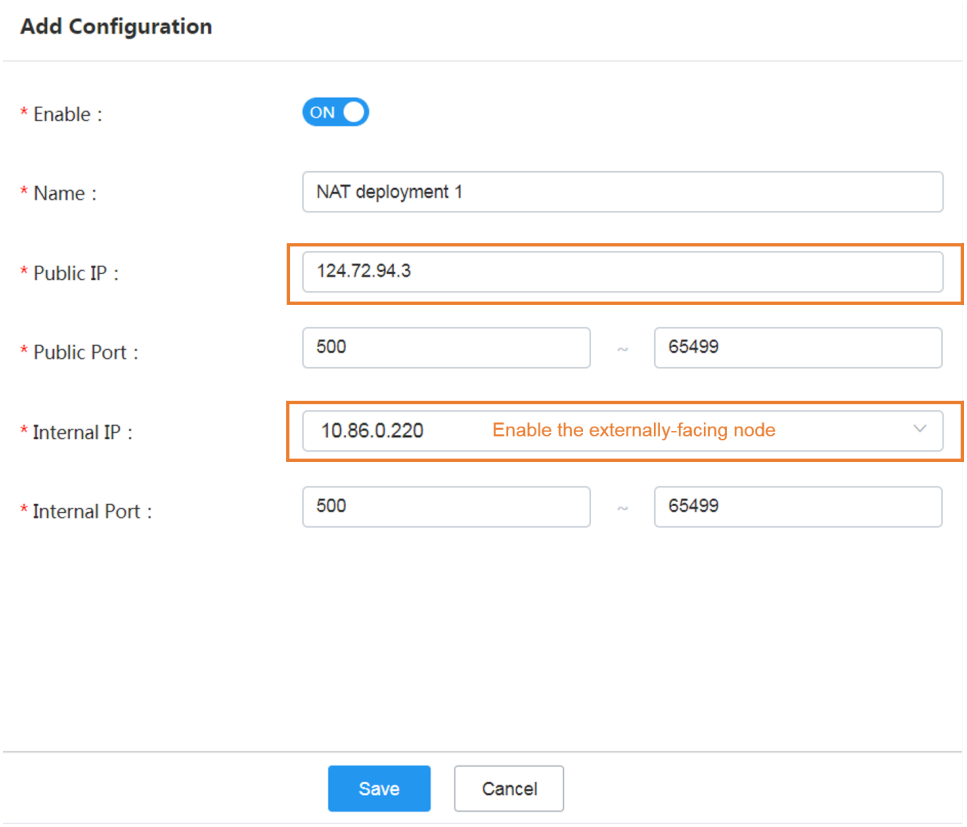
- **Routing Rules**



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

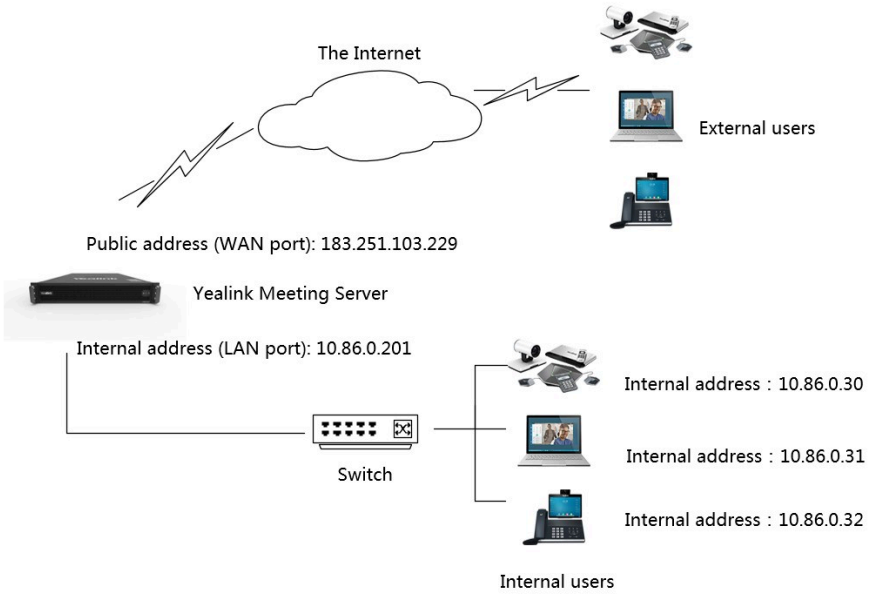
- **Address Port Mapping**

  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.



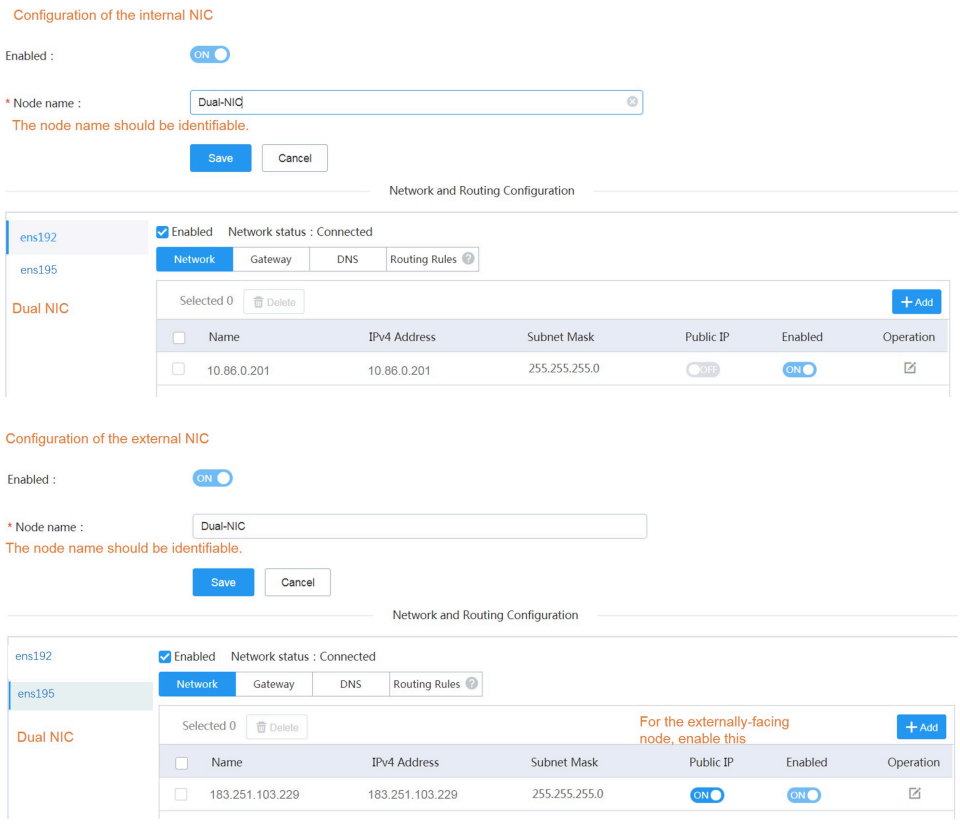
Internal and External Deployment with Dual NIC

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.

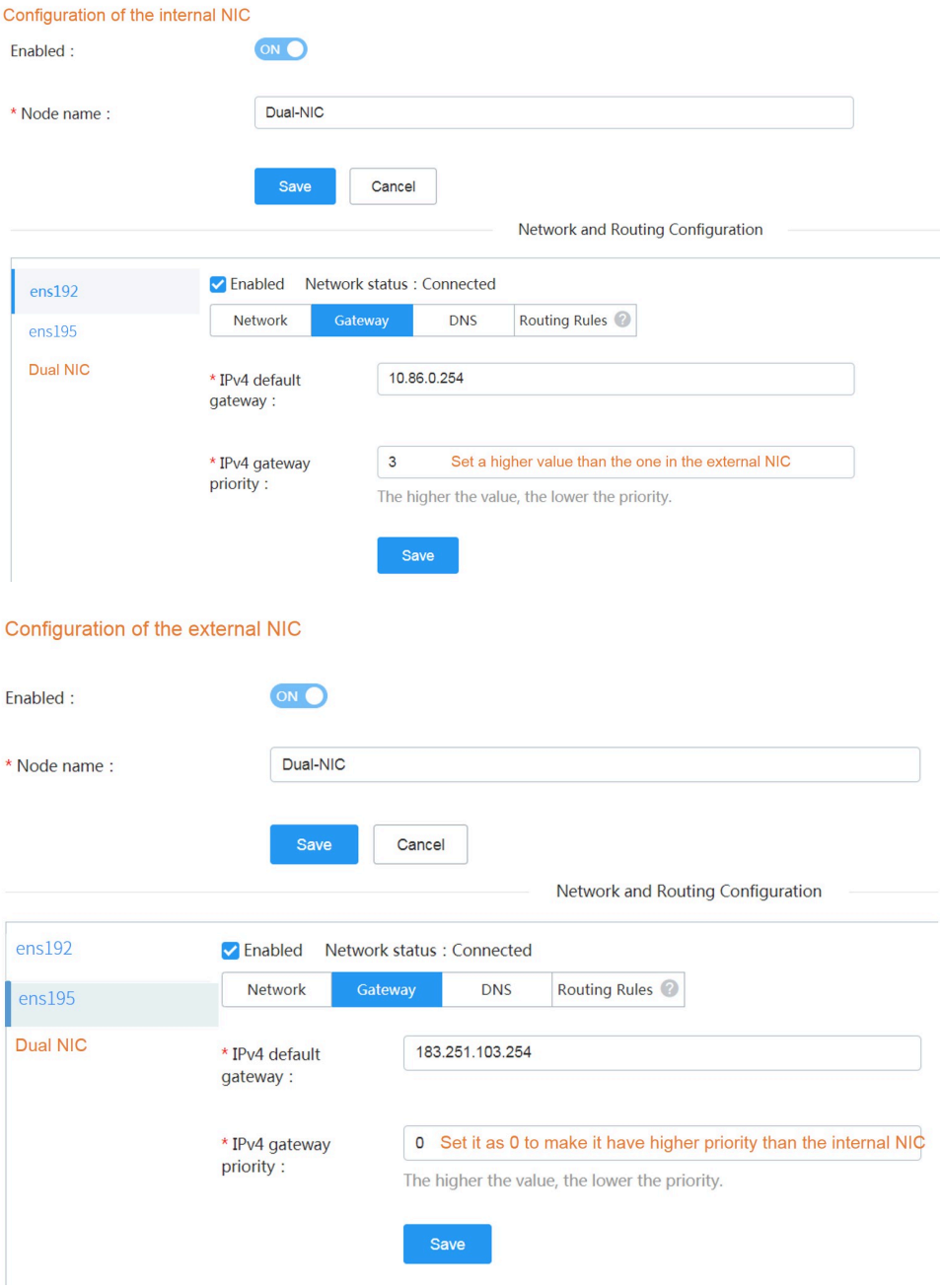


Go to the page of Node Management, and check the following configuration:

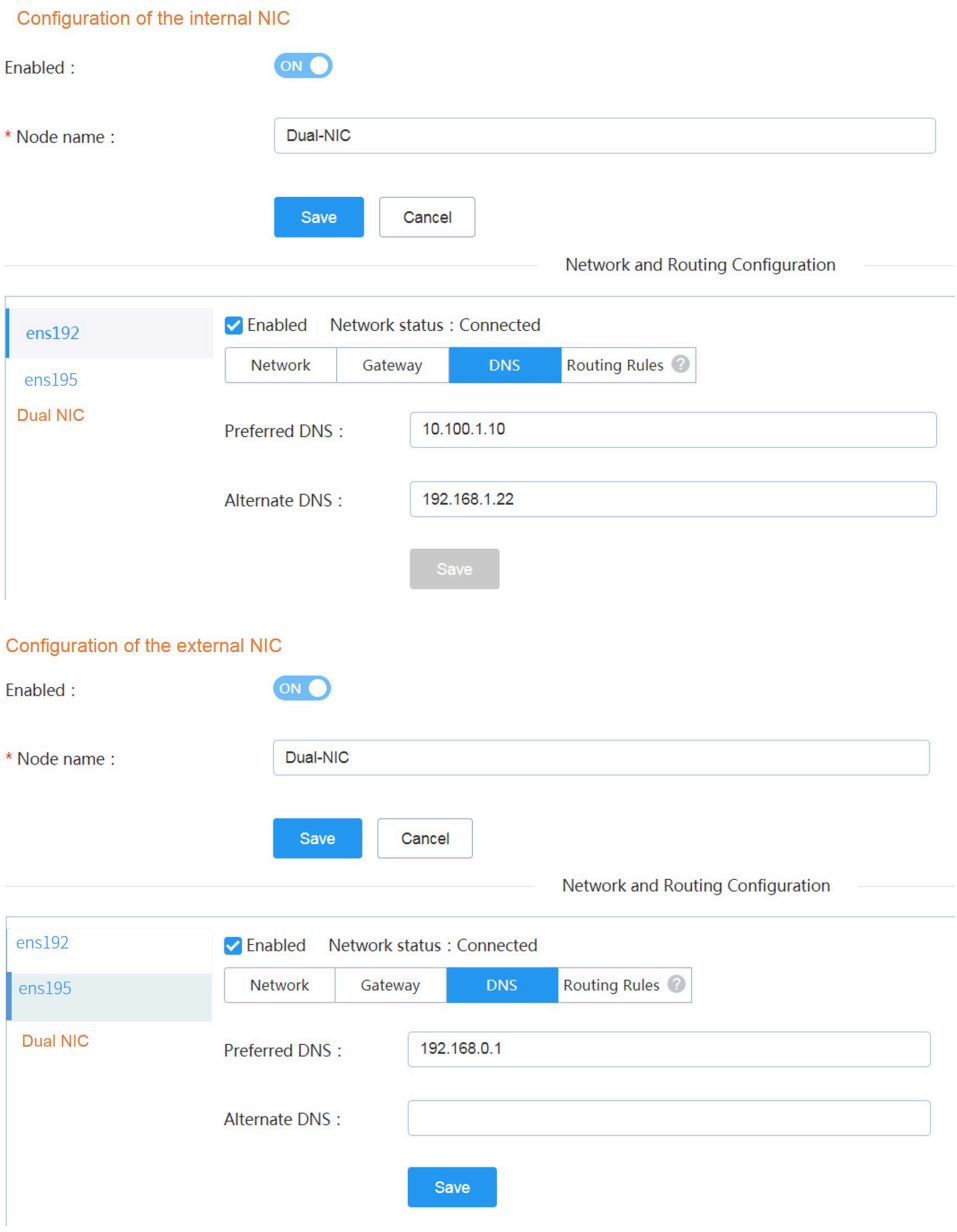
- **Network**



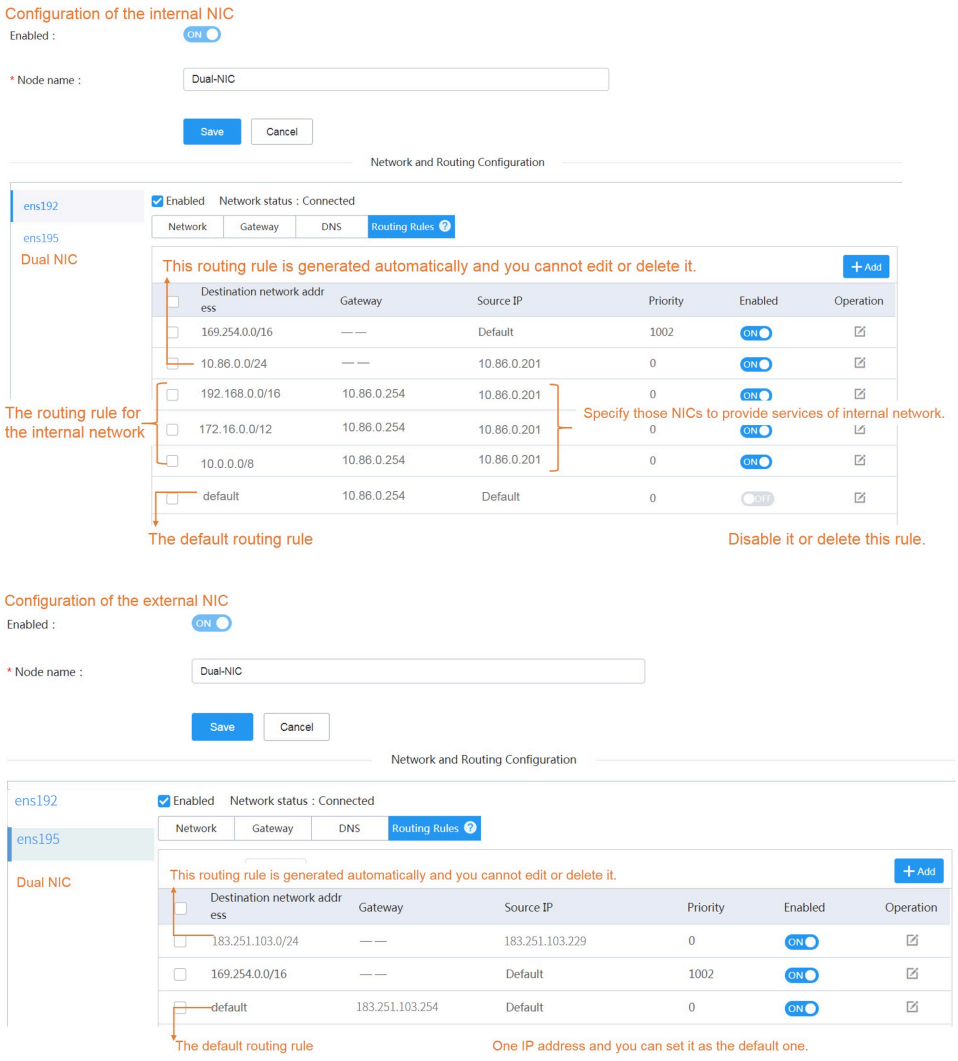
- **Gateway**


Configuration of the internal NIC
Enabled :
ON
* Node name :
Dual-NIC
Save
Cancel
Network and Routing Configuration
ens192
ens195
Dual NIC
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
* IPv4 default gateway :
10.86.0.254
* IPv4 gateway priority :
3
Set a higher value than the one in the external NIC
The higher the value, the lower the priority.
Save
Configuration of the external NIC
Enabled :
ON
* Node name :
Dual-NIC
Save
Cancel
Network and Routing Configuration
ens192
ens195
Dual NIC
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
* IPv4 default gateway :
183.251.103.254
* IPv4 gateway priority :
0
Set it as 0 to make it have higher priority than the internal NIC
The higher the value, the lower the priority.
Save

- **DNS**

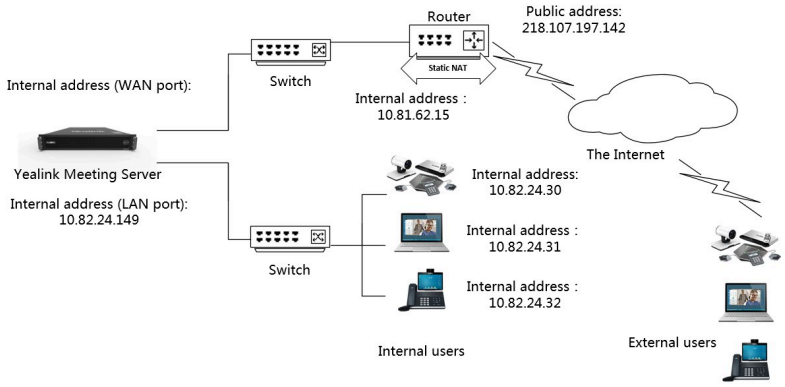

Configuration of the internal NIC
Enabled :
ON
* Node name :
Dual-NIC
Save
Cancel
Network and Routing Configuration
ens192
ens195
Dual NIC
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
Preferred DNS :
10.100.1.10
Alternate DNS :
192.168.1.22
Save
Configuration of the external NIC
Enabled :
ON
* Node name :
Dual-NIC
Save
Cancel
Network and Routing Configuration
ens192
ens195
Dual NIC
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
Preferred DNS :
192.168.0.1
Alternate DNS :
Save

- **Routing Rules**



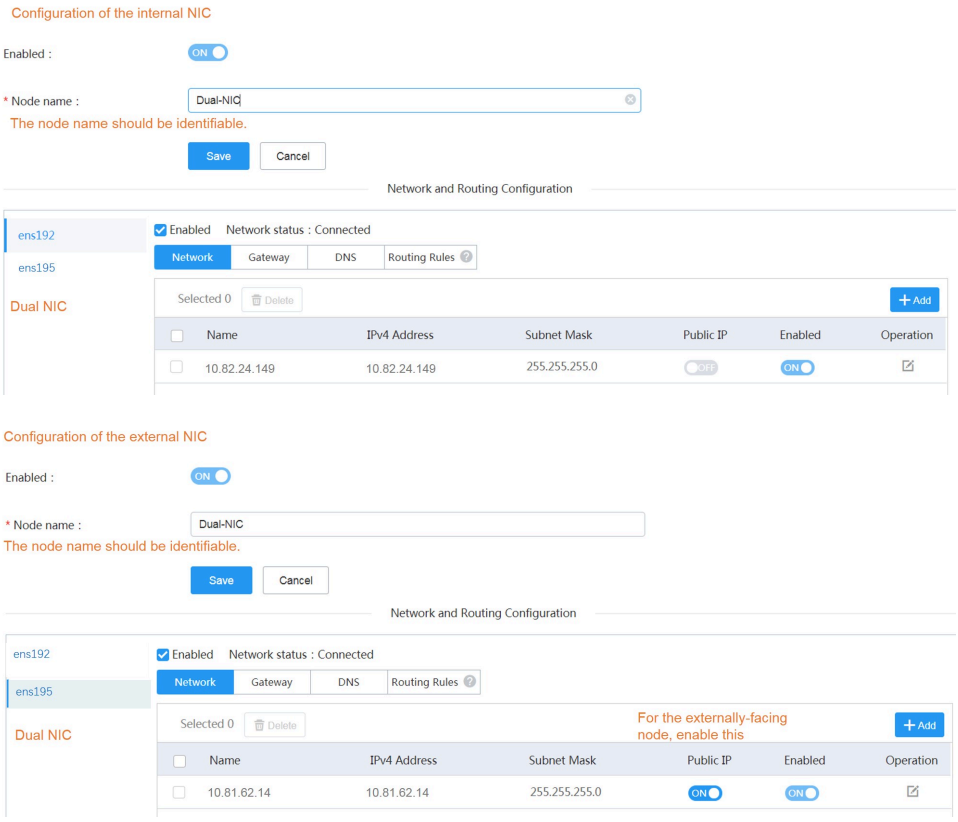
Internal and External Deployment with Dual NIC (with NAT)

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.

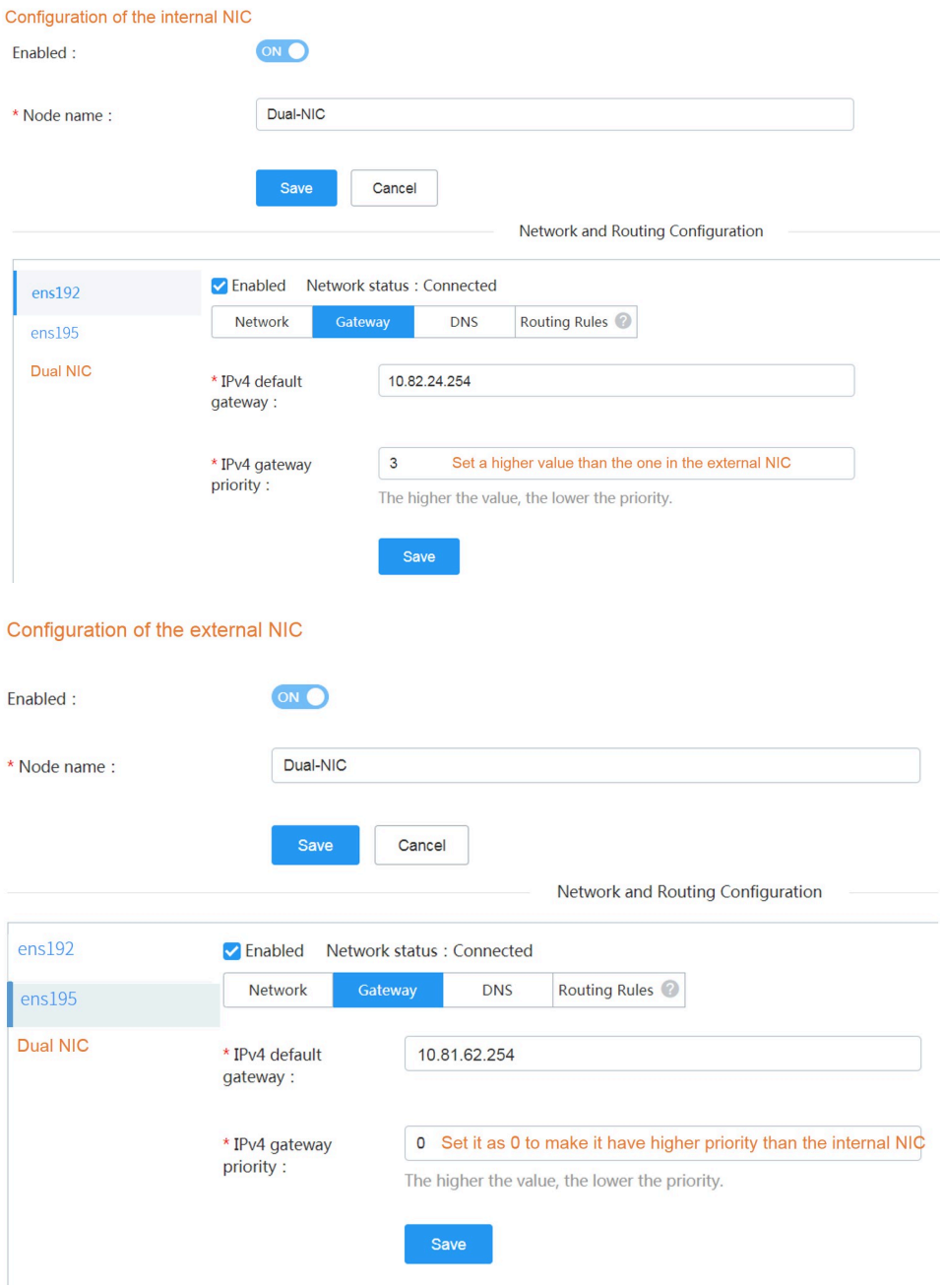


Go to the page of Node Management, and check the following configuration:

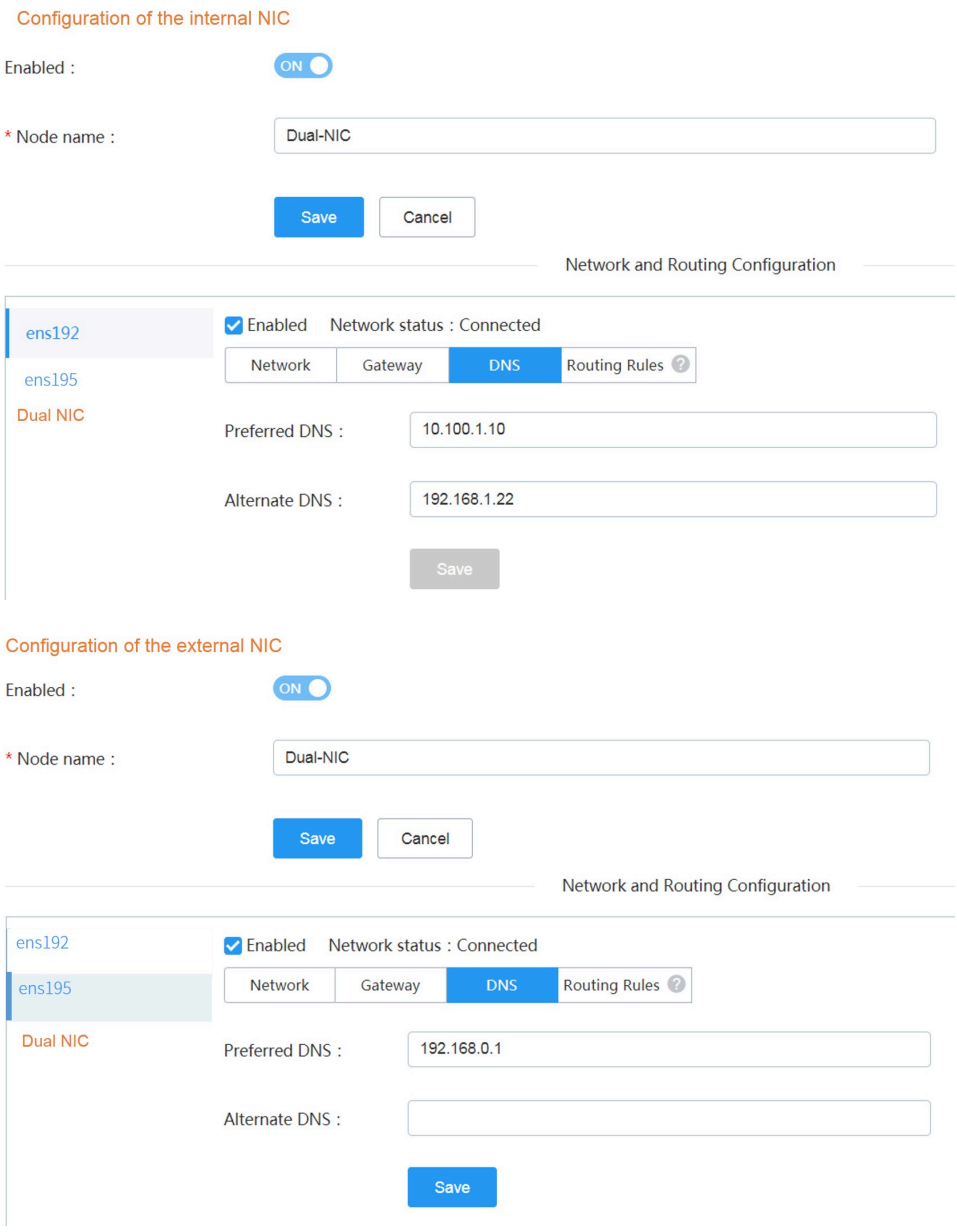
- **Open the external service port in Port Requirements of the Router.**
- **Network**



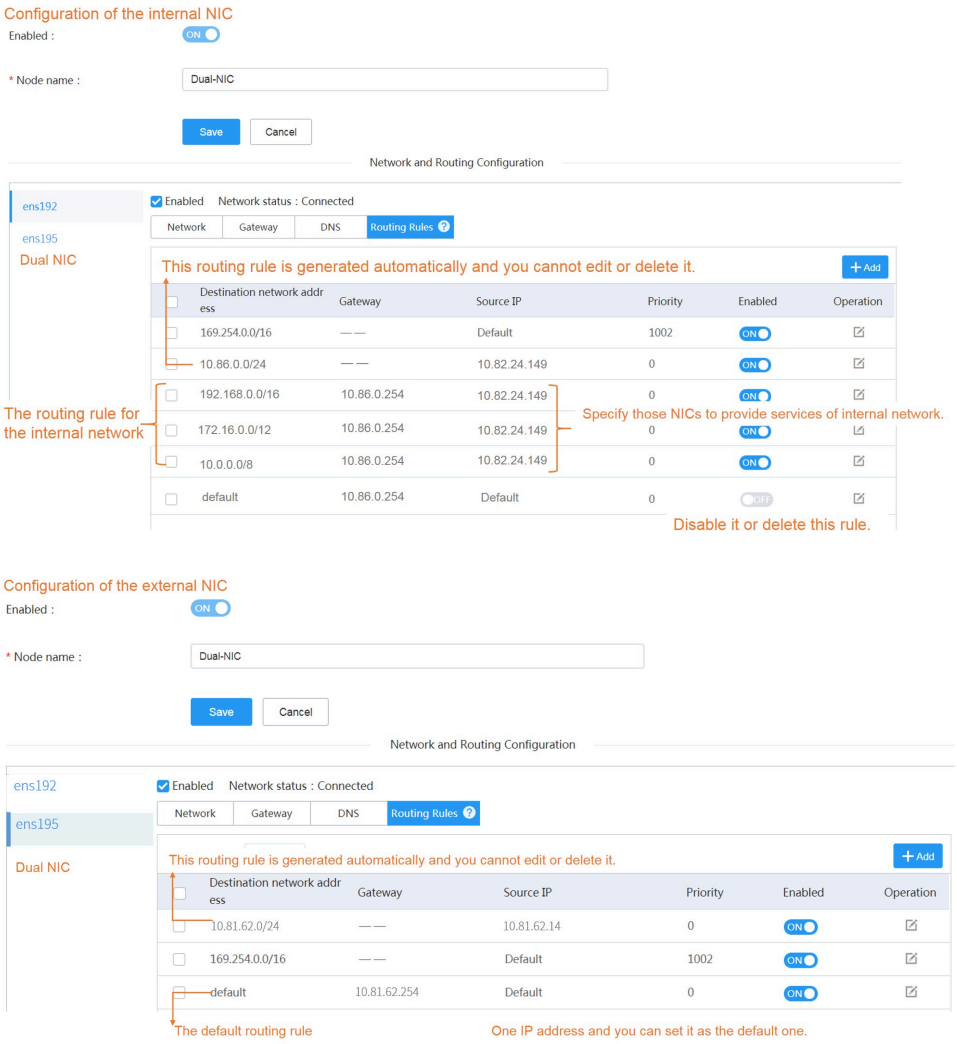
- **Gateway**


Configuration of the internal NIC
Enabled :
ON
* Node name :
Dual-NIC
Save
Cancel
Network and Routing Configuration
ens192
ens195
Dual NIC
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
* IPv4 default gateway :
10.82.24.254
* IPv4 gateway priority :
3
Set a higher value than the one in the external NIC
The higher the value, the lower the priority.
Save
Configuration of the external NIC
Enabled :
ON
* Node name :
Dual-NIC
Save
Cancel
Network and Routing Configuration
ens192
ens195
Dual NIC
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
* IPv4 default gateway :
10.81.62.254
* IPv4 gateway priority :
0
Set it as 0 to make it have higher priority than the internal NIC
The higher the value, the lower the priority.
Save

- **DNS**


Configuration of the internal NIC
Enabled :
ON
* Node name :
Dual-NIC
Save
Cancel
Network and Routing Configuration
ens192
ens195
Dual NIC
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
Preferred DNS :
10.100.1.10
Alternate DNS :
192.168.1.22
Save
Configuration of the external NIC
Enabled :
ON
* Node name :
Dual-NIC
Save
Cancel
Network and Routing Configuration
ens192
ens195
Dual NIC
Enabled
Network status : Connected
Network
Gateway
DNS
Routing Rules
Preferred DNS :
192.168.0.1
Alternate DNS :
Save

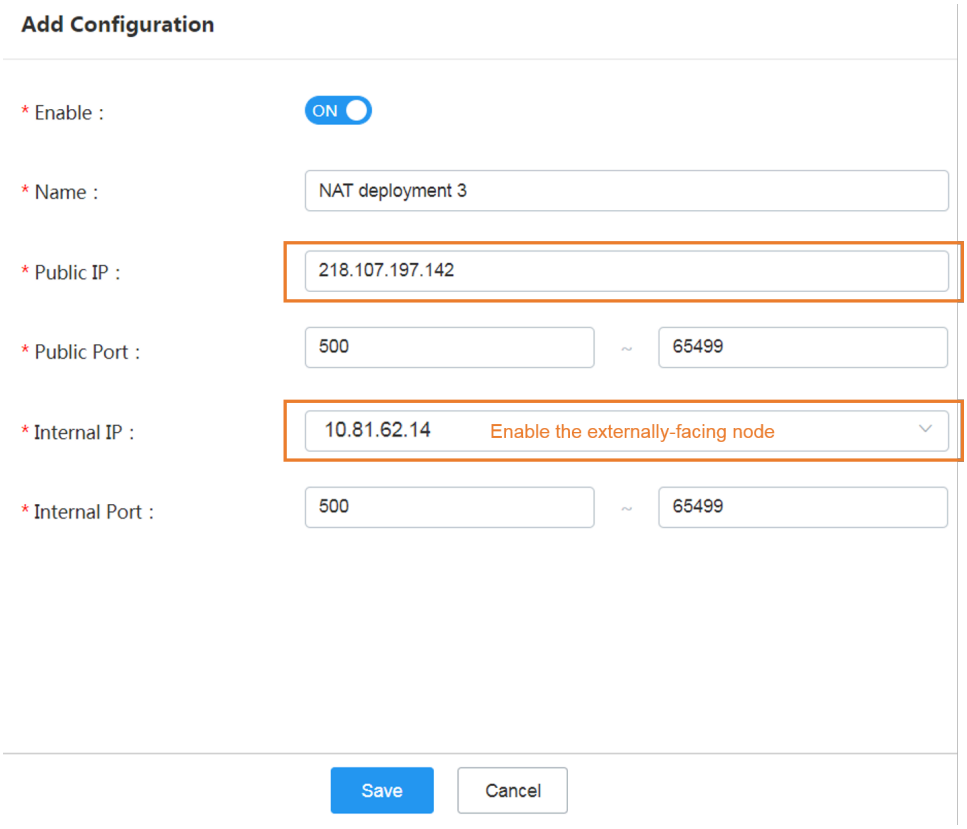
- **Routing Rules**



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.



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

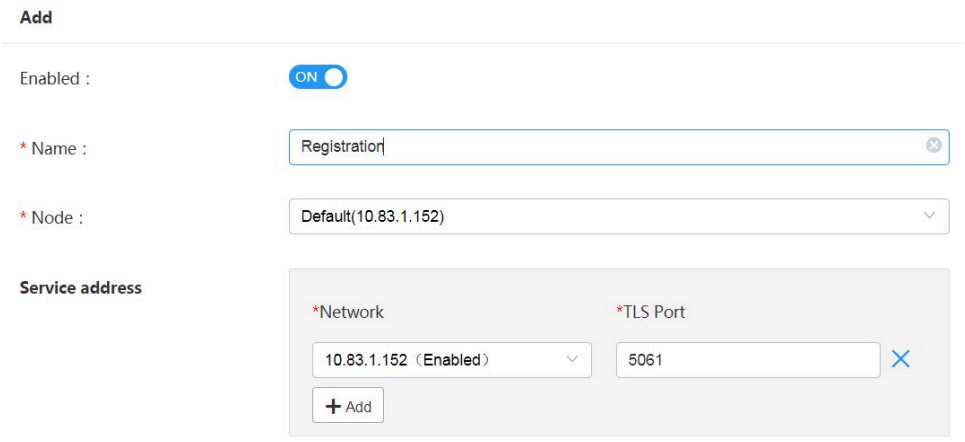
If you want to connect YMS and the LDAP server to synchronize the accounts on YMS with the accounts on LDAP, you need to configure the LDAP first (Configuring the LDAP).

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.

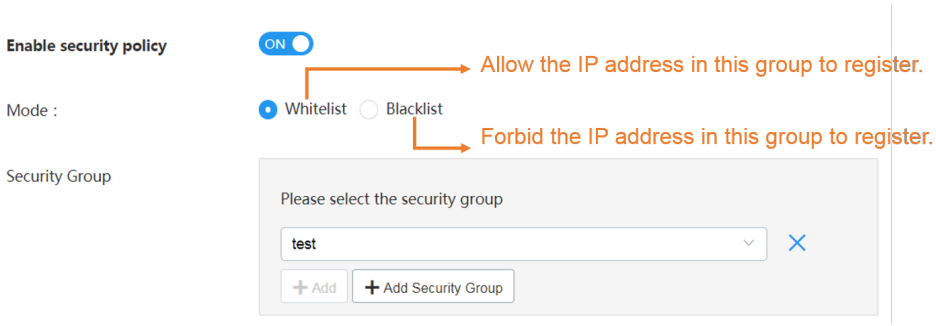
Procedure

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

3. Set the parameters.



4. Optional: Configure the security policy.
   For adding a security group, seeAdding a Security Group



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.

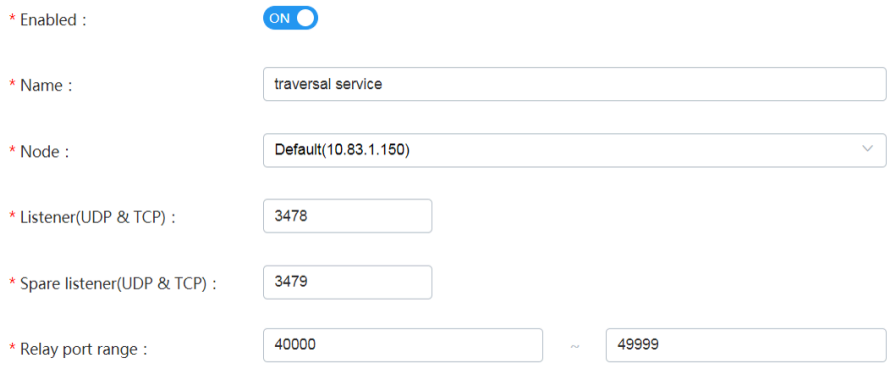
About this task

- 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.

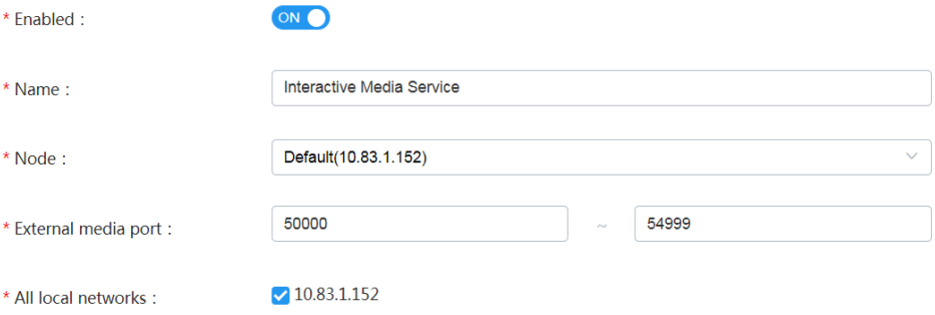


Setting the Interactive Media Service

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.



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

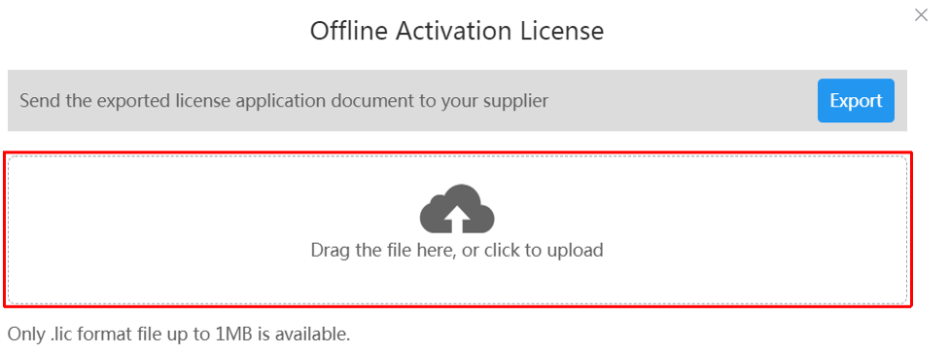
If the server cannot access the public network, you can activate the license offline.

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.

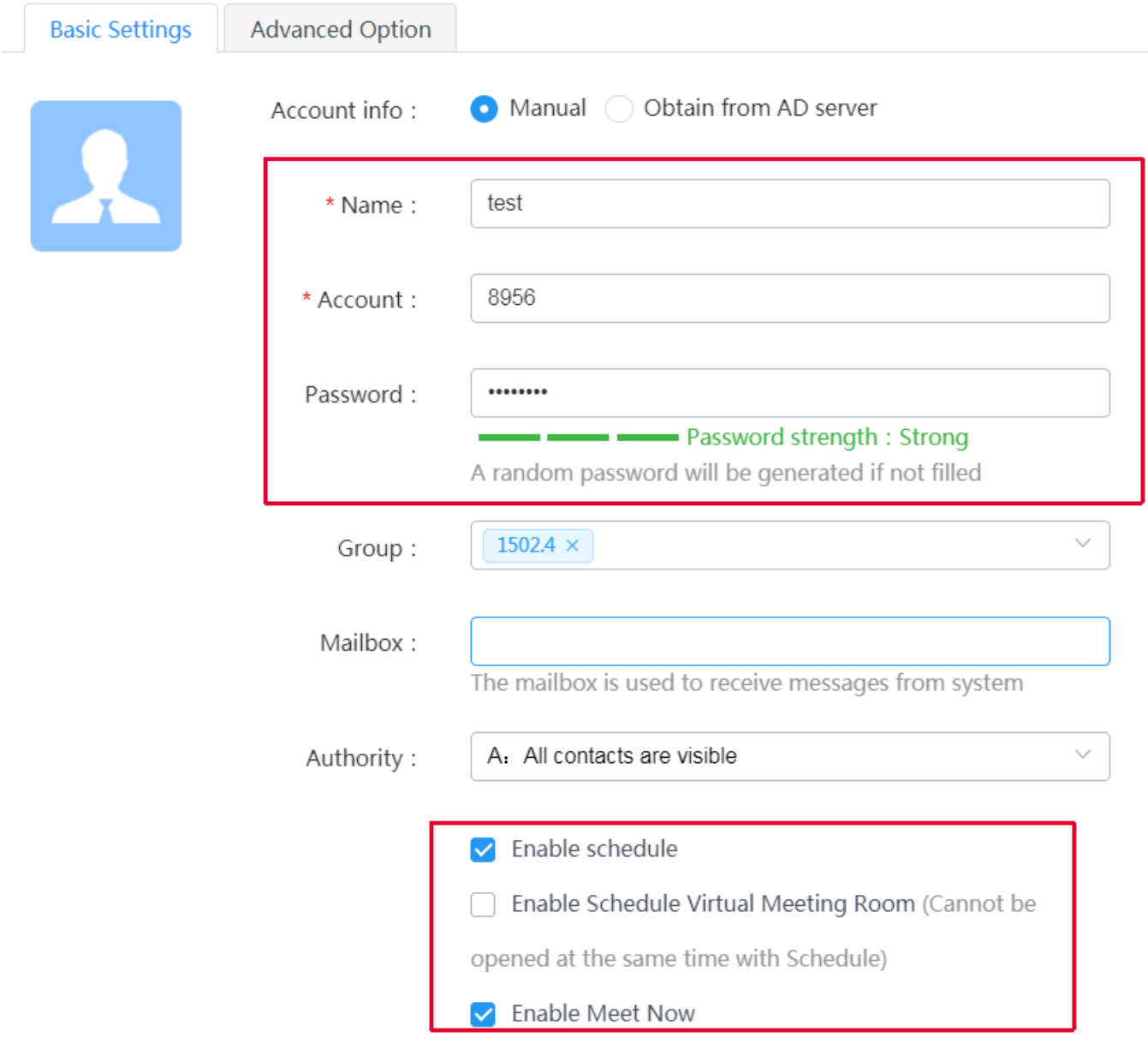
Creating Accounts

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.

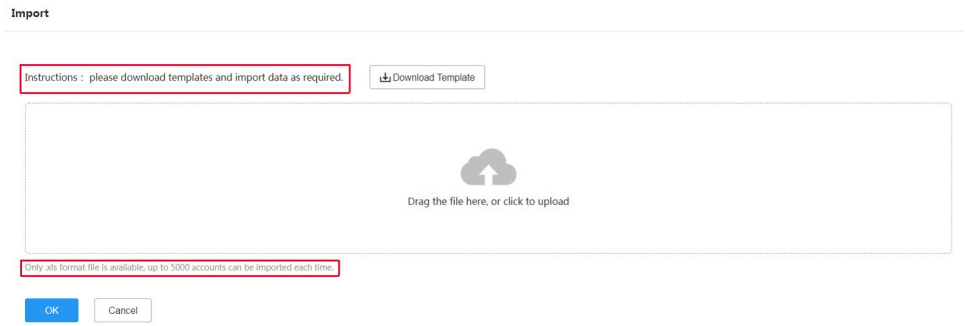
Procedure

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

2. Add an account or import a batch of accounts.
   - **Add an account**



   - **Import a batch of accounts**

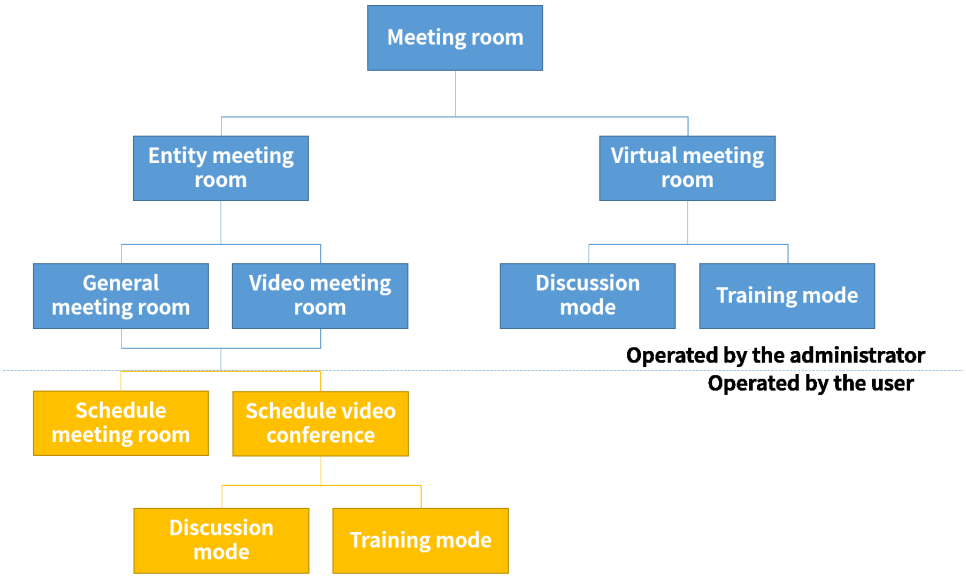


3. Save the configuration.

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.

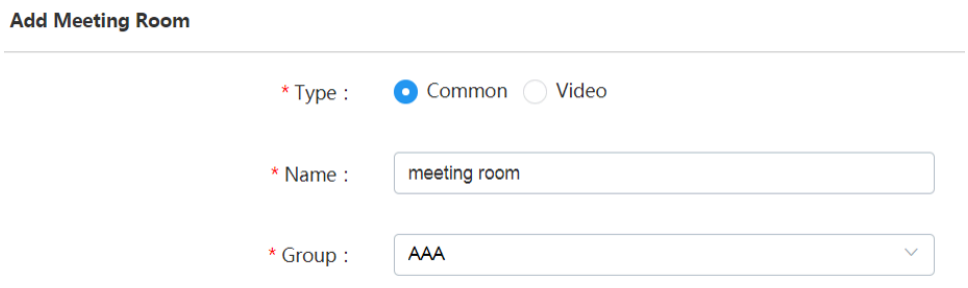
About this task



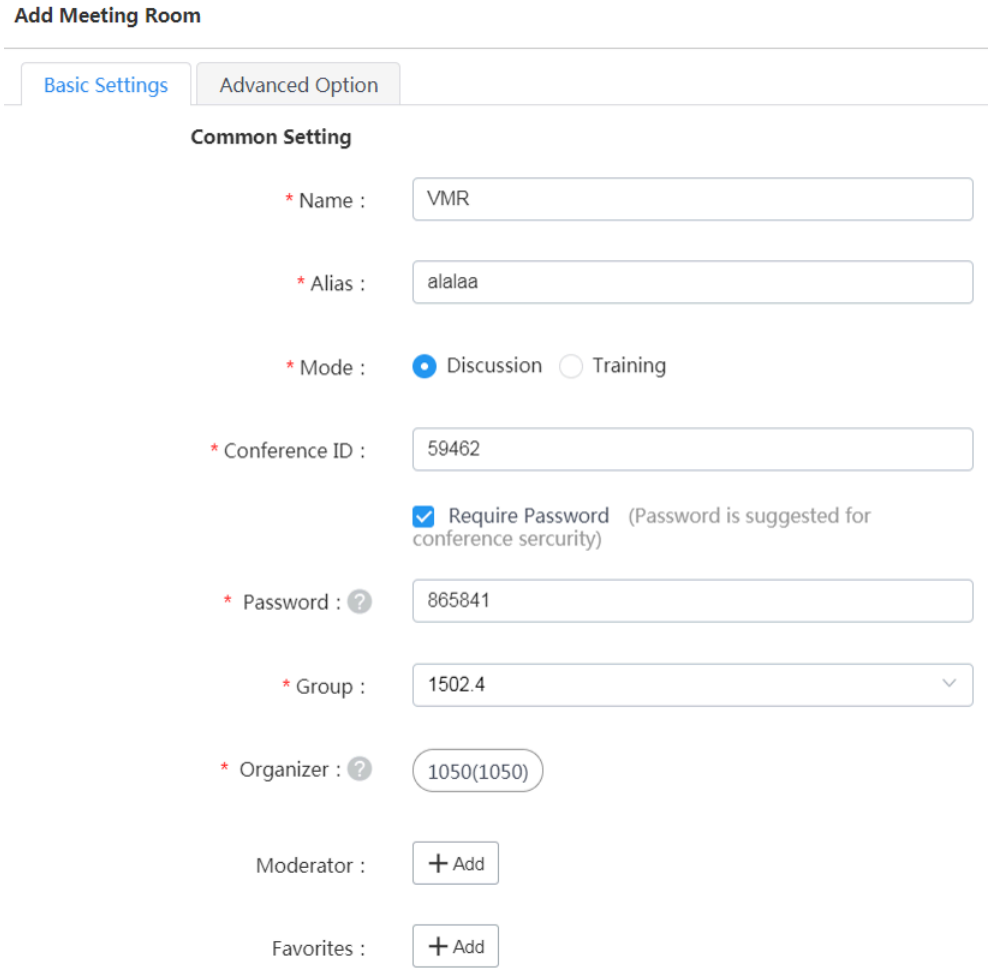
Procedure

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

2. Add an entity meeting room or a VMR.
   - **Adding Entity Meeting Rooms**



   - **Adding a VMR**

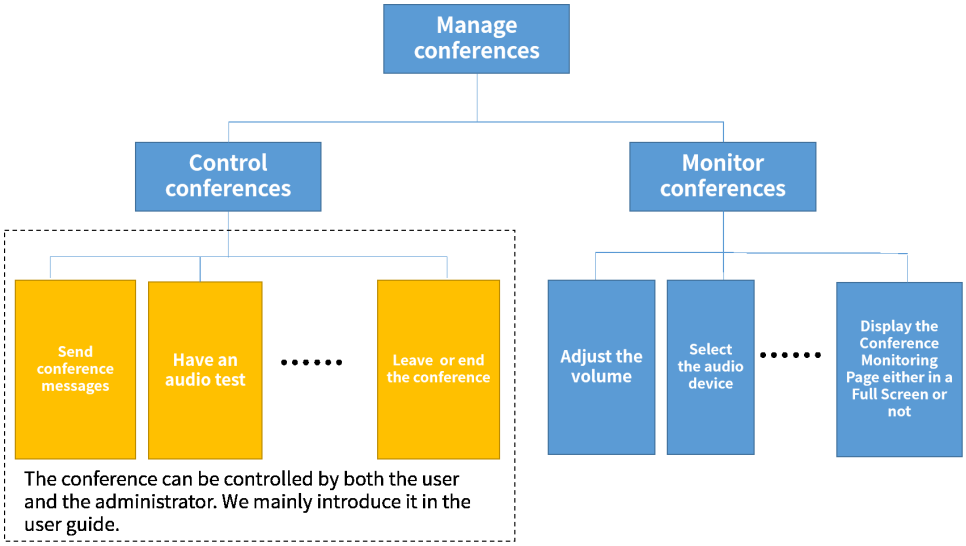


3. Save the configuration.

Managing Conferences

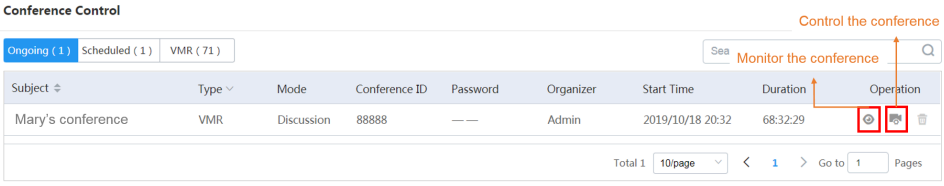
You can control and monitor the conferences. For more information, refer to Managing Conferences.

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 Web Access Port
- Enabling the NTP Service
- 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.

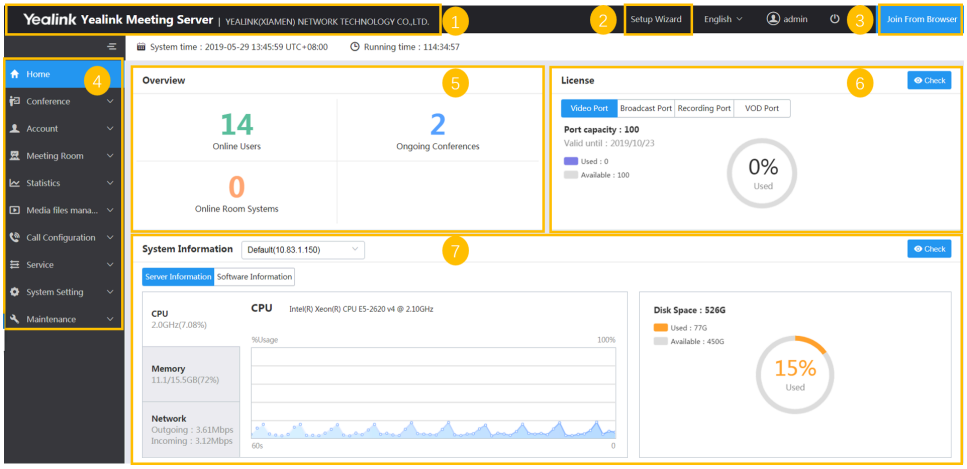


Table 10:

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 Yealink Web App User Guide.
4	The navigation bar.
5	• View the number of the online users, the ongoing conferences, and the online room system accounts. • Go to the corresponding module quickly.
6	• Click **Check** to go to the Licenses page. • View the related port information, including the capacity, the validity, and the usage.

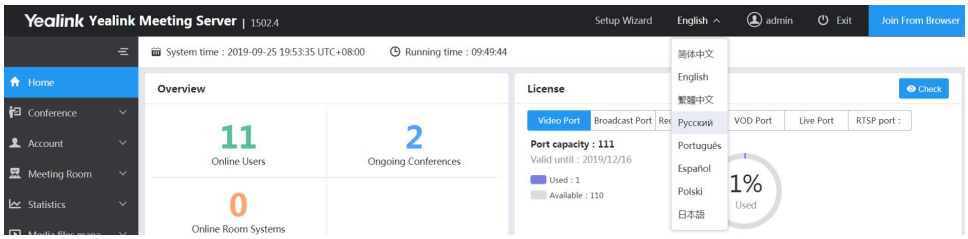
Number	Description
7	View the system information of the corresponding node. • View the server CPU, the memory, the network, and the disk space. You can click **Check** to view the detail information. • View the information about the software version.

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

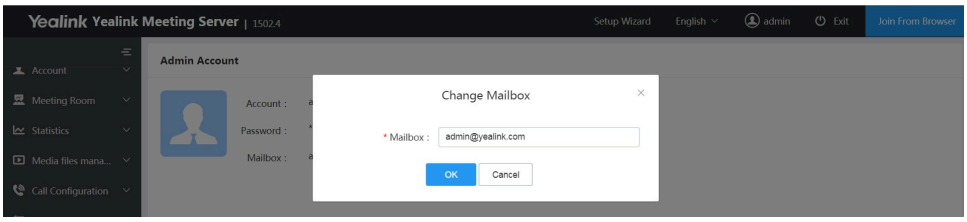
You can edit the registered email. This email is used to receive emails about resetting passwords and system alarms.

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.



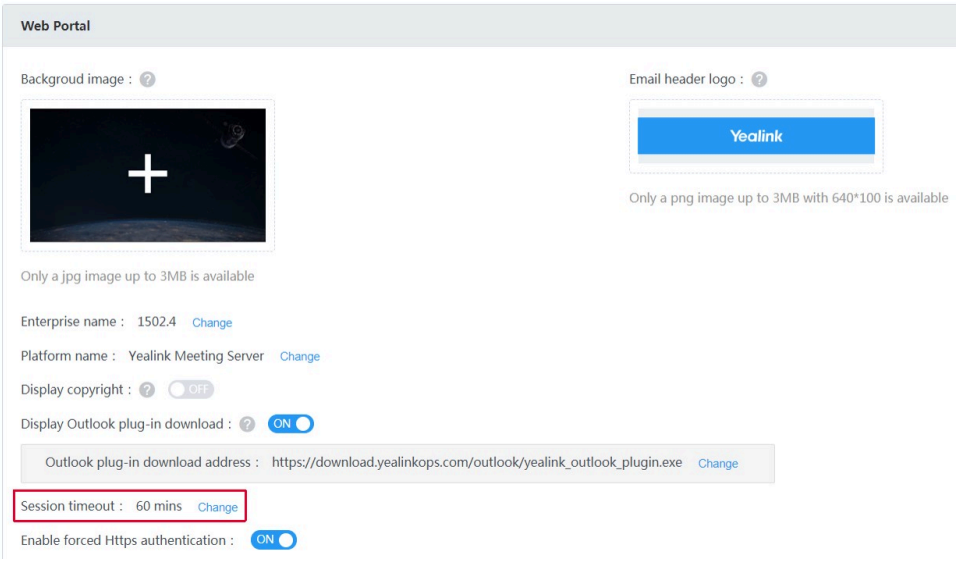
Setting the Session Timeout

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.

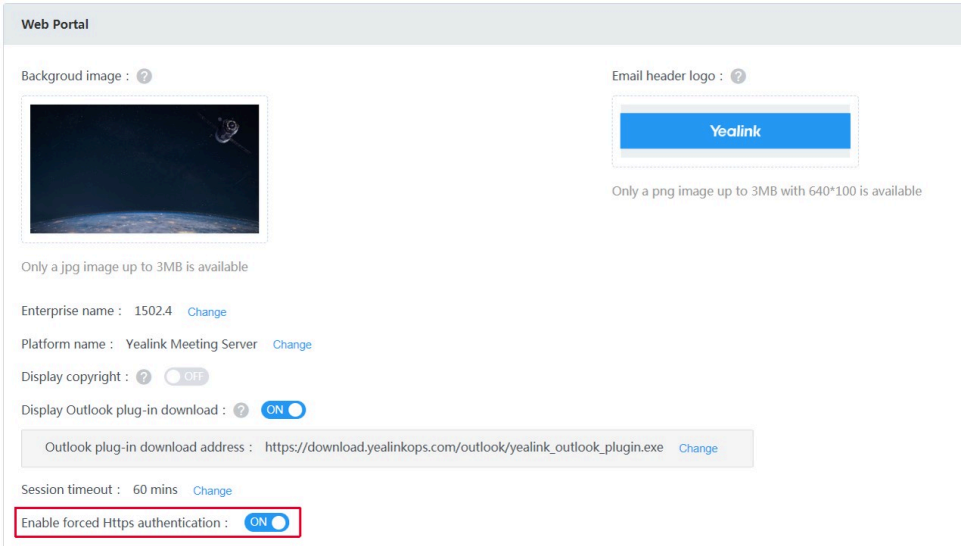


Enabling Forced Https Authentication

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**.



Adding a Sub Admin Account

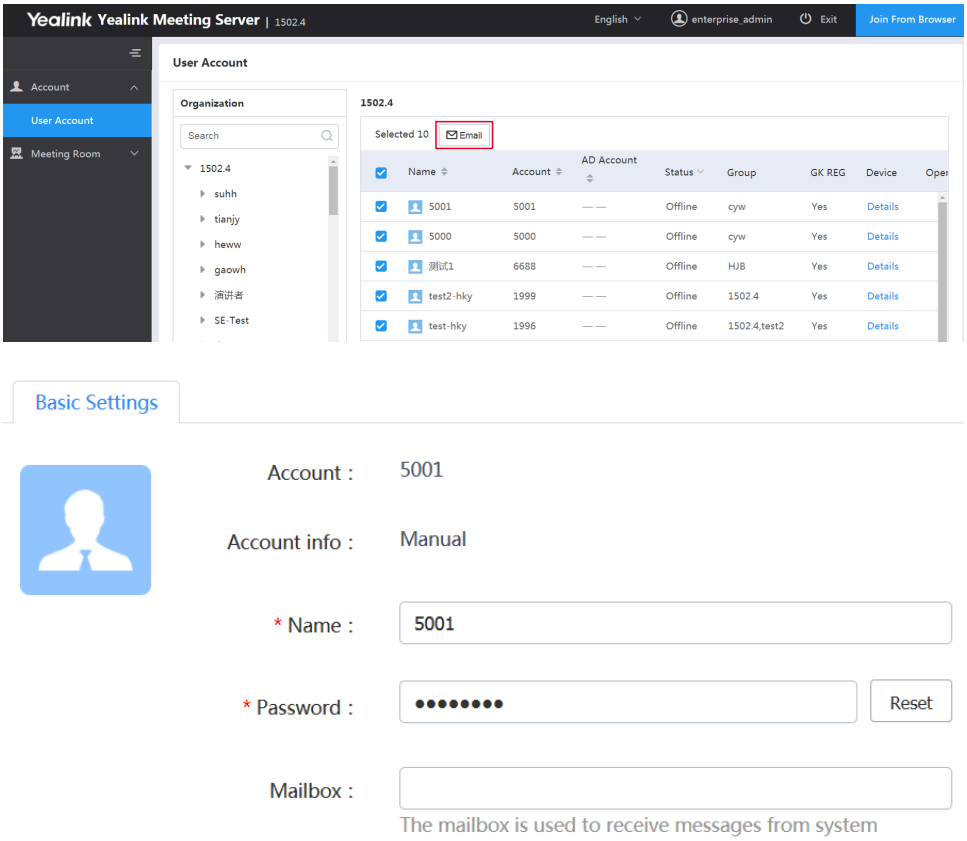
For the system security, you can add different sub admin accounts, and assign the desired module or permission to them.

About this task

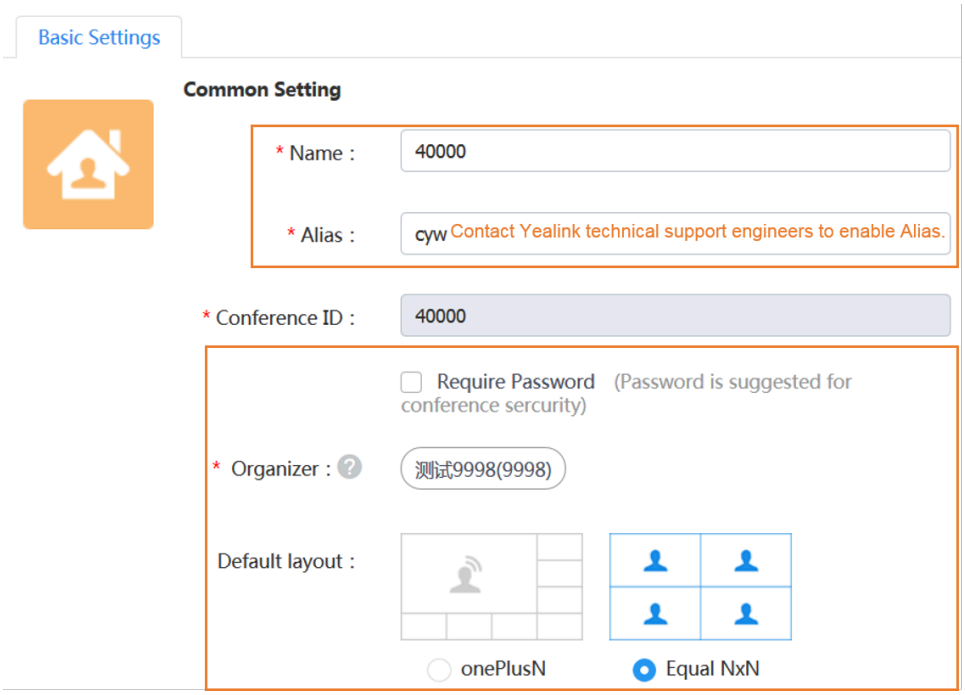
There are five types of the sub admin account: the conference manager, the conference operator, the operation manager, the enterprise administrator, and the customization. You can add up to 100 sub admin accounts.

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**



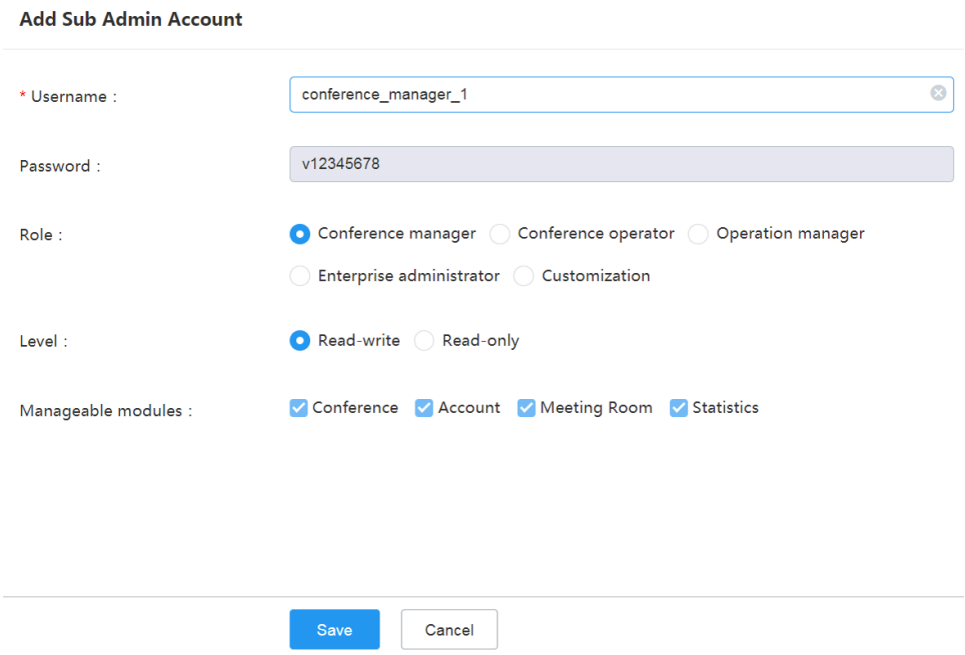
- **The privilege of VMR**



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.



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

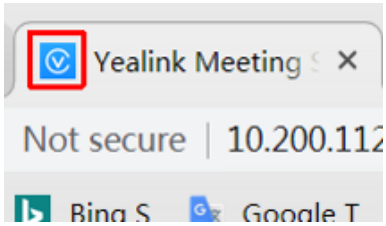
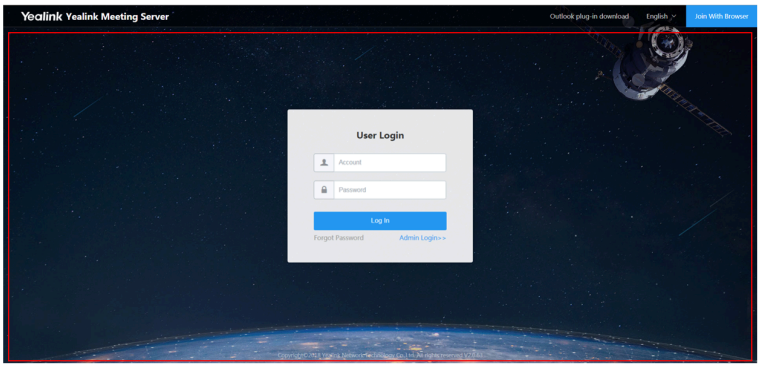
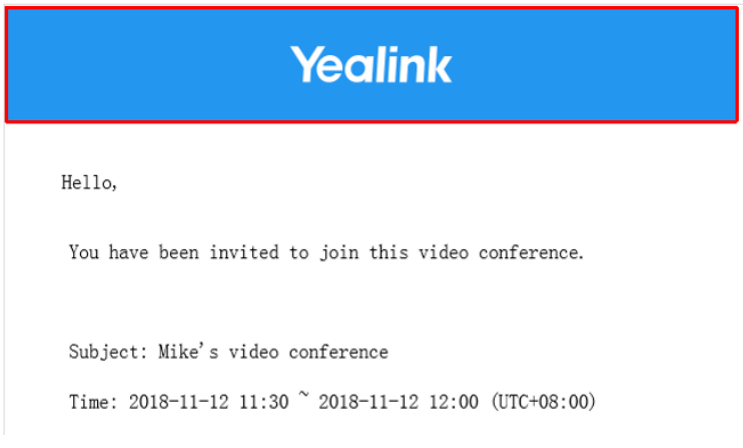
Parameter	Effect
Portal logo	
Tab logo	 **Note:** A free conversion tool is available on the Internet.

Table 12: Parameters of the Web Portal

Parameter	Effect
Background image	
Email header logo	

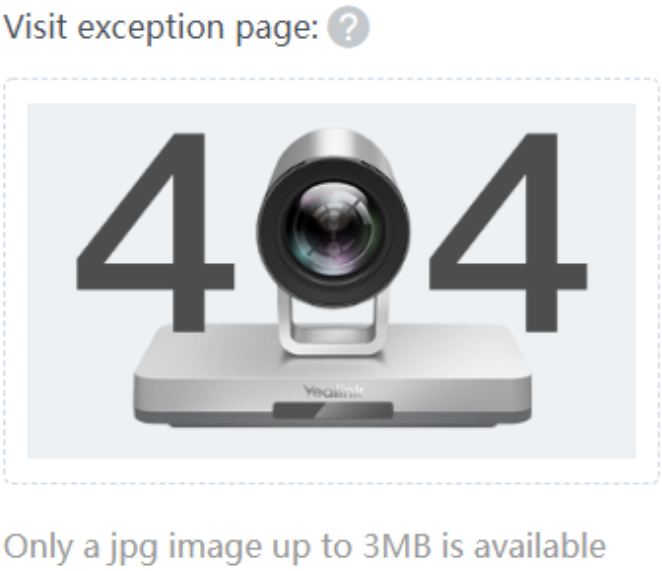
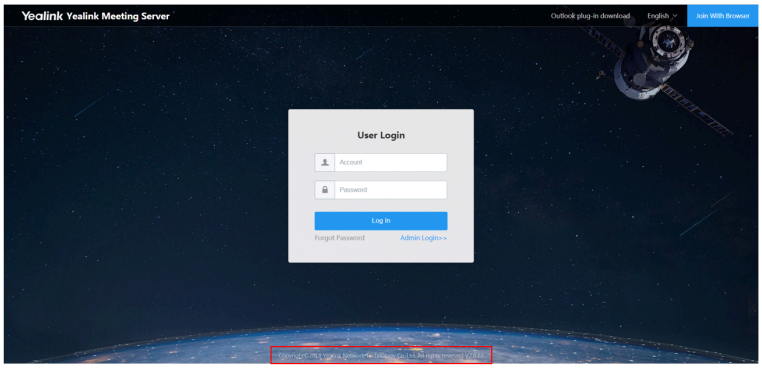
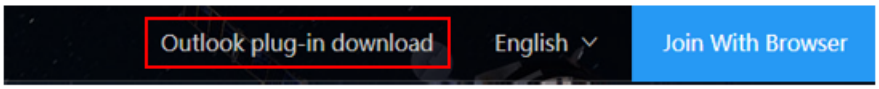
Parameter	Effect
Visit exception page	
Enterprise name	
Platform name	
Display copyright	
Display Outlook plug-in download	

Table 13: Parameters of the WebRTC Portal

Parameter	Effect
Enable WebRTC	Allow or refuse the user to join the conference via browser.

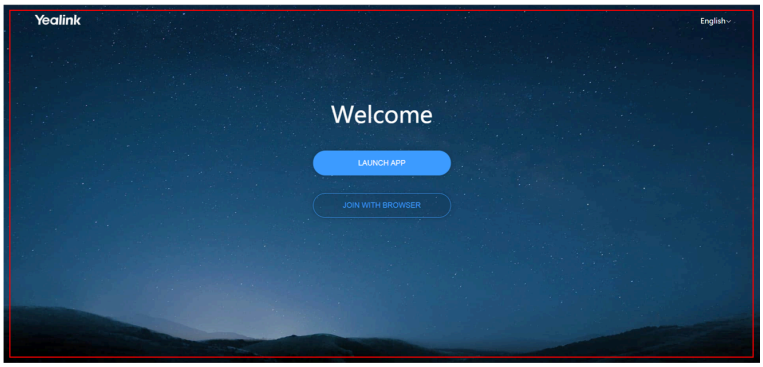
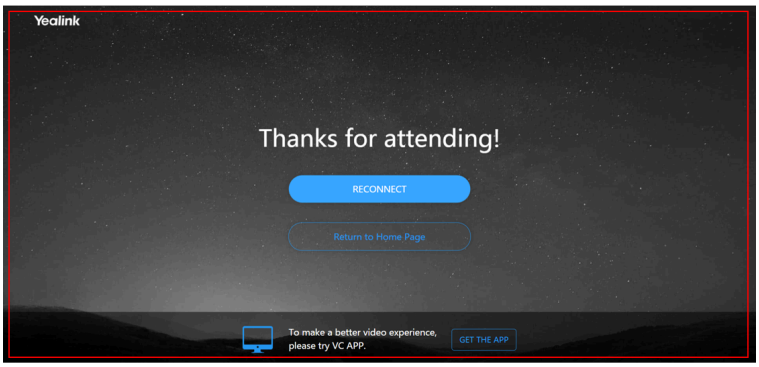
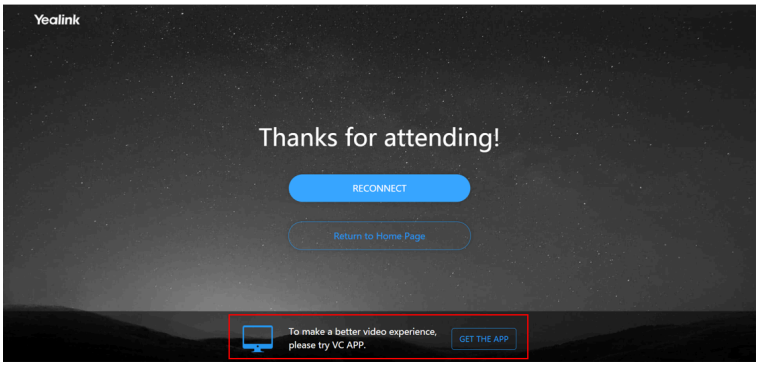
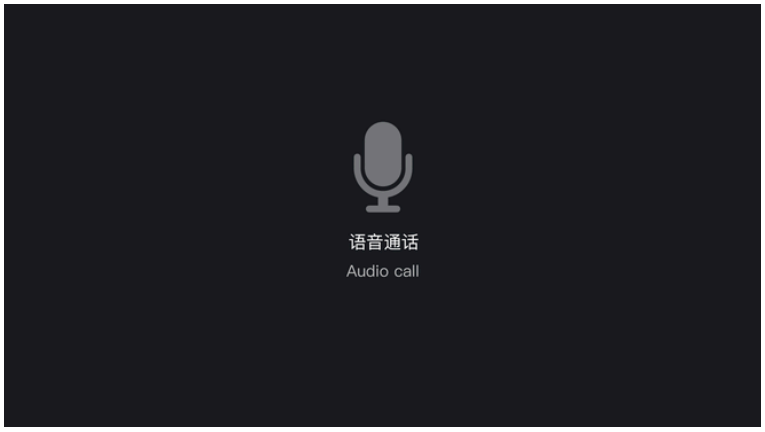
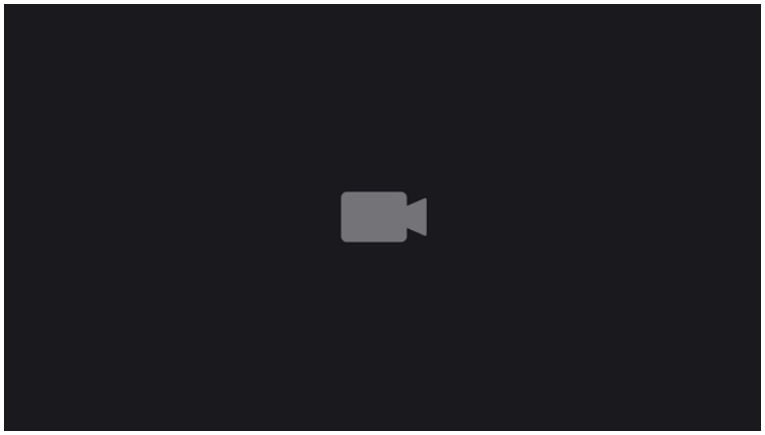
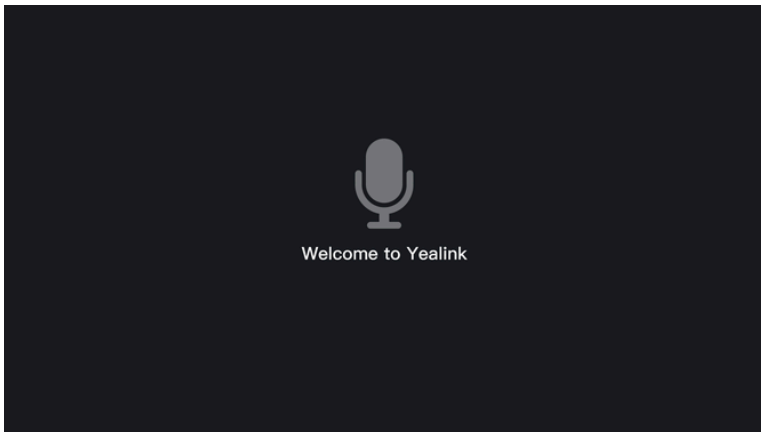
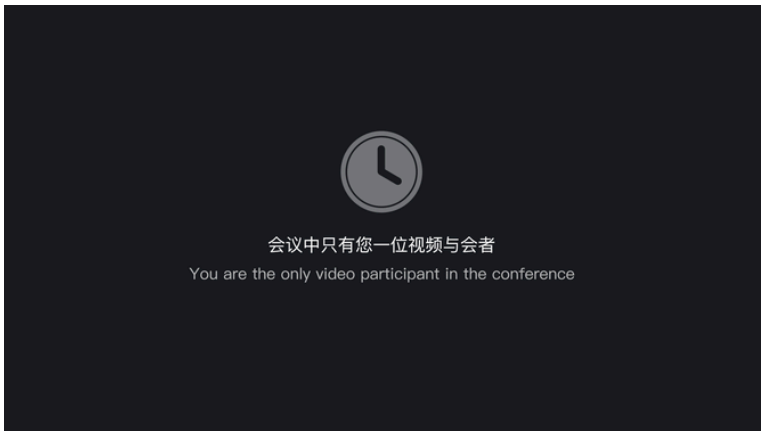
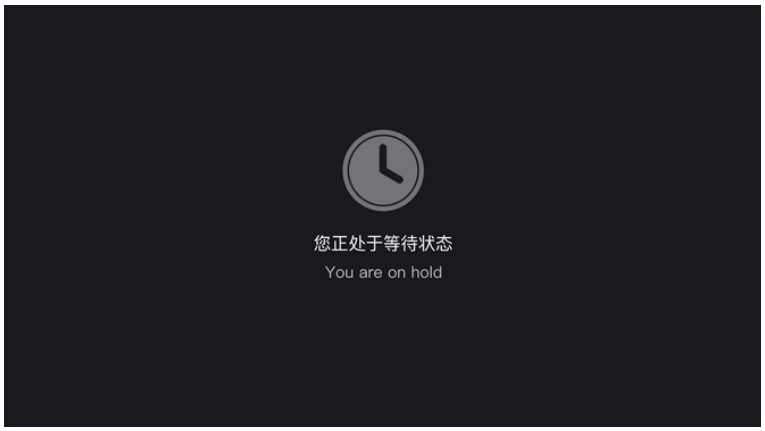
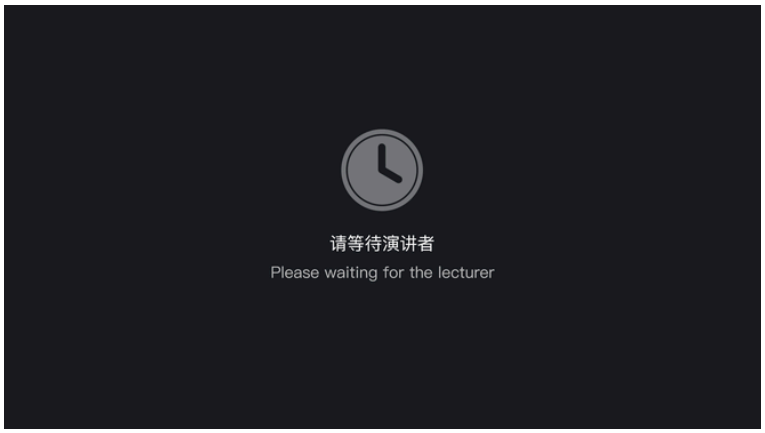
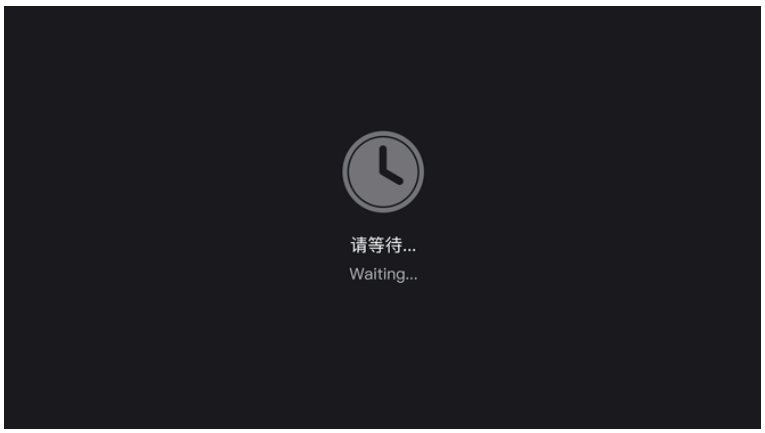
Parameter	Effect
Background image for WebRTC home screen	
Background image of WebRTC end page	
Extension download address	The address for downloading Yealink content sharing plugin that you can see when you use Google Chrome to visit Yealink Web App, and share content with the remote.
Display PC soft-client download	
Windows	Specify the address for downloading Yealink VC Desktop for Windows.
Mac	Specify the address for downloading Yealink VC Desktop for Mac.
iOS	Specify the address for downloading Yealink VC Desktop for iOS.
Android	Specify the address for downloading Yealink VC Desktop for Android.

Table 14: Video Conference

Parameter	Effect
User agent settings	Set the server user agent displayed in the call statistics of the audio or video conferences.

Parameter	Effect
Parameters of the Video Conference	
Audio call image	
License limited image	
No video data image	

Parameter	Effect
Camera OFF image	
Welcome screen image	
The sole video call party image	

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.

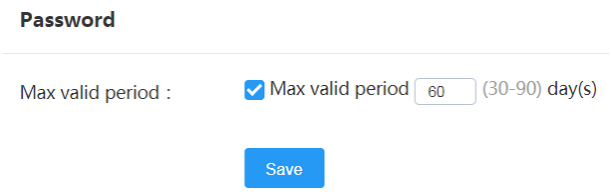
   If the device negotiates with the server to use the resolution of 360P, 720P, and 1080P, the ratio of length to width of the video image is 16:9; if they negotiate to use the resolution of CIF and 4CIF, it is 4:3.

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

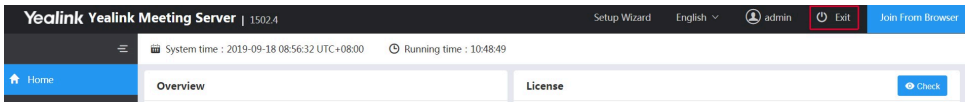
Click **Account** > **Password**.



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 access 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.

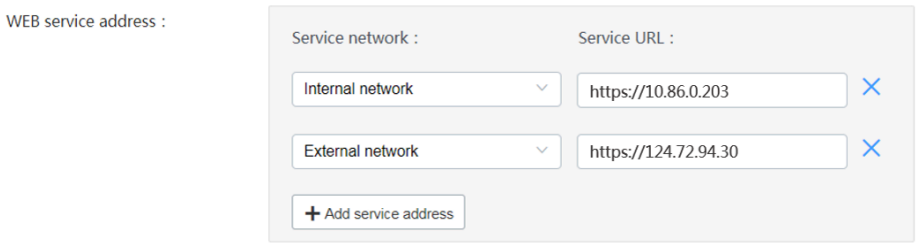
About this task

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.



- 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.

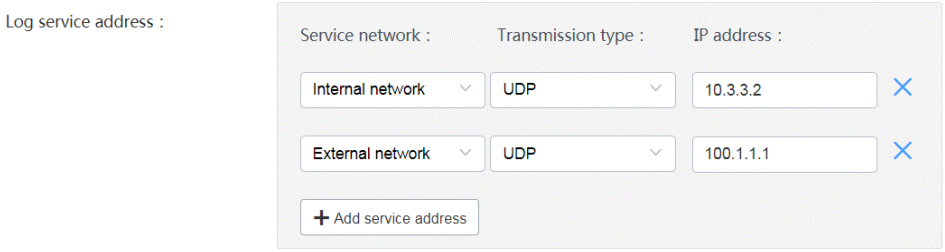
About this task

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.



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 Web Access Port

Procedure

1. Click **System Setting** > **Common Setting** > **Network Association**.
2. Set the Http listener port and the Https listener port respectively.

3. Save the configuration.

Enabling the NTP Service

If you enable the **NTP Service**, it allows you to take YMS as the NTP server, which means you need to configure the the primary NTP addresses of your endpoints as YMS address, so the time on the endpoints can be synchronized with the time on YMS. In the private deployment, the endpoints usually cannot access the external network so you can enable **NTP service** to synchronize the time on the endpoints with the time on YMS. If you disable the **NTP service**, you need to configure the primary NTP addresses of your endpoints as the NTP address configured on YMS.

Before you begin
You register the endpoints with YMS accounts.

Procedure

1. Click **System Setting** > **Common Setting** > **Time**.
2. Enable **NTP server**.

Setting the Time Zone

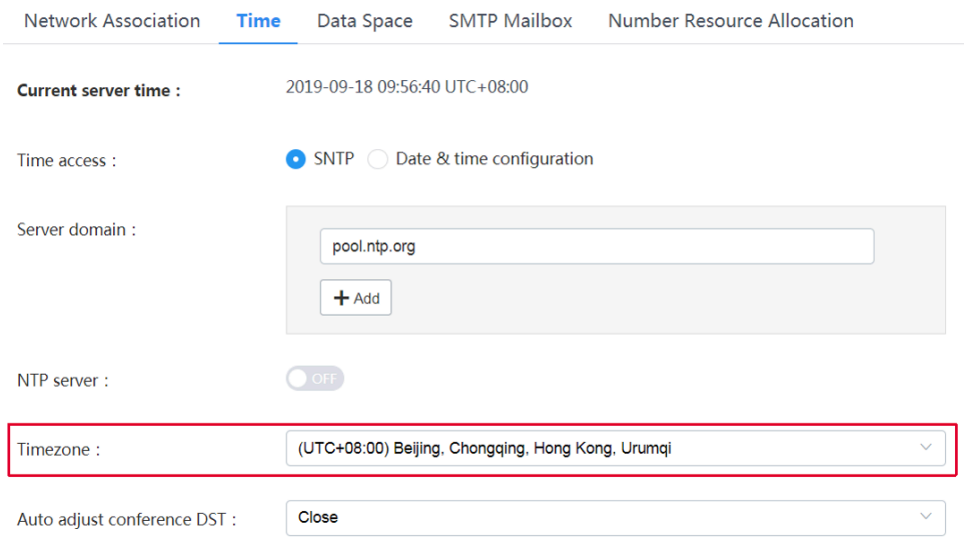
If you change the time zone, it will effect the current server time.

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.



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

Importing the Trusted CA Certificate

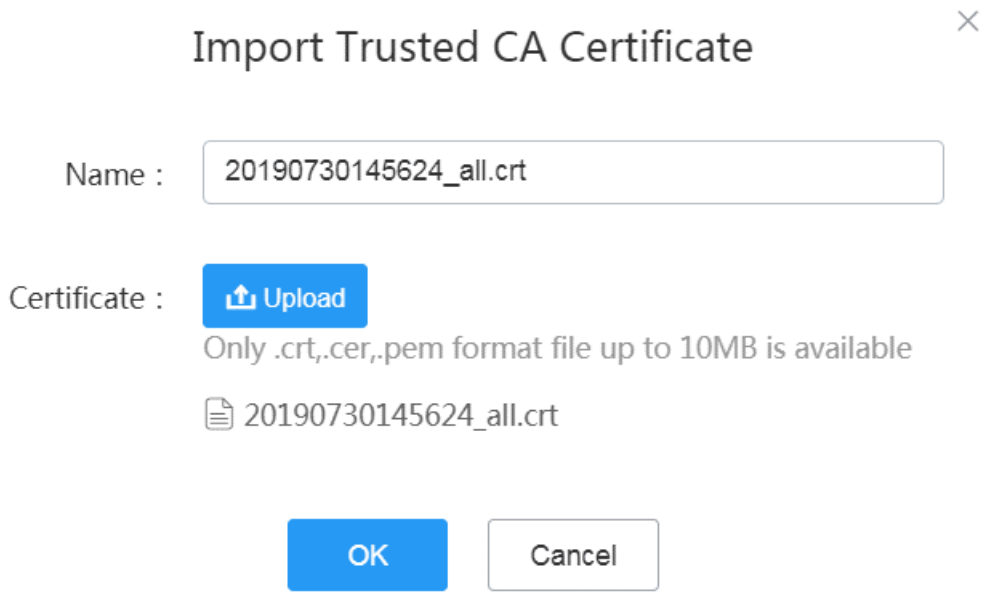
When YMS sends the request of TLS connection to devices, the server needs to verify whether the device is reliable according to the CA certificate. There are 105 built-in CA certificates in YMS. If devices require their self-signed certificates, you need to import the custom CA certificates.

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**.



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

Importing the HTTPS Certificate

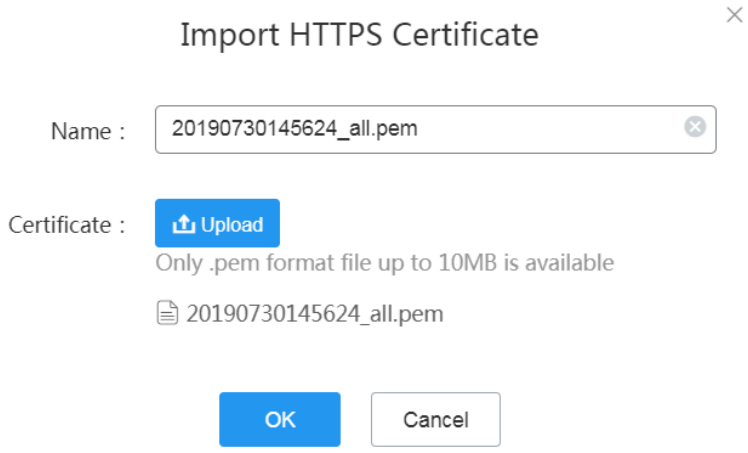
When you access YMS by HTTPS, the browser might prompt that it is insecure. To solve this problem, you can import the certificate trusted by the browser.

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**.



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

Importing the TLS Certificate

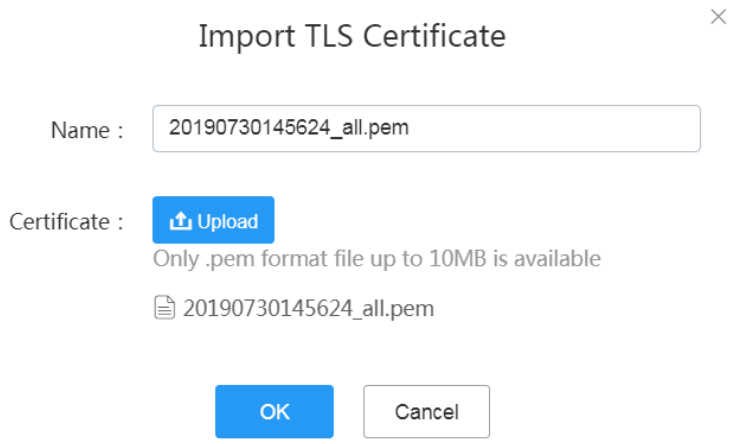
When the device sends a request of TLS connection to YMS, the device will verify whether YMS is reliable according to the TLS certificate sent by YMS.

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**.



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

Configuring the Port

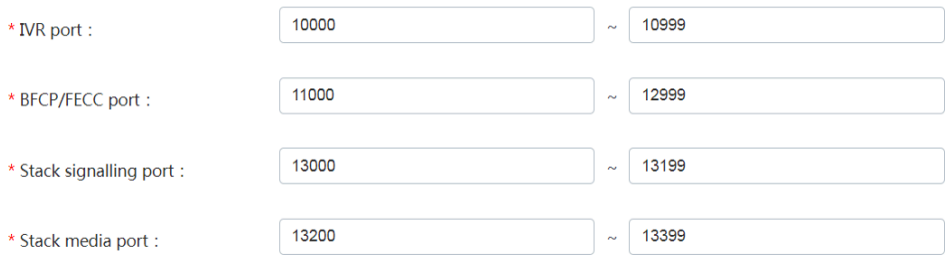
When the default port range fails to satisfy the actual demand, you can set the IVR port, the BFCP/FECC port, the stack signaling port, and the stack media port.

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.



3. Save the configuration.

Setting the Data Space

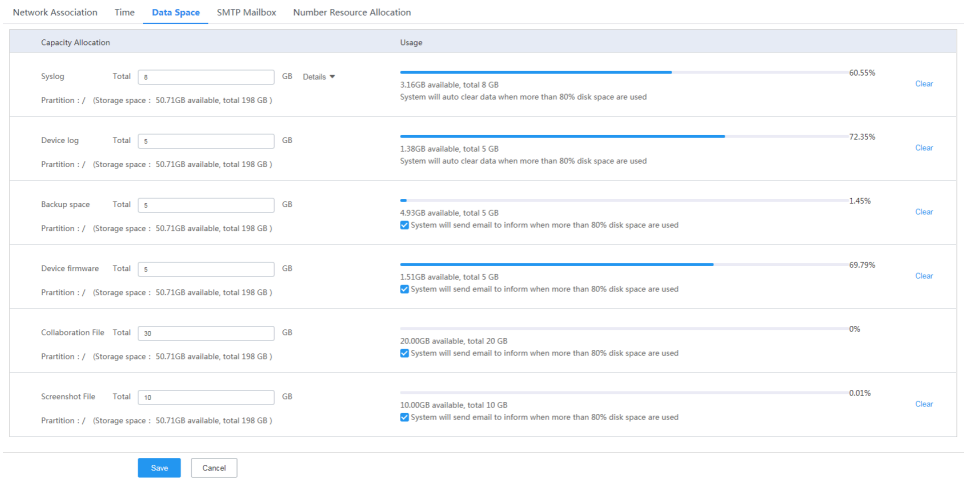
You can manually allocate the space quota for the **Syslog**, the **Device log**, the **Backup space, the screen captures, the Collaboration file**, and the **Device firmware**.

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.



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.

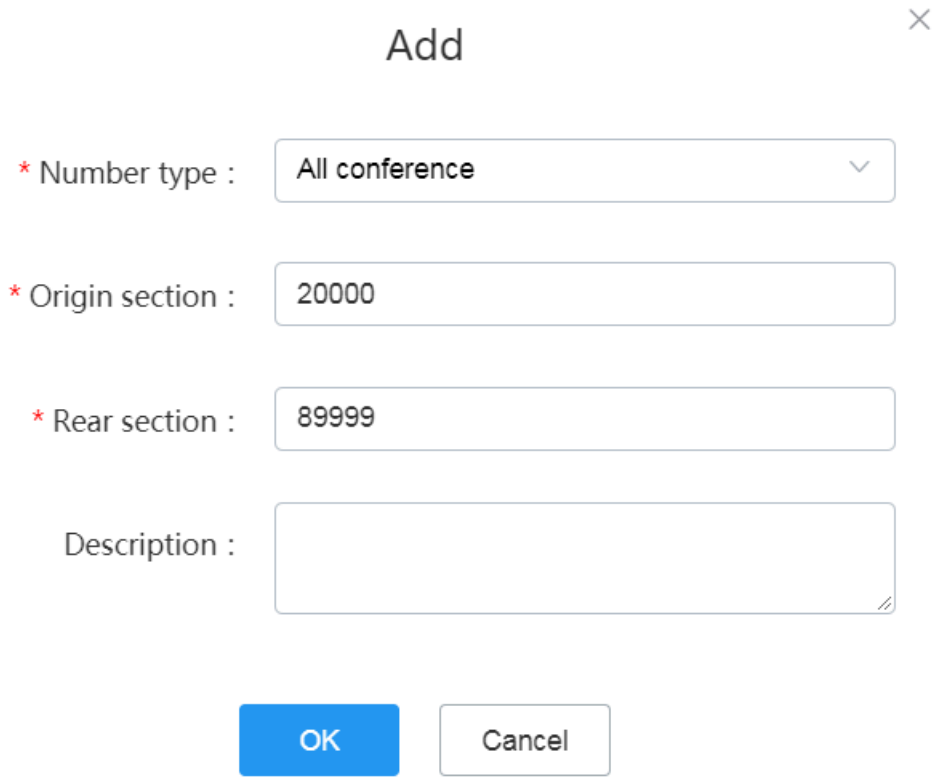


Table 15: Parameters of the number resource

Parameter	Description
Number type	Specify the type of the number. The supported types are as follows: • **System account**: it contains the user accounts and the room system accounts. • **All conference**: it contains the conference IDs of scheduled conferences, Meet Now conferences and VMRs. • **Meet Now** • **Scheduled conference** • **VMR** **Note**: if you set **All conference** and **Meet Now**, the system will use the **Meet Now** with priority. This can also be applied to **Scheduled conference** and **VMR**.

4. Save the configuration.

Related concepts

Parameters of User Account and Room System Account

Related tasks

Adding a Group

Add a User Account

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.

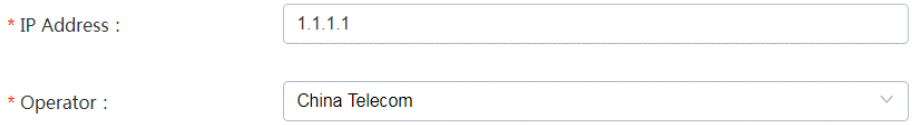


Table 16:

Parameter	Description
IP address	Specify the IP address for the external network.
Operator	Select the operator type. **Note**: 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.

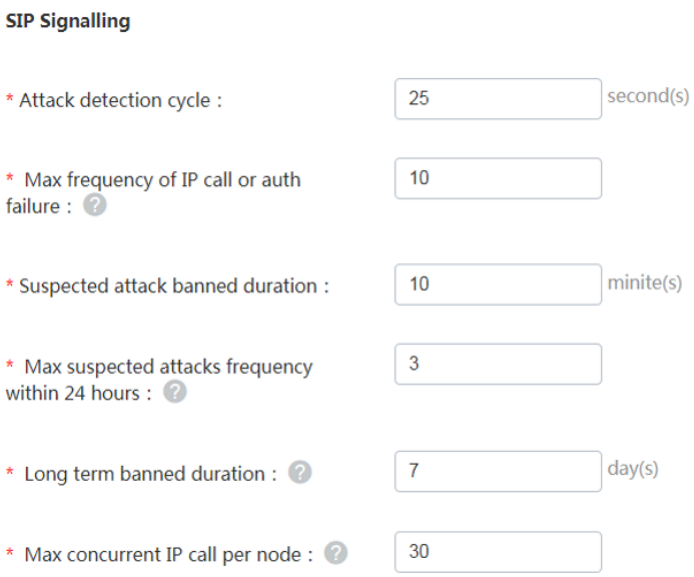


Table 17: Intelligent Security Strategy

Parameter	Description
Attack detection cycle	Specify the cycle for detecting an attack. **Default**: 25 seconds.
Max frequency of IP call or auth failure	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.
Suspected attack banned duration	Specify the duration of blocking the suspected attack. **Default**: 10 minutes.
Max suspected attacks frequency within 24 hours	It instructs YMS to block any source IP address where the suspected attacks come from, within 24 hours. Default: 3 times.
Long term banned duration	Specify the banned duration. **Default**: 7 days.
Max concurrent IP call per node	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. **Default**: 30.

3. 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.
4. 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

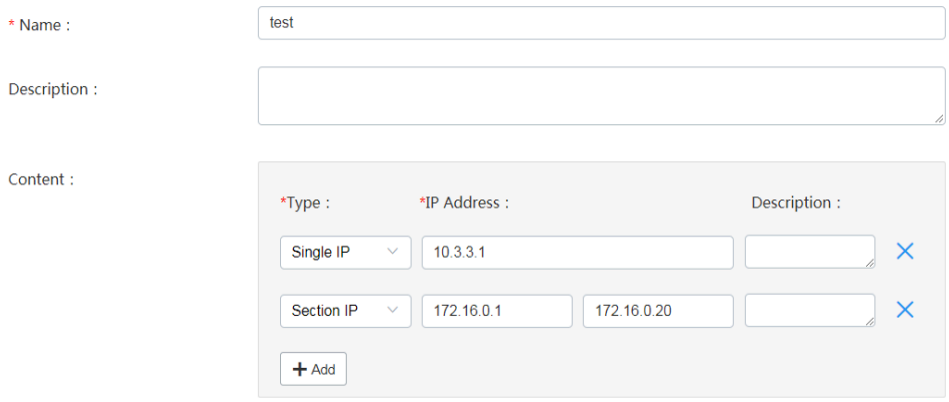
Communicating with the PSTN

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.



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.

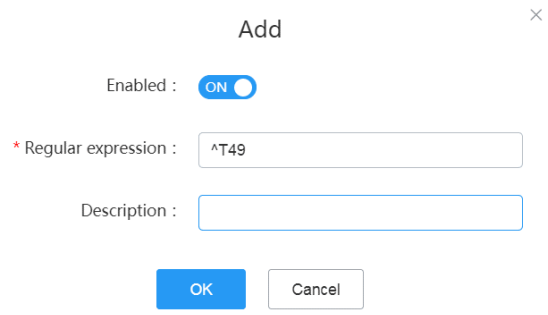


Table 18:

Parameter	Description
Enabled	Enable or disable this blacklist. **Default**: enabled.
Regular Expressions	Specify the Perl Compatible Regular Expressions (PCRE). **Note**: 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.
Description	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.

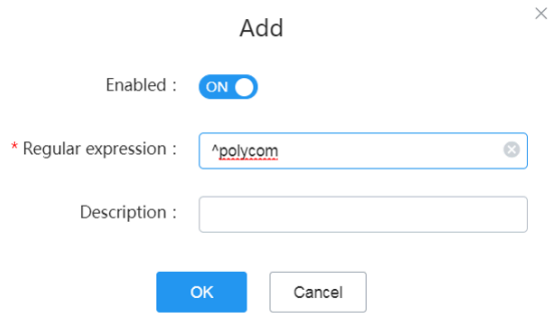


Table 19:

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

4. Click **OK**.

Configuring the Email Template

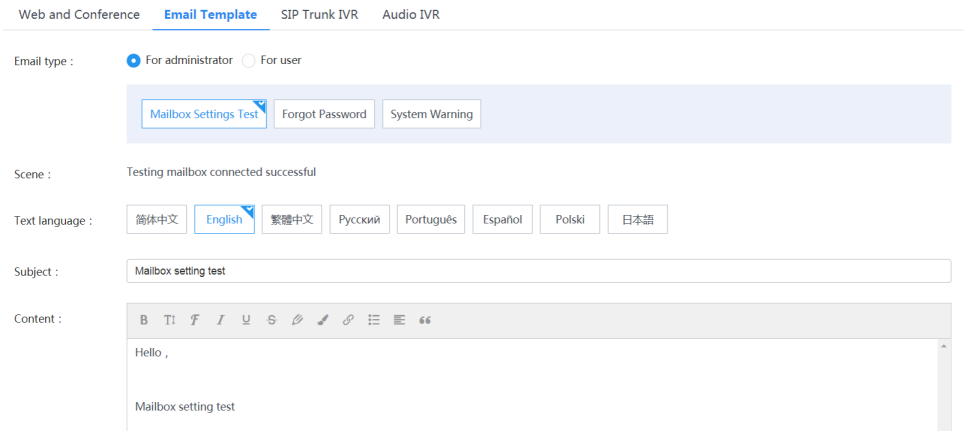
You can customize the email template for different uses. For administrators, they receive emails about the system alarm, SMTP mailbox testing or others. For users, they receive emails about the information of conferences that they are invited or create, the notification that the recording is finished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



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

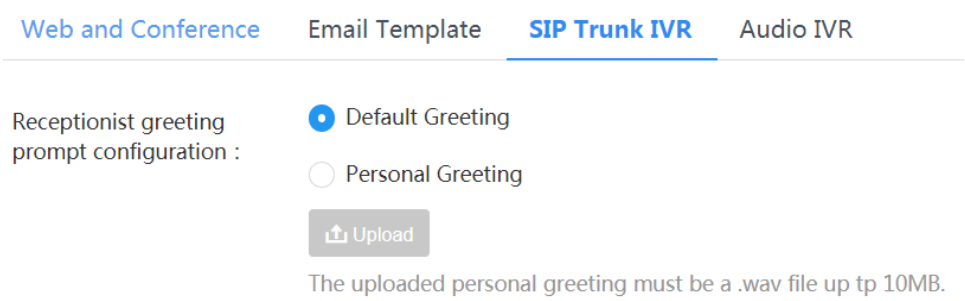
Dial *main_ivr@server domain name* to go to the SIP trunk IVR.

Procedure

1. Click **System Setting** > **Customization** > **SIP Trunk IVR**.

2. Configure the receptionist greetings, and do one of the following:

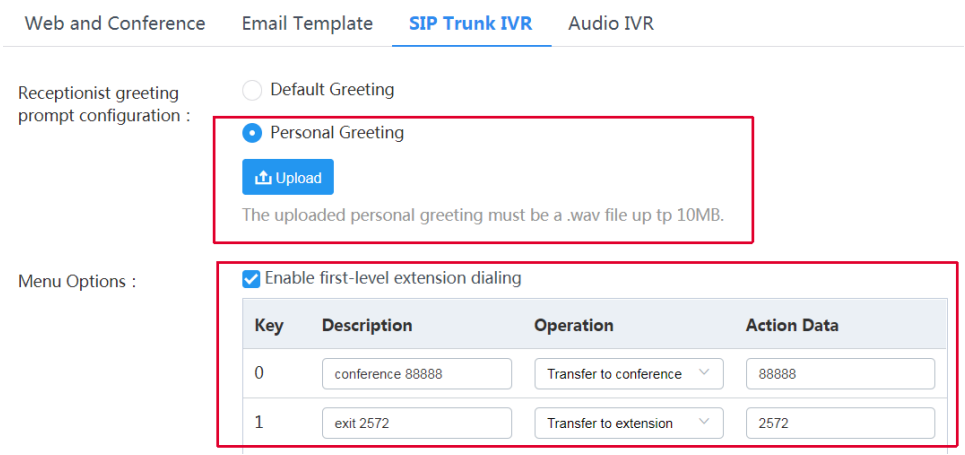
   - Select **Default Greeting**. The language depends on the IVR language, refer to Setting IVR language.



   - Select **Personal Greeting**.

     Click **Upload** to upload the desired file.

     Configure a feature for each key.



   - 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.

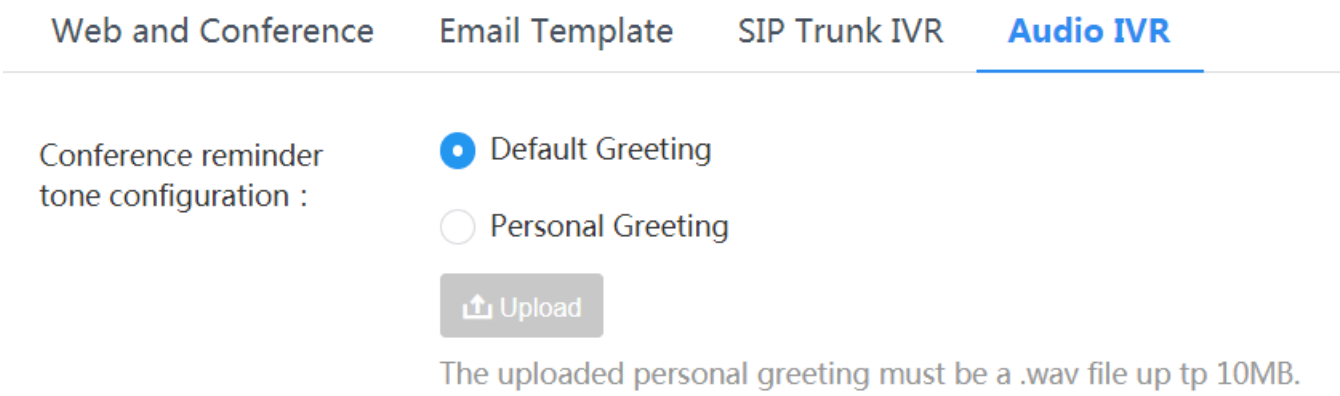
About this task

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:



- 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 for different situations.

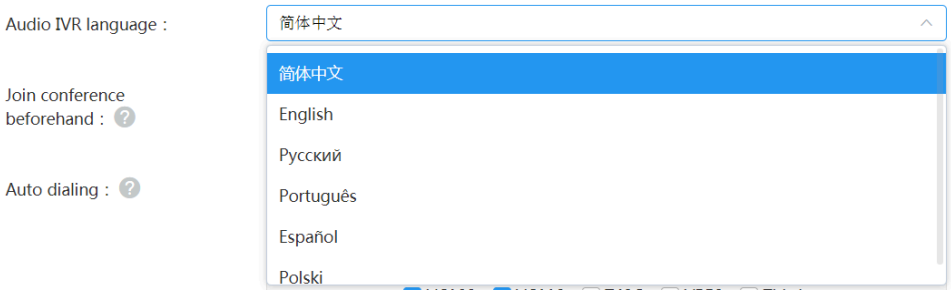
3. Save the configuration.

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 RTSP Gateway Service
- Face Recognition 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.

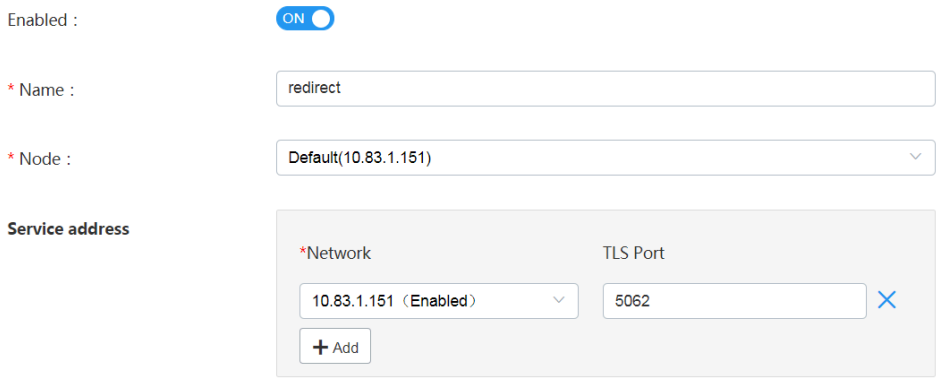
Before you begin

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.



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.

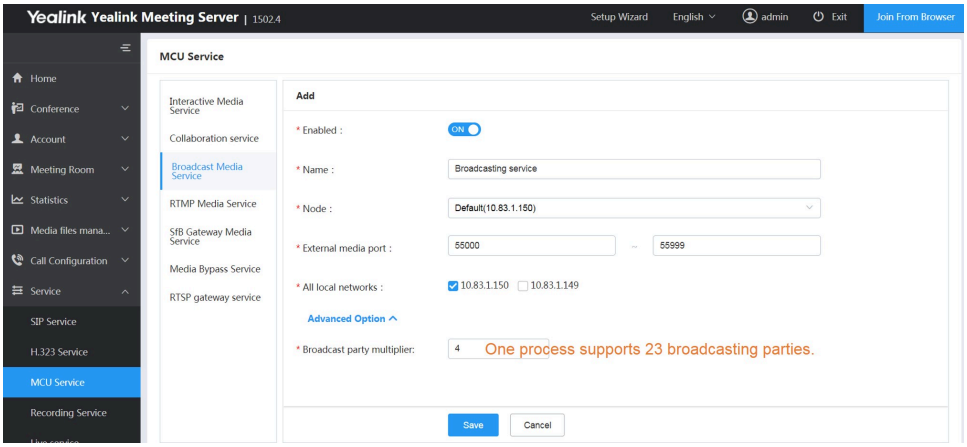
4. For VMR, refer to Enabling Broadcasting Interactive for VMR to enable **Broadcasting Interactive**.

- 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.

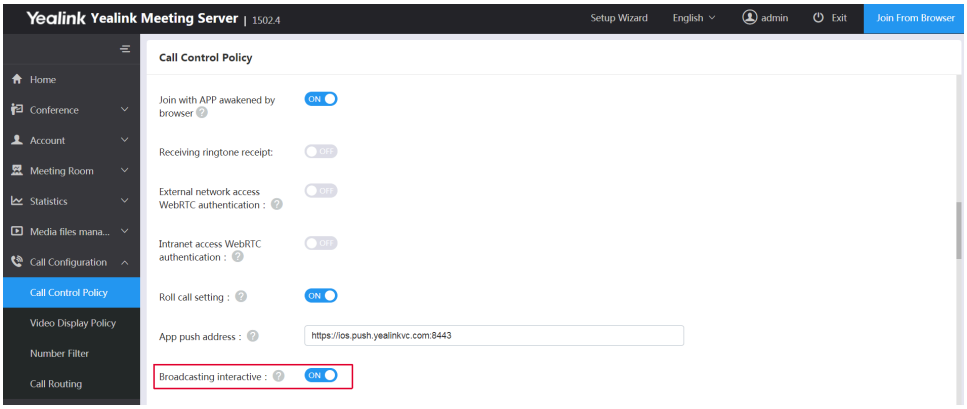
Before you begin

- 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.

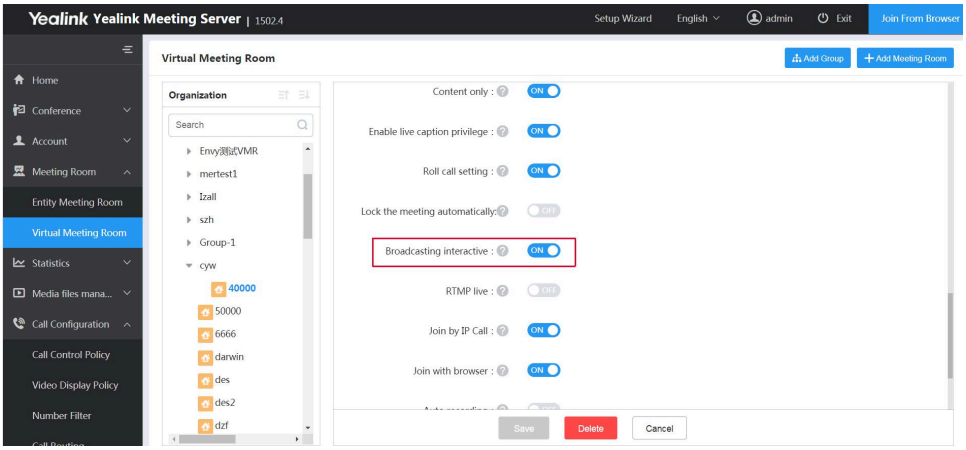
Procedure

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. Enabling Auto Recording

3. Customize the recording parameters, for example, Recording Template, Displaying the Recording Icon during Recording, Adding Watermark for Recording Files or others. For more information, refer to Managing the Recording Settings.

4. Enable recording privileges for user accounts, refer to Enabling the Recording Privileges for User Accounts.

5. For scheduled conferences, when users schedule conferences, users can set the recording privilege. For more information, refer to Yealink Meeting Server User Guide.

6. For VMRs, users can see Enabling the Recording Privileges for VMRs to set the recording privilege.

7. 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 2，5 or 6, you can skip this step.

Note: For YMS-registered devices with the recording privileges, including third-party devices and Yealink VC devices, YMS allows them do the following operations via DTMF. Press #7 to start the recording or #9 to end it. Besides, in discussion mode, press *7 to mute the speaker or *8 to unmute it. For more information, refer to **System Setting** > **Customization** > **DTMF**.

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.

Note: The maximum size of a single recording file is 2GB by default. When the size of a single recording file reaches the limit, the system will automatically end the recording, generate a recording file, and start a new recording. However, if there is not enough recording space, you cannot start a new recording.

- Enabling the Recording Service
- Enabling Auto Recording
- Managing the Recording Settings
- Enabling the Recording Privileges for User Accounts
- Enabling the Recording Privileges for VMRs
- Managing the Recording Files
- Managing the Sharing Link
- Viewing the Recording Log
- Managing Screenshot Files

Enabling the Recording Service

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

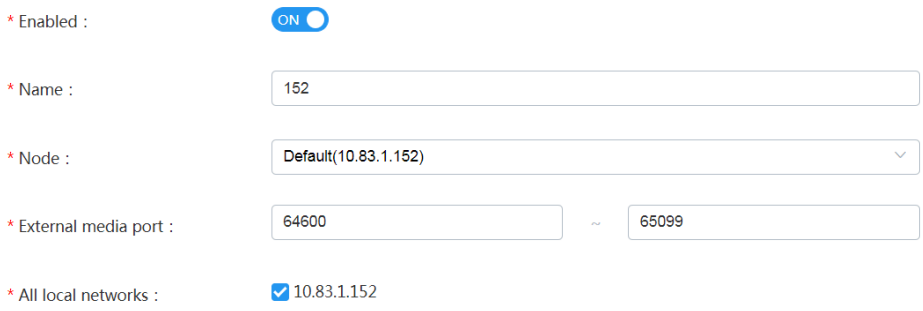
Before you begin

- 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.



Enabling Auto Recording

If your enterprise requires to record every conference, you can enable this feature globally.

About this task

Note:

For scheduled conferences or Meeting Now conferences:

- When users schedule conferences or create Meet Now conferences, the auto recording setting is same as the one you set in the Global Setting.
- During the conference, if you enable the auto recording 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 auto recording feature on the Conference Control page, refer to Yealink Meeting Server User Guide.

For VMRs:

- When adding or editing VMRs, the auto recording setting is same as the one you set in the Global Setting.
- During the conference, if you enable the auto recording in the Global Setting, it does not affect the ongoing conferences.
- For more information about setting the auto recording feature for VMRs, refer to Enabling the Recording Privileges for VMRs.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Auto recording** and save it.

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 recording template applies to the conference organizer.

- 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.
Video resolution	Set the maximum video resolution for the recording file. Default: 720P/30FPS.
Audio and video code rate	Set the maximum bandwidth for the recording file. **Default**: 2 Mbps. If you set the **Video resolution** as 360P and the **Audio and video code rate** as 4M, you can only record a video of 360P even though the bandwidth is 4M.
Layout	Set the layout of the recording file. • Default layout: the layout used in the conference. • 1+N, the default value of N is 4. When a participant is sharing content, you can see the content as your large video image, and the video images of participants are reduced to thumbnails. When no participant is sharing content, you can see the current speaker as your large video image (the voice-activated feature is enabled and the voice-activated time is 2 seconds) and other participants are reduced to thumbnails. When the number of participants is larger than 4, their video images will be switched automatically in live thumbnails every 30 seconds. • Picture in picture: when a participant is sharing content, you can see the content as your large video image and the video image of the speaker is reduced to a thumbnail in the bottom-right corner. When no participant is sharing content, you can see the current speaker as your large video image (the voice-activated feature is enabled and the voice-activated time is 2 seconds).
Recording File	If you select the video, when you finish the recording, video files and images will be generated. If you 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.

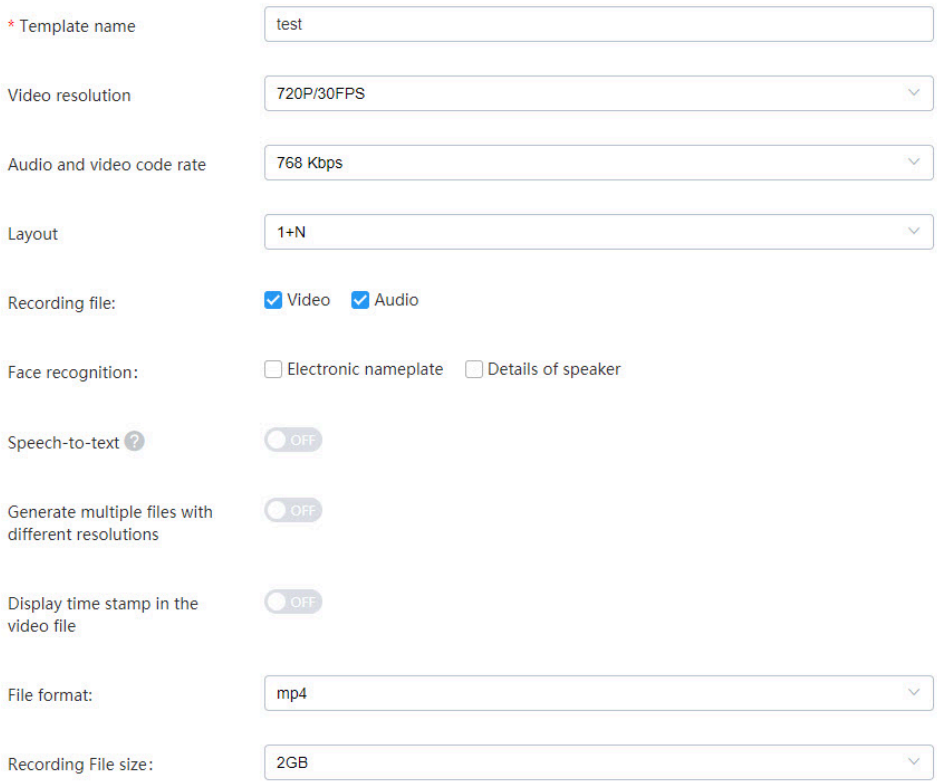
Parameter	Description
Face recognition	• Electric nameplate: if you enable it, YMS can automatically recognize the participant face and display the participant name. **Note:** The enterprise administrator manages the face database. If participants whose faces cannot be found in the face database or be identified by YMS, they are called guests. YMS can recognize up to 50 electronic nameplates (The number depend on your YMS performance). • Details of speaker: if you enable it, YMS can automatically present a brief introduction of the participant. **Note:** The enterprise administrator sets the brief instruction. According to the order of recognizing the participant face, YMS can present the brief introductions of the first 3 recognized participants at most.
Speech-to-text	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.
Generate multiple files with different resolutions	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.
Display time stamp in the video file	If you enable this configuration, a timestamp with the format as xxxxxx-xx xx:xx:xx, will be displayed in the bottom-right corner of the generated recording files, for example, 2019-07-22 17:40:04.
File format	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**.

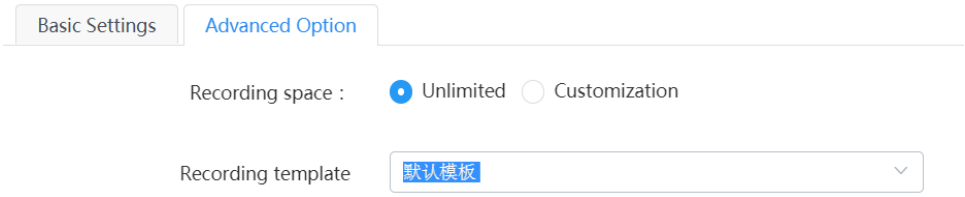
3. Set the parameter and save it.



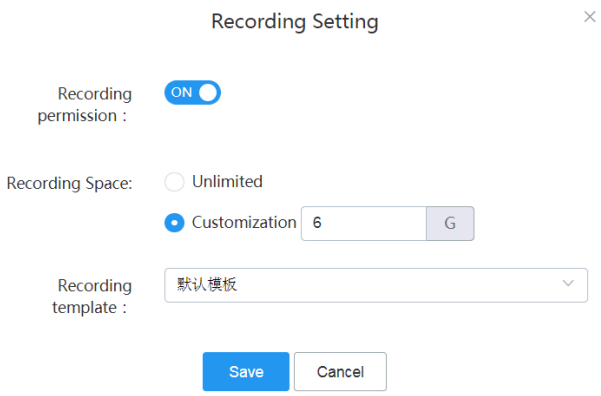
4. You can select users who can use this template. You can also do it later. Refer to Managing Recording Templates or Selecting Recording Templates for Accounts.

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.



- **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.

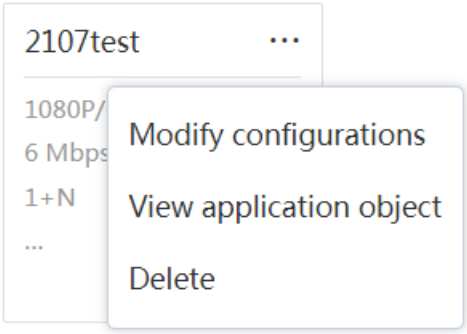


Managing Recording Templates

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

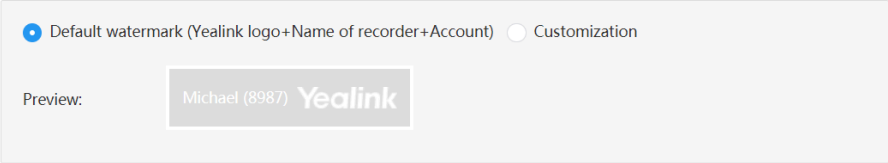
1. Click **Media file management** > **Recording Setting**.
2. Enable **Show recording icon**.

Adding Watermark for Recording Files

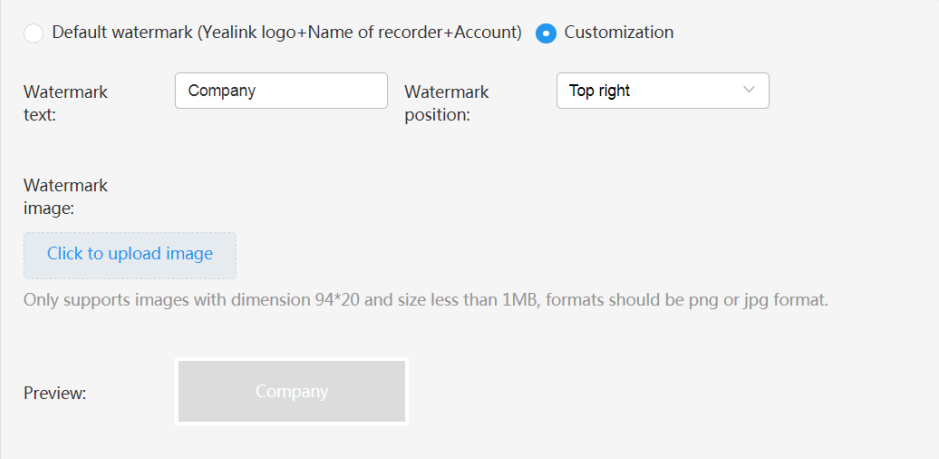
If you enable **Add watermark to recording file**, you can see a watermark in the top-right corner of the generated recording file.

Procedure

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



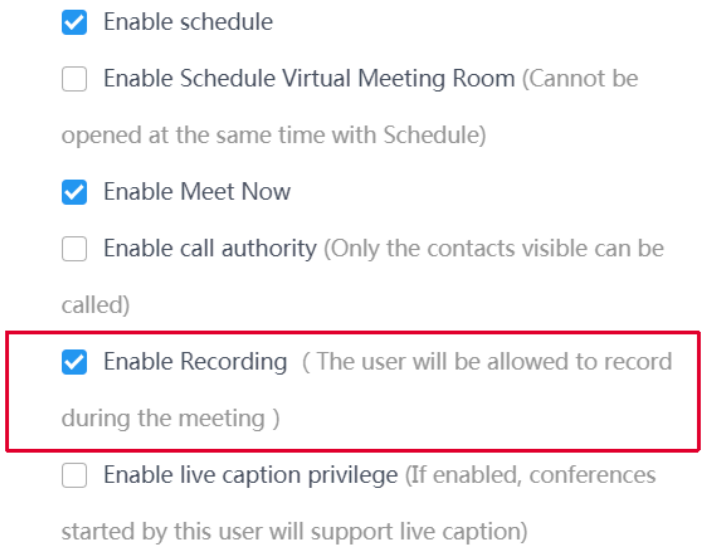
   - **Customization**



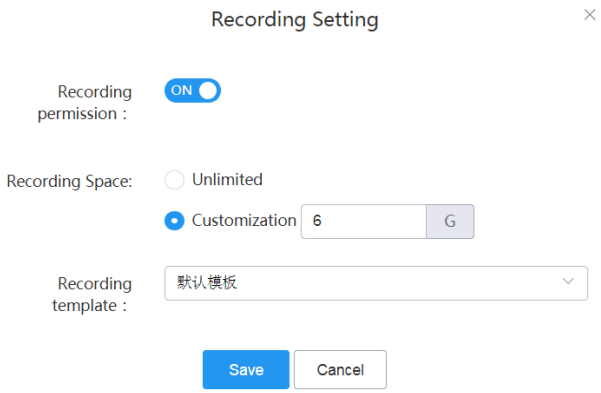
Enabling the Recording Privileges for User Accounts

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.



- **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.



Enabling the Recording Privileges for VMRs

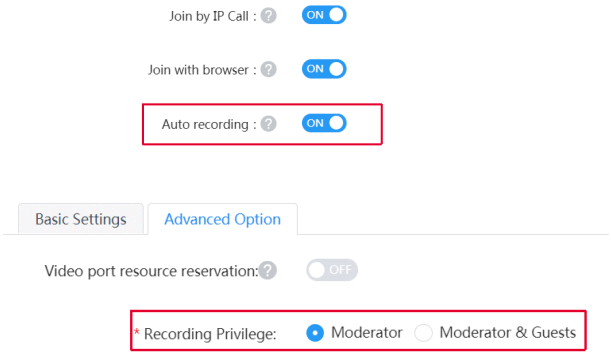
Procedure

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
- Sharing Recording Files
- Making Backups for Recording Files
- Viewing the Usage

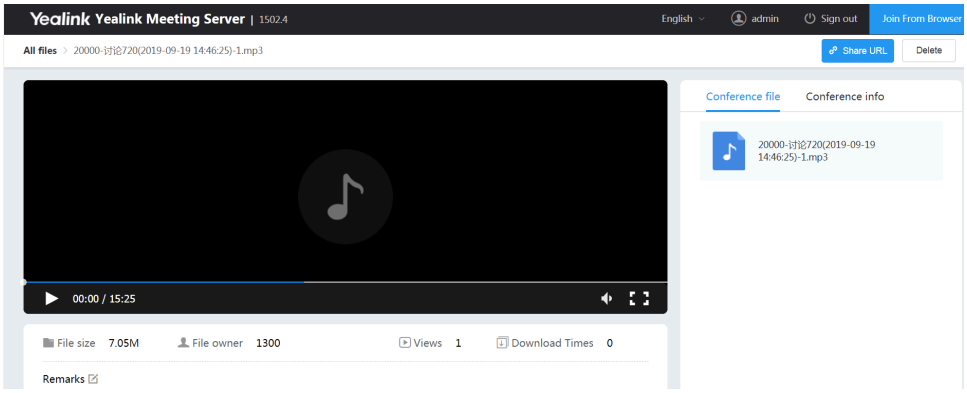
Managing the Recording Files

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. The shared links are in the tab of **URL Share MGMT**.
- Click **Delete** in the top-right corner, and delete the recording according to the prompts. If you share the file with others, the shared file will be deleted too.
- 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.

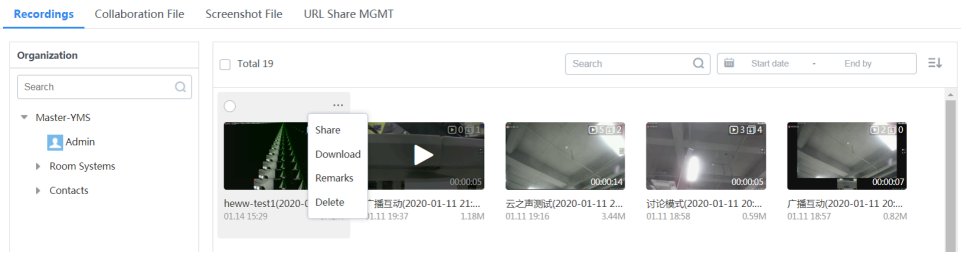
Related tasks

Managing the Sharing Link
Disabling the Sharing Link

Sharing Recording Files

Procedure

1. Click **Media file management** > **File Management** > **Recordings**.
2. Click in the top-right corner of the file and select **Share**.



3. Do one of the following to share the file:

- Share URL: share the link with other users and set the link parameters. The shared links are in the tab of **URL Share MGMT**.
- Internal sharing: share the file with other users in your enterprise. The users that the file owner can share with depends on his visible authority. Users who receive the shared file can find the file is in the tab of **Shared file** after logging in to YMS.

Making Backups for Recording Files

You can making backups for recording files manually or automatically.

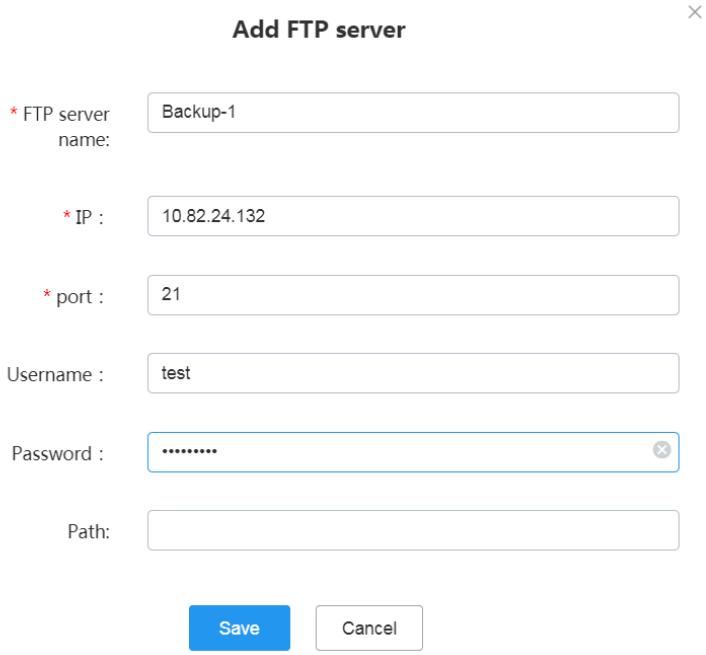
Before you begin

The FTP server is available.

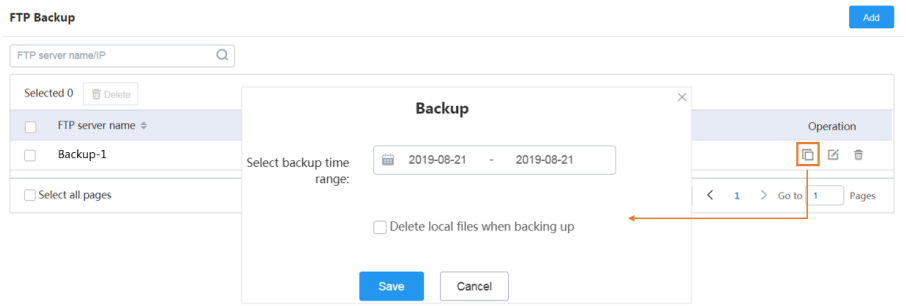
Procedure

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.



3. Click  .



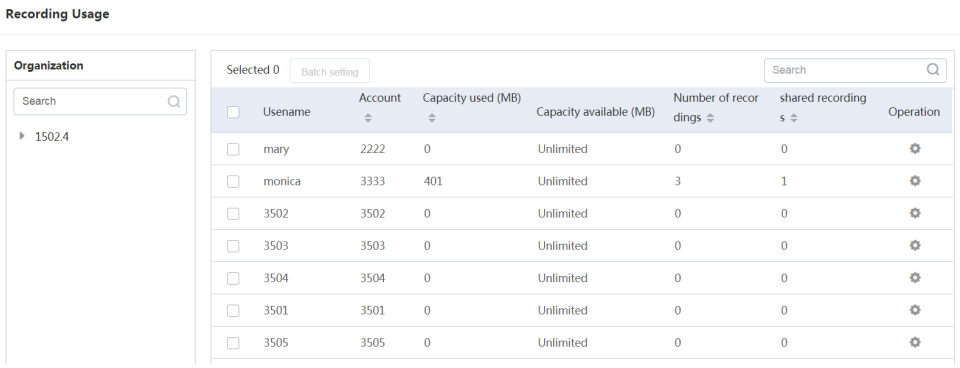
4. You can also click **Automatic backup settings** to set the auto backup.

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

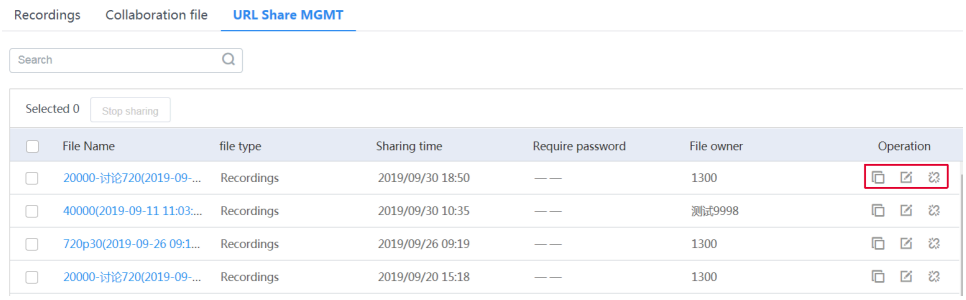
Click **Media file management** > **Recording usage**.



Managing the Sharing Link

Procedure

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



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

Related tasks

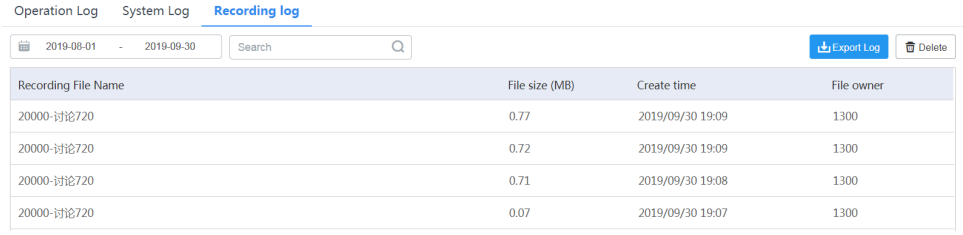
Managing the Recording Files

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**.



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

Managing Screenshot Files

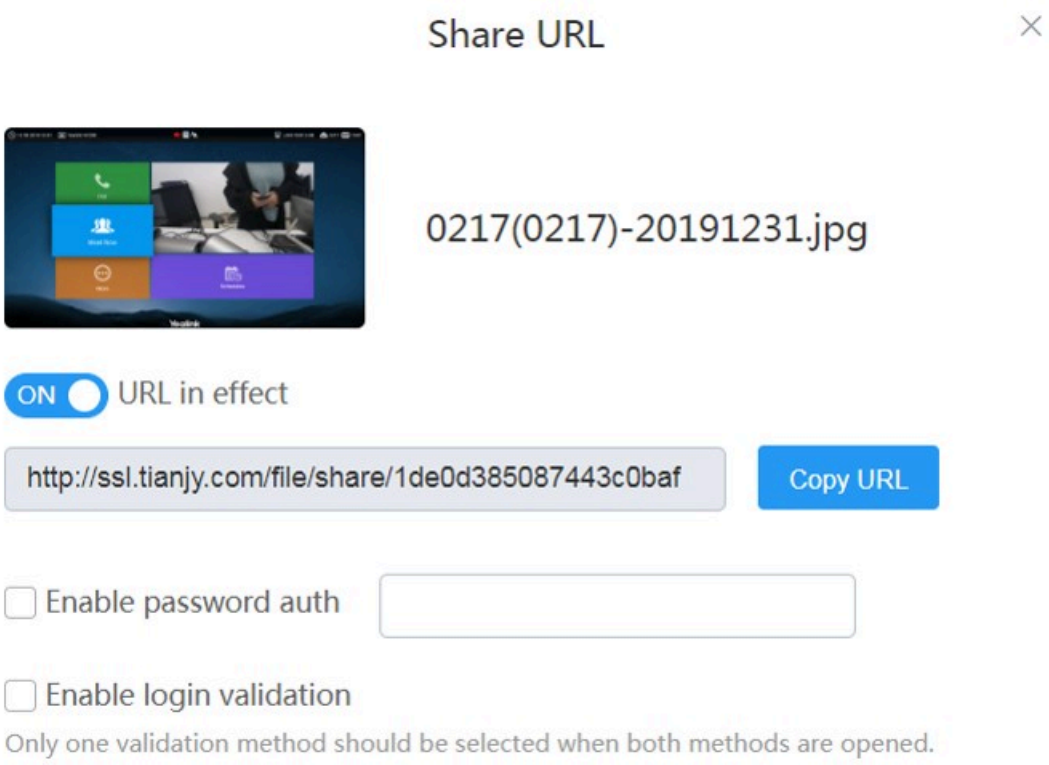
If users have the recording privilege, they also have the privilege to take screenshots. They can only take the screenshots of their devices, and the screenshots will be sent to YMS automatically. For more information, refer to the device user guide. The disk space of the screenshot is configurable, to configure it refer to Setting the Data Space .

Before you begin

- Enabling the Recording Service
- Enabling the Recording Privileges for User Accounts

Procedure

1. Click **Media file management** > **File Management** > **Screenshot File**.
2. Click the desired screenshot file.
3. Click ••• in the top-right corner of the screenshot and do one of the following:
   - Click **Share URL** in the top-right corner and configure the corresponding parameter. Other people can download this file via this URL. The shared links are in the tab of **URL Share MGMT**.



Note: If you enable **Enable password auth**, others need to enter the password to view this file when they open the link. If you enable **Enable login validation**, others need to enter the login credentials to view this file when they open the link.

   - Click **Download**, and download the file according to the prompts.
   - Click **Delete**, and delete the file according to the prompts.

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 Port 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

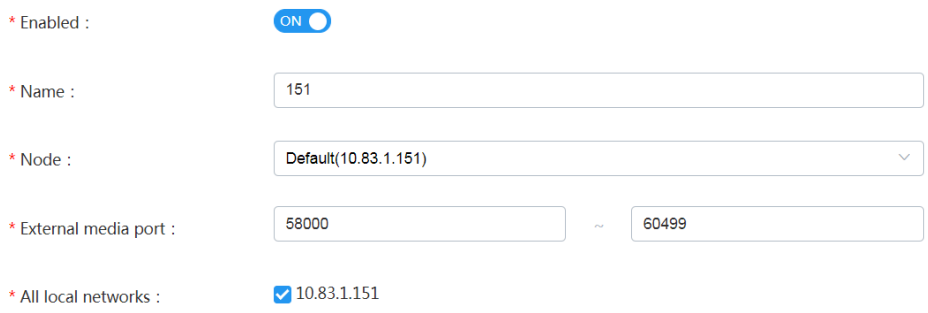
Configuring the REG Trunk Service

Configuring the H.323 Gateway

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).



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:

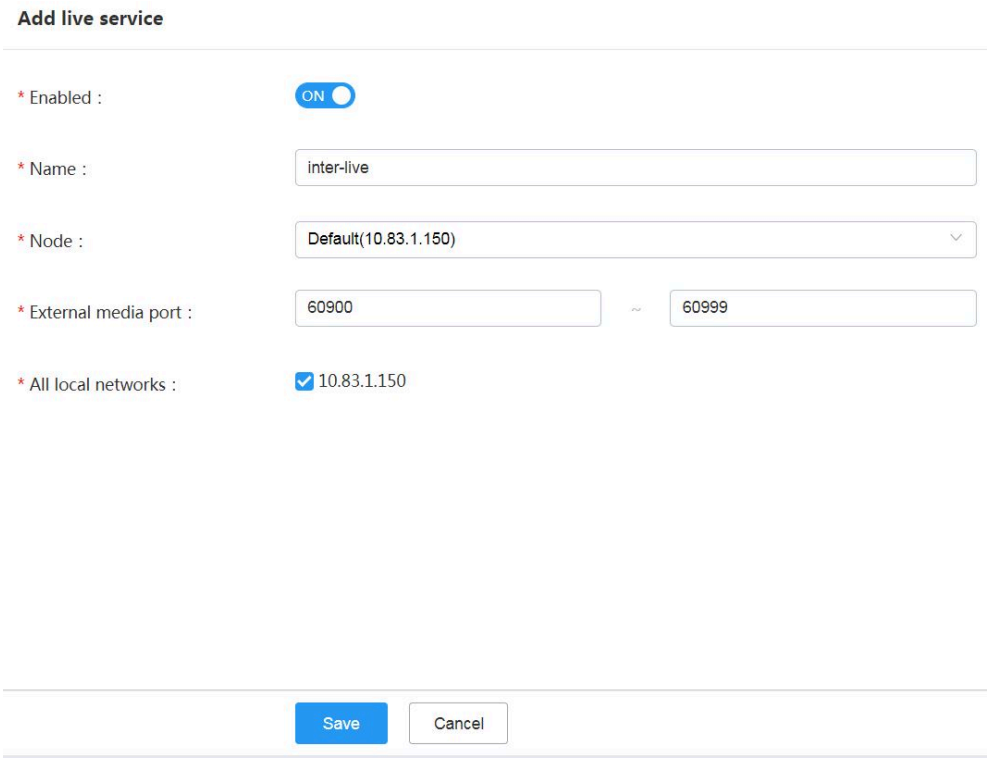
- The server can access the external network
- If your company has limitation to the web surfing, make sure that the server has the video privilege.

- 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.



Configuring YMS System RTMP Live

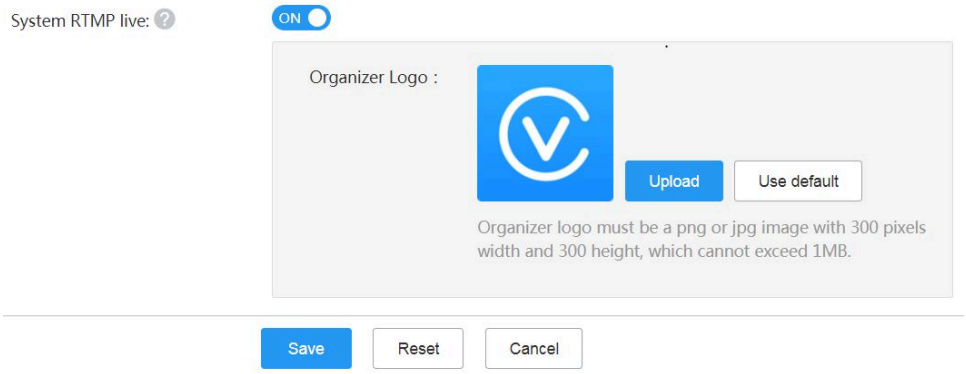
Before you begin

- Activating a License.
- Enabling Live Service.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.

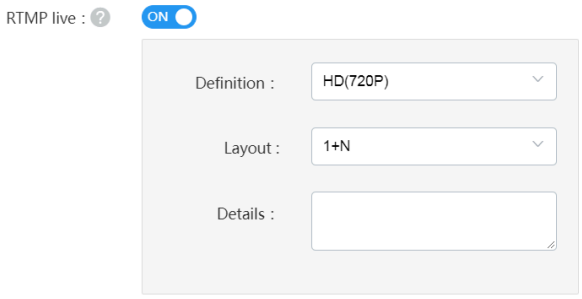
2. Enable **System RTMP live**.



Setting the RTMP Live for VMRs

Procedure

1. Click **Meeting Room** > **Virtual Meeting Room**.
2. Do one of the following:
   - If you want to add a VMR, click **Add Meeting Room**.
   - If you want to edit a VMR, click .



3. 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. **Default**: disabled.
Definition	It refers to the video resolution that the MCU sends to a public streaming services. The supported video resolution is as below: • 1080P(1080P) • HD(720P) **Default**: HD.

Parameter	Description
Layout	Configure the video layout displayed in the webcast. The supported layouts are as below: • **1+N**: 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. • **Picture in picture**: 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. • **Selected speaker**: 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. • **Default controlled layout**: the audience can see the same video layout as the conference participants. Besides, this layout will change as the conference moderator changes the video layout.
Event details	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

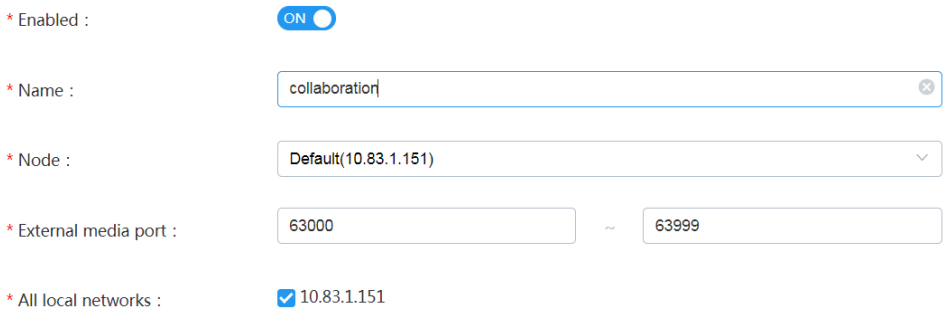
If you want to use the collaboration feature of the endpoint, you need to enable the collaboration service.

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.



4. Save the configuration.

Managing Collaboration Files

Before you begin:Setting the Collaboration Service

- Managing Collaboration Files
- Managing the Sharing Link

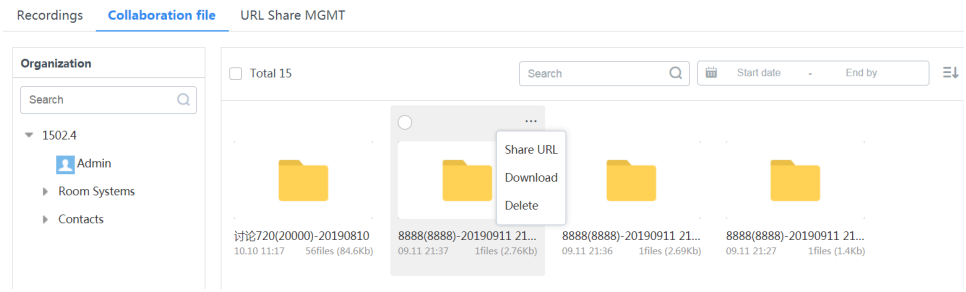
Managing Collaboration Files

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:

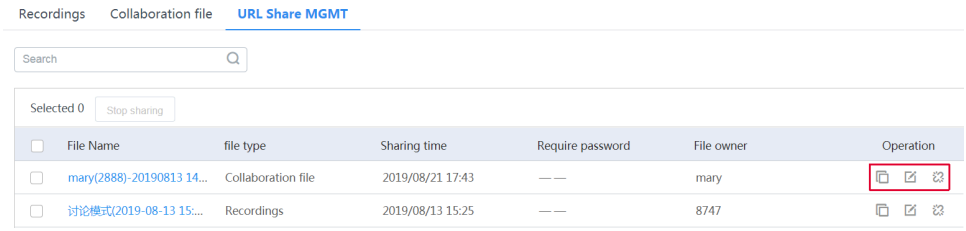


- Click **Share URL**, and share the link with others and set the link parameter.
- Click **Delete** to delete the collaboration file.
- Click **Download** to download the collaboration file.

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.

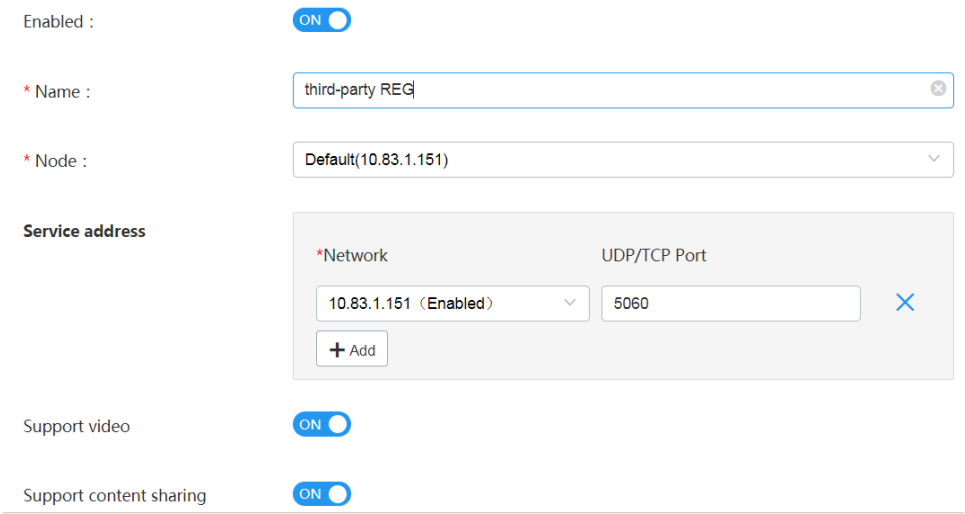
About this task

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.



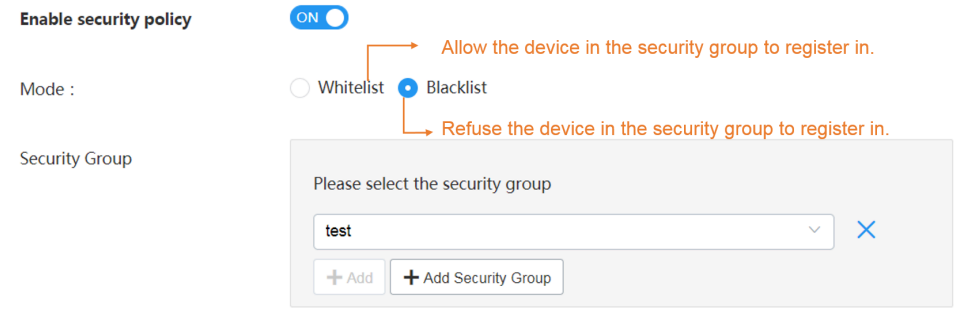
4. Enable **Media Bypass** to improve the server performance and to support a larger number of participants in the conference. Note that the third-party devices have lower compatibility.

   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.

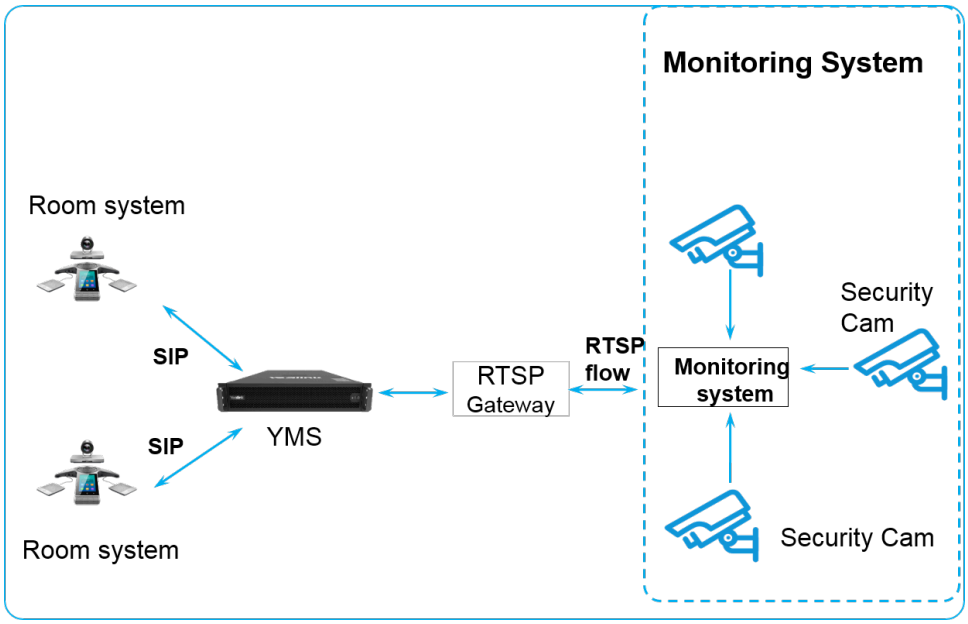
   For adding a security group, seeAdding a Security Group



Configuring the RTSP Gateway Service

Supporting GB/T28181, YMS allows you to connect the monitoring devices to YMS conferences via RTSP, so the remote control can be realized better with the combination of the video and the monitoring device in the large enterprise, or when an emergency occurs.

About this task

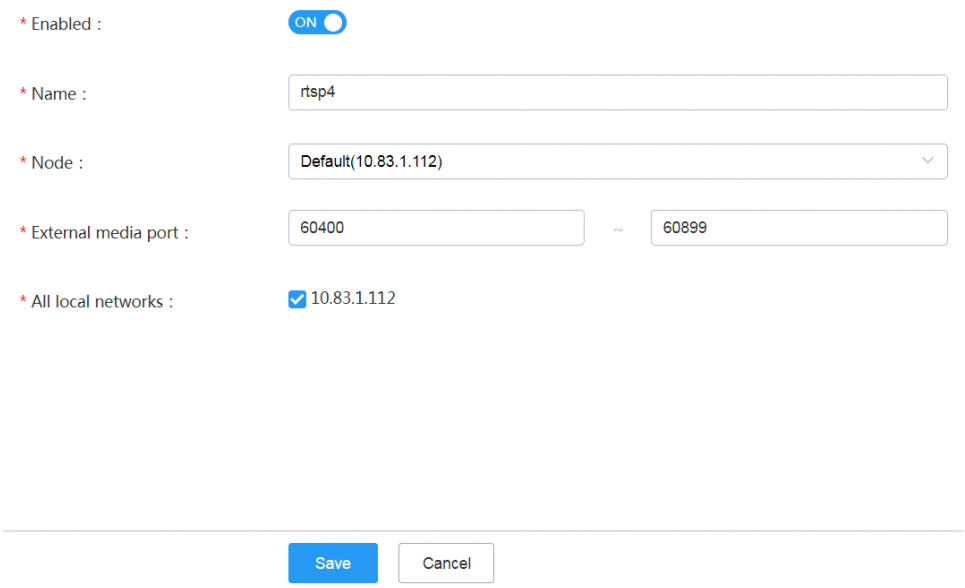


After you enable the RTSP gateway service, you can invite the desired monitoring device to YMS conferences by URI. Take two examples, selecting RTSP when adding other accounts, or selecting RTSP and entering the URI address (for example, rtsp://numax:numax@211.162.122.83:8554/live/1) in the number field when inviting others to a conference.

Procedure

1. Click **Service** > **MCU Service** > **RTSP gateway service**.
2. Add a RTSP gateway service.

3. Set the parameter and save it.



Face Recognition Service

You can follow the steps below to configure the face recognition service:

1. Installation of the Face Recognition Service

2. Enabling the Face Recognition Service

3. Registering Faces or Registering Faces (Quick Registration for External Users). If participants whose faces cannot be found in the face database or be identified by YMS, they are called guests.

4. Moderators go to the Conference Control page to control the conference. In the **Selected Speaker** and **1+N** layout, moderators can enable **Electronic nameplate** to recognize the participant role and display the participant name, and can enable **Details of speaker** to present a brief introduction of the participant. For more information, refer to Yealink Meeting Server User Guide.

Note: By default, one conference can recognize 10 human faces and occupies one AI face port.

- Installation of the Face Recognition Service
- Enabling the Face Recognition Service
- Registering Faces
- Registering Faces (Quick Registration for External Users)

Installation of the Face Recognition Service

- Downloading the Installation Package
- Installing the Face Recognition Service

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:

     ```
     wget address    # It is the address for downloading the installation package (you can obtain the address from Yealink technical support engineers) to #
     ```

- **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 desired installation package on the pop-up window.

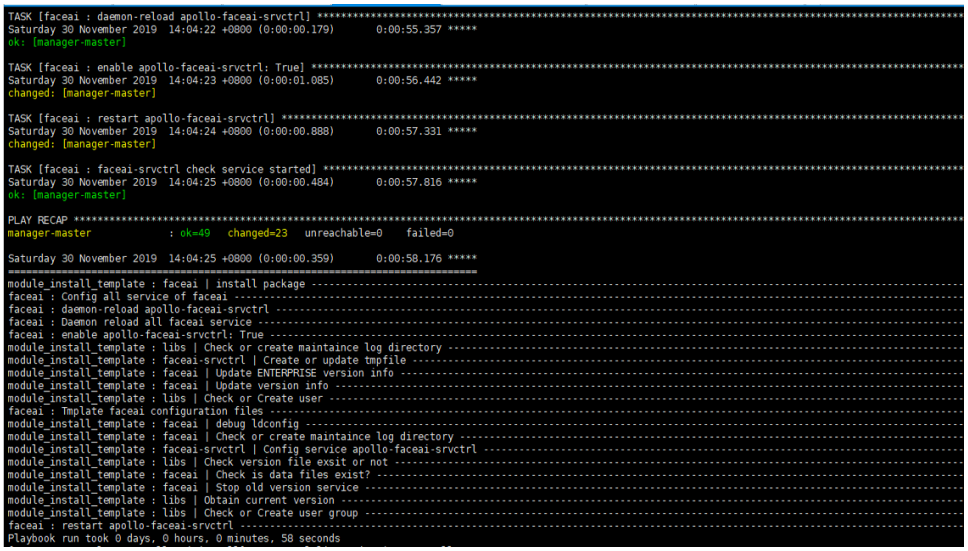
Installing the Face Recognition Service

Procedure

1. Run the following command:

   ```
   cd /usr/local                    #go to the directory where the installation package locates#
   tar xzf YMS-AI-release-x.x.x.x.tar.gz        # unzip the installation package (change x.x.x.x to the version number you want to install)#
   cd apollo_ai_install                # go to the installation directory#
   tar xzf ai_install.tar.gz          # unzip the installation script#
   ```

2. Run command ./install.sh to install the face recognition service.

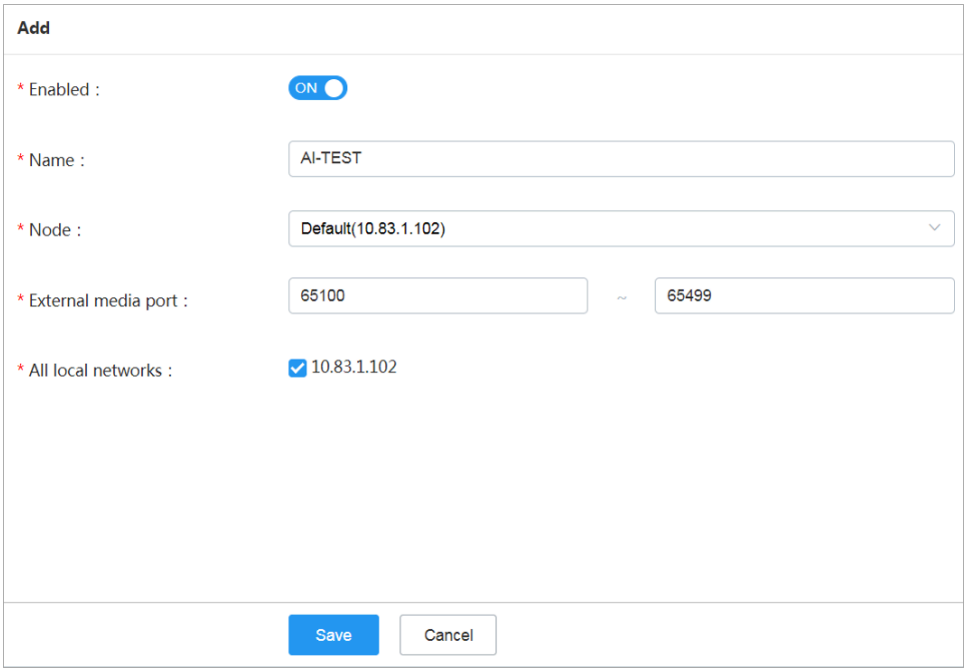


Enabling the Face Recognition Service

Procedure

1. Click **Service** > **AI service** > **Add**.

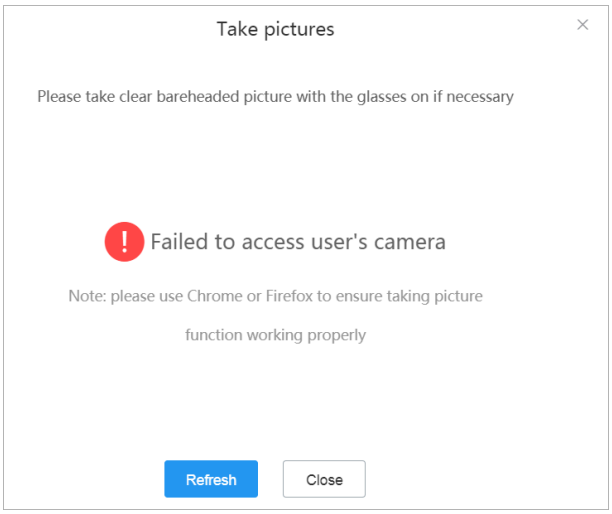
2. Set the parameter and save it.



Registering Faces

Before you begin

If you want to take photos by clicking, you need to meet two requirements. One is using Google Chrome or Firefox as your browser, and the other is accessing YMS via HTTPS.



Procedure

1. Click **AI management** > **Face database management**.
2. Do one of the following:
   - For enterprise users, find the desired user from the enterprise organization on the left side.
   - For external users, click **Face registration** in the top-right corner.
3. Set the face parameter and save it.

Registering Faces (Quick Registration for External Users)

We provide links or QR codes (contact Yealink technical support) for external users to register faces. The link are as below:http://DMIP/aiExternalPCGuest (PC)/http://DMIP/aiExternalmobileGuest (Mobile).

About this task

Note: You can subscribe to this service from Yealink technical support.

Procedure

1. External users can visit the link or scan the QR code.
2. Set the face parameter and save it.

   Note: The face information is stored in the face database and does not belong to any group.

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.

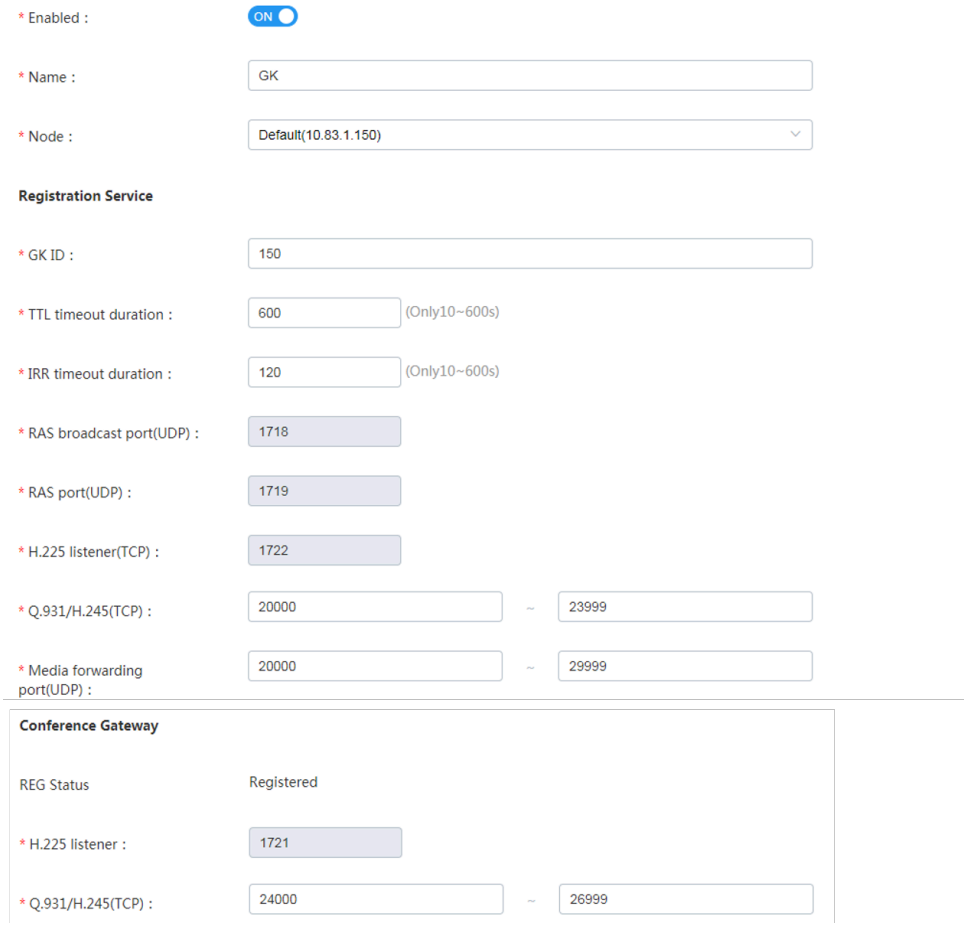


Table 22: Basic Parameters

Parameter	Description
H.235 encryption	The supported types are as follows: • **Optional**—negotiate with the remote party about whether or not H.235 encryption can be used in H.323 calls. • **Compulsory**—H.235 encryption has to be used in H.323 calls. • **Disable**—H.235 encryption is disabled in H.323 calls. **Default**: Optional.
H.239	Enable or disable the H.239. **Default:** 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.
Conference media ByPass	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. **Note**: it is disabled by default. If **Conference media ByPass** is enabled, media bypass service should be enabled too. For more information, see Configuring the Media Bypass Service.

4. Save the configuration.

Enable GK Registration for Accounts

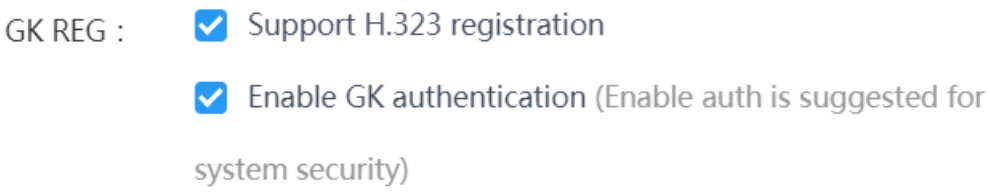
Procedure

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 GK注册.

  Set the parameter.



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.

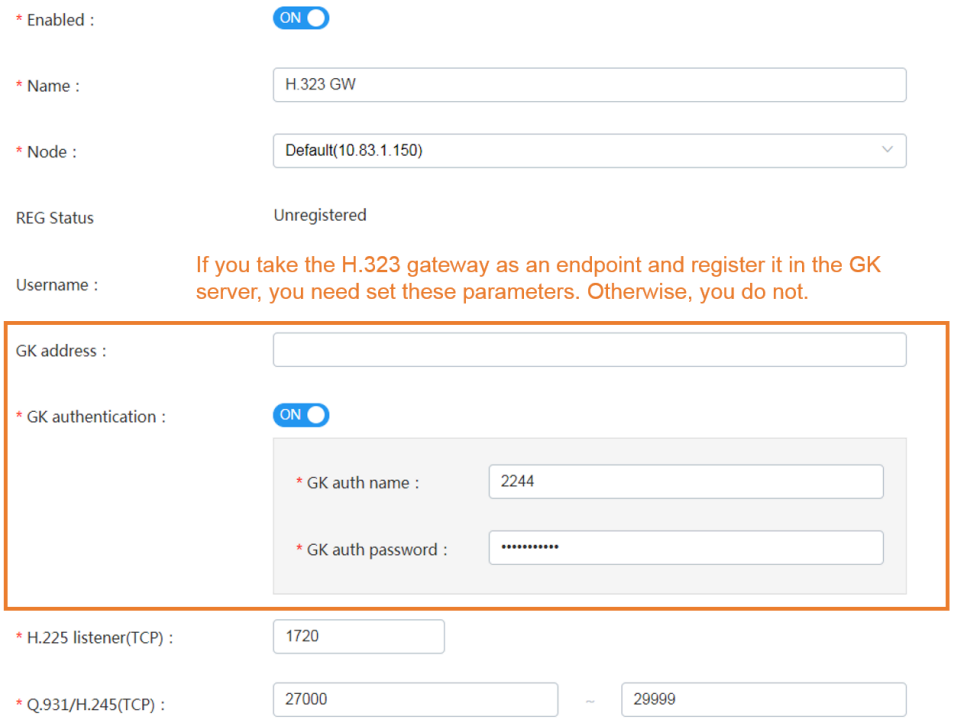
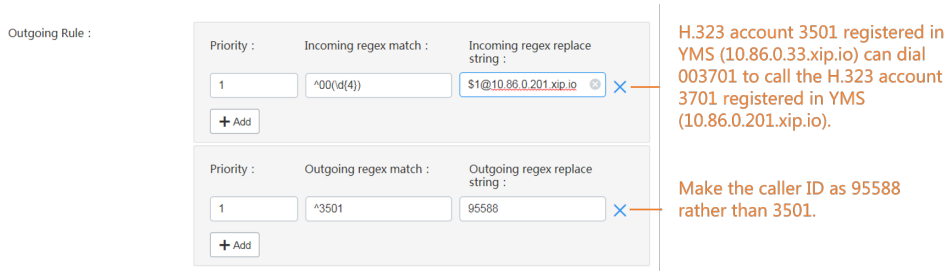


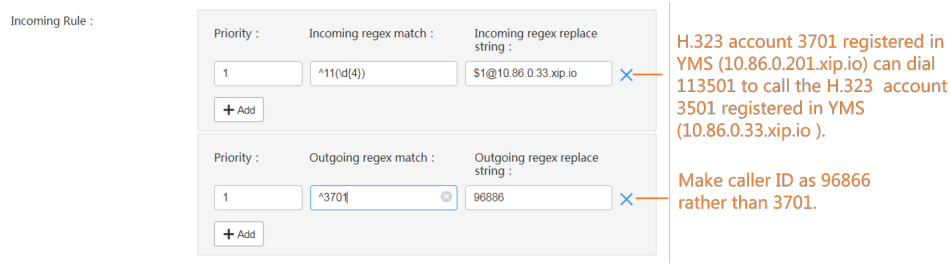
Table 23: Basic Parameters

Parameter	Description
H.235 encryption	The supported types are as follows: • **Optional**—negotiate with the remote party about whether or not H.235 encryption can be used in H.323 calls. • **Compulsory**—H.235 encryption has to be used in H.323 calls. • **Disable**—H.235 encryption is disabled in H.323 calls. **Default**: Optional.
H.239	Enable or disable H.239. **Default:** enabled. When the H.323 devices join YMS video conferences via H.323, H.239 is used to receive and share content.
H.460	Enable the H.460 protocol to support firewall traversal for H.323 signaling or not.
Conference media ByPass	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. **Note**: it is disabled by default. If **Conference media ByPass** is enabled, media bypass service should be enabled too. For more information, see Configuring the Media Bypass Service.

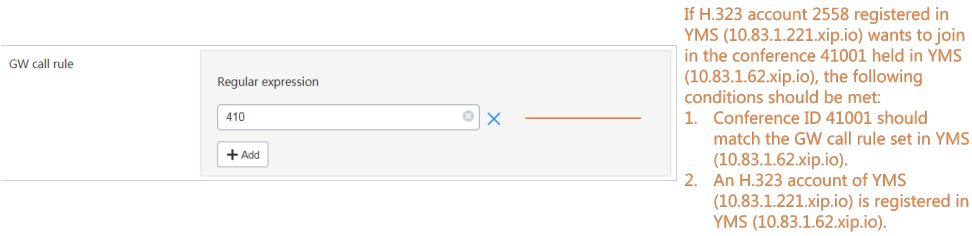
4. Click **Advance Option**, and configure the outgoing call rule.



5. Configure the incoming call rule.



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.



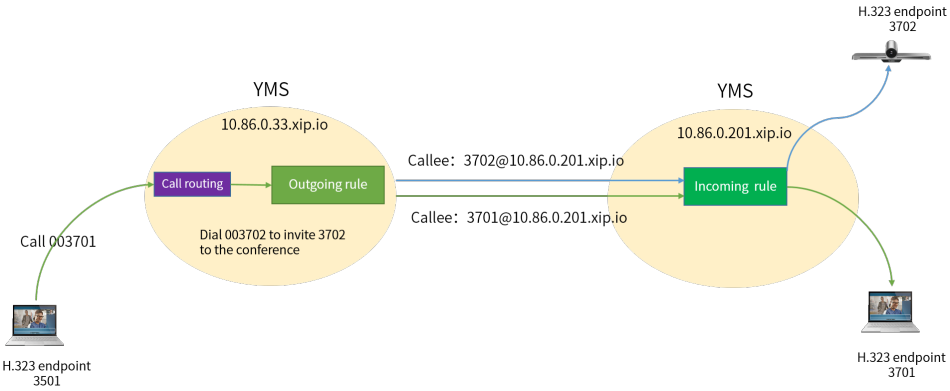
7. Save the configuration.

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

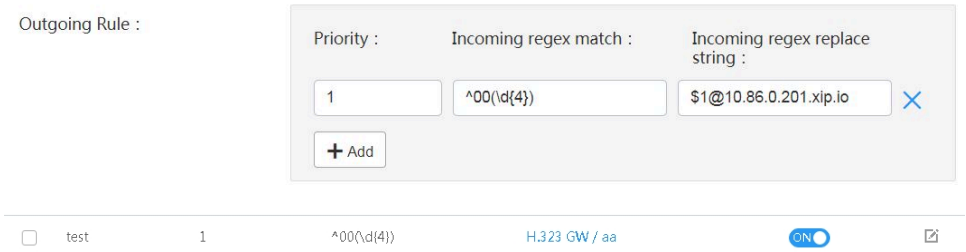
Related concepts

Common Regular Expressions and Replacement Strings

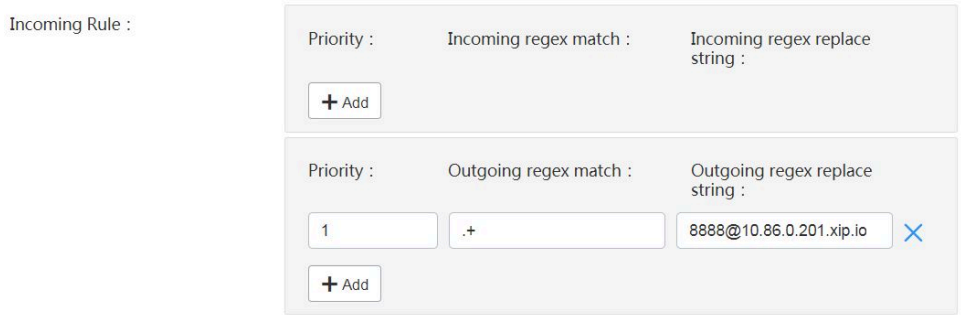
H.323 Gateway Example



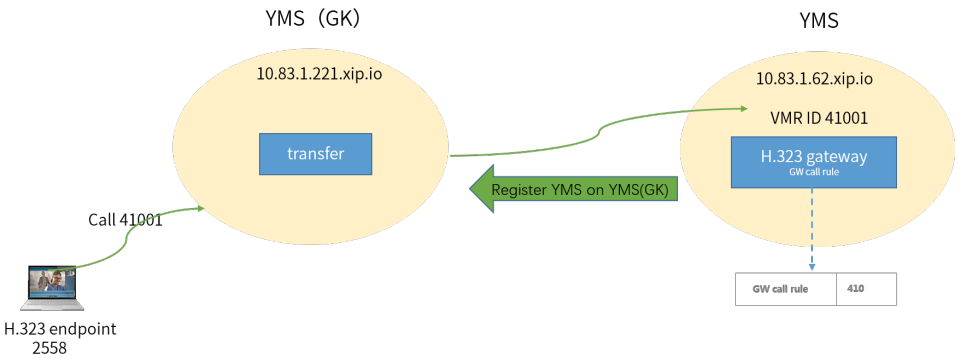
- **Situation**
  - H.323 account 3501 can dial 003701 to call another YMS H.323 account 3701. You can make the caller ID displayed as 8888 rather than 3701.
  - In a conference, you can dial 003702 to call YMS account 3702 to join the conference. You can make the caller ID displayed as 8888 rather than 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



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

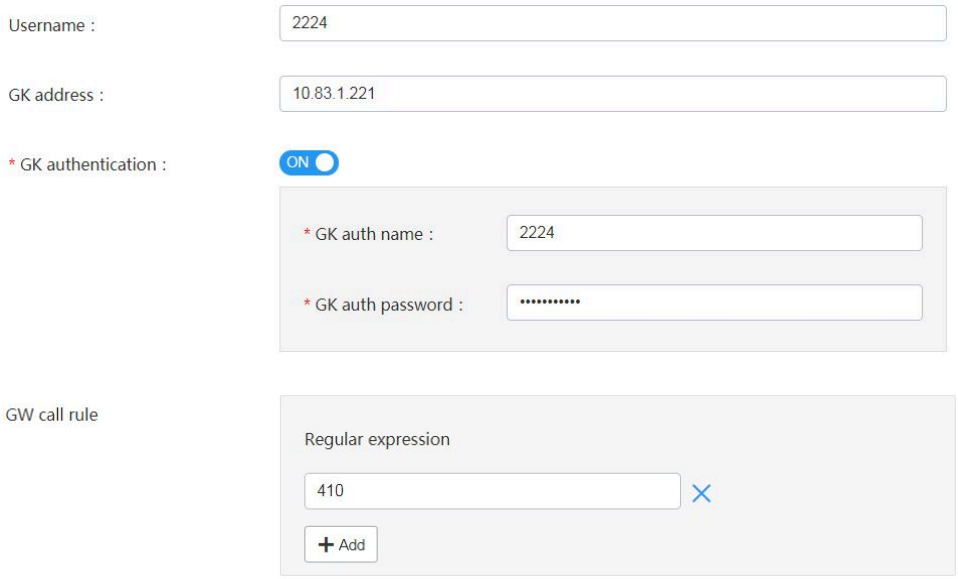


H.323 Gateway Example (Taking H.323 Gateway as an Endpoint)



- **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



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

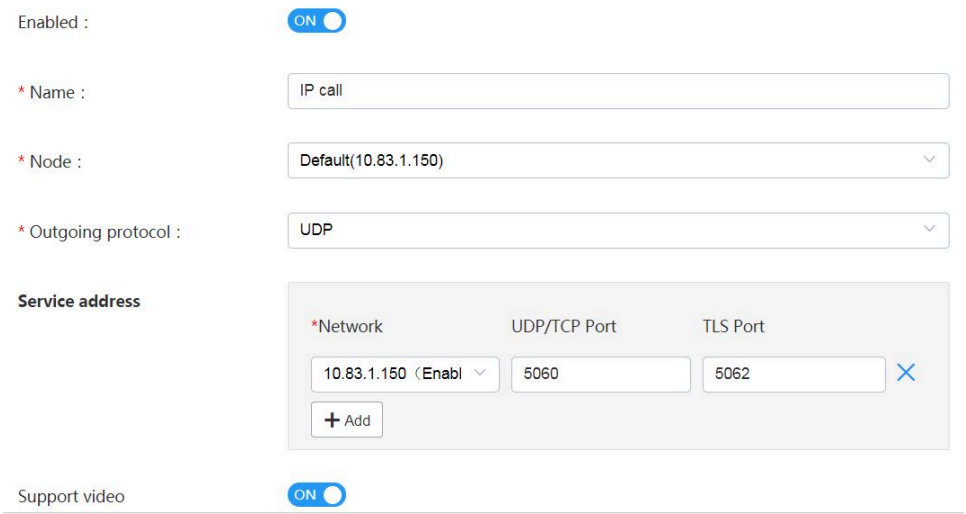
About this task

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.



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.

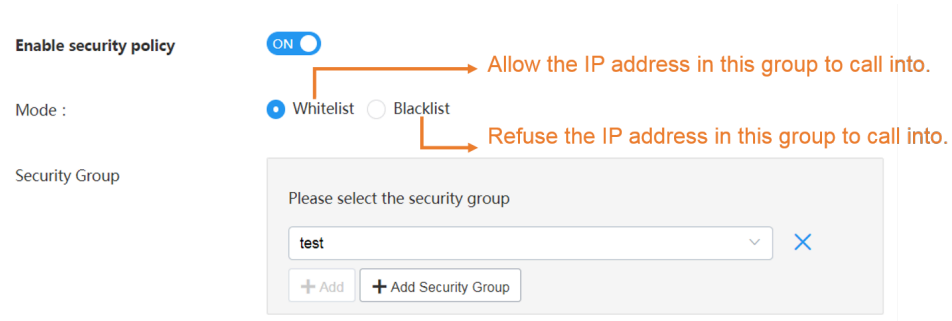
5. Enable **Media Bypass** to improve the server performance and to support a larger number of participants in the conference. Note that the third-party devices have lower compatibility.

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

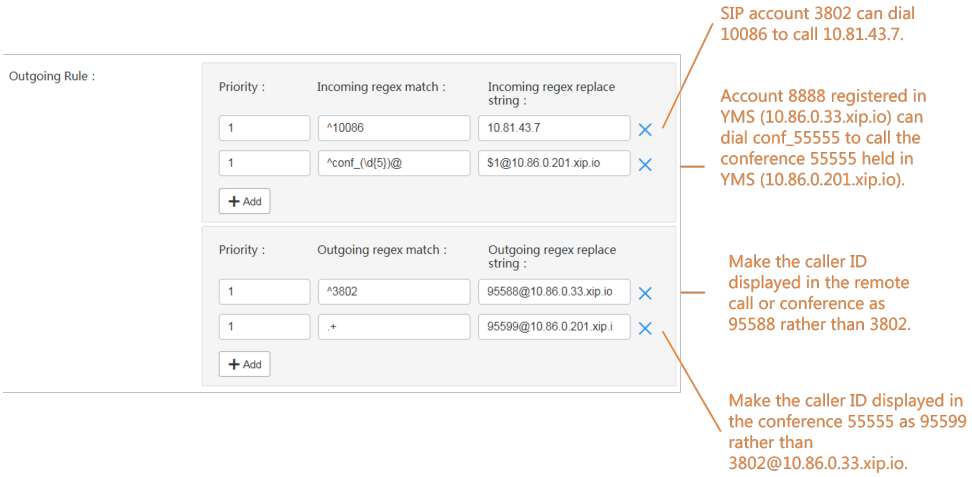
   If **Media Bypass** is enabled, Media bypass service should be enabled too. For more information, refer to Configuring the Media Bypass Service.

6. Optional: Configure the security policy.

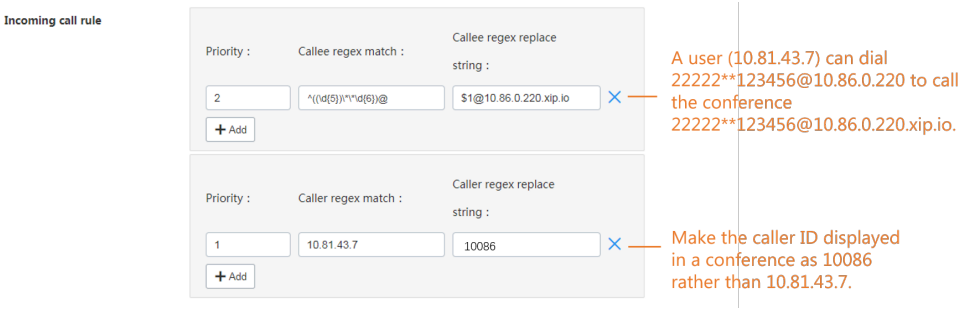
   For adding a security group, seeAdding a Security Group



7. Configure the outgoing call rule.



8. Configure the incoming call rule.

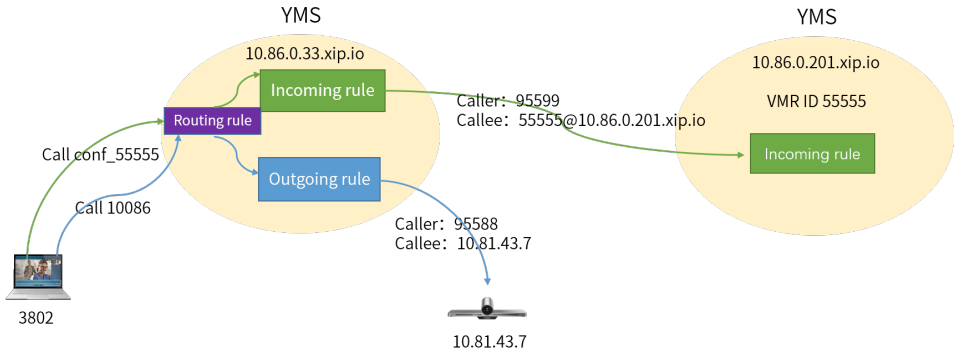


9. Save the configuration.

Related concepts

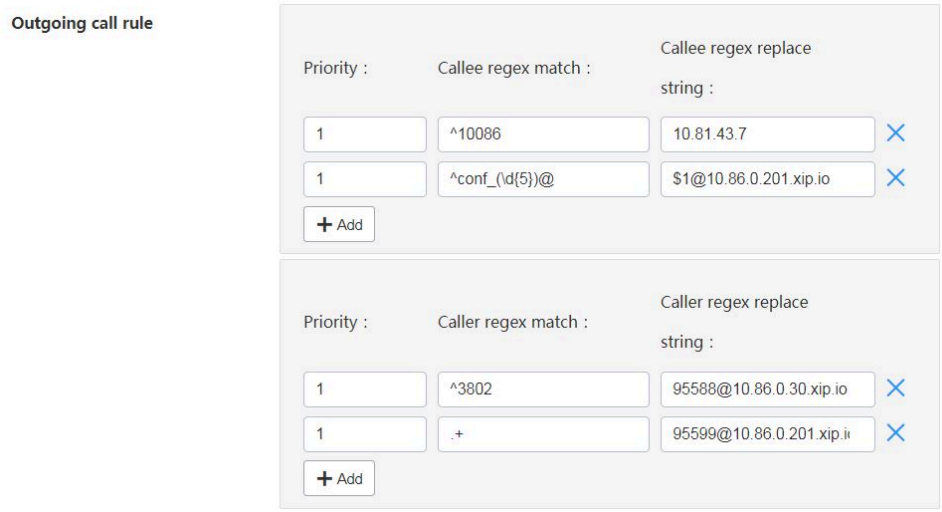
Common Regular Expressions and Replacement Strings

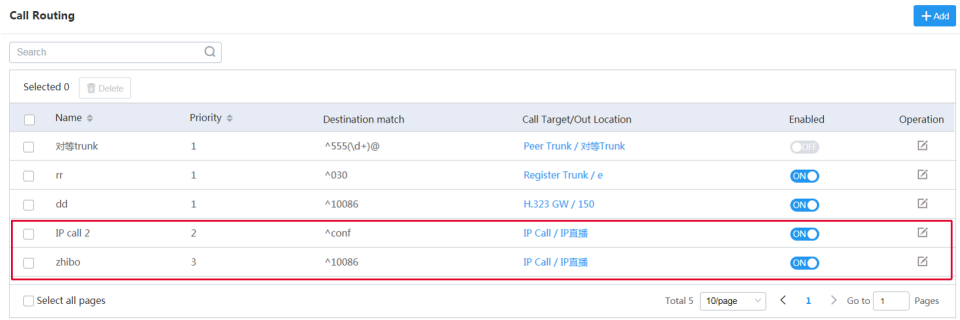
IP Call Example



- **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





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

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.

Characters	Description
|	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 single character specified in the brackets.
[^xyz]	Matches anything except the character specified in the brackets.
[a-z]	Matches any single character 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
^(13[0-9]|14[5|7]|15[0|1|2|3|5|6|7|8|9]|18[0|1|2|3|5|6|7|8|9])\d{8}$	Matches 11-digit mobile phone number, the first 3 digits includes the following types, and the last 8 digits can be any digits: • Start with 13 and the third number is any digit from 0 to 9 • Start with 14 and the third number is 5/7 • Start with 15 and the third number is 0/1/2/3/5/6/7/8/9 • Start with 18 and the third number is 0/1/2/3/5/6/7/8/9 For example, 13012345678, 14512345678, 15987654321 or 18243218765

PCRE	Description
^(\d{3,4}-)?\d{7,8}$	Matches the following number format: • **XXX-XXXXXXX, 10-digit** • **XXX-XXXXXXXX, 11-digit** • **XXXX-XXXXXXX, 11-digit** • **XXXX-XXXXXXXX, 12-digit** • **XXXXXXX, 7-digit** • **XXXXXXXX, 8-digit** For example, XXXX-XXXXXXX represents 07311234567 or other 7-digit number
\d{3}-\d{8}|\d{4}-\d{7}	Matches the following number format: • **XXX-XXXXXXXX, 11-digit** • **XXXX-XXXXXXX, 11-digit** For example, XXX-XXXXXXXX represents 012-12345678 or other 11-digit number, XXXX-XXXXXXX represents 0123-1234567 or other 11-digit number
(\d{11})|((\d{3,4})-)?(\d{7,8})(-(\d{1,4}))?	Matches the following number format: • **11-digit mobile phone number** • **XXXXXXXX, 8-digit number** • **XXXXXXX, 7-digit number** • **XXX/XXXX-XXXXXXX/XXXXXXXX, 4 formats in total** • **XXX/XXXX-XXXXXXX/XXXXXXXX-X/XX/XXX/XXXX, 16 formats in total** • **XXXXXXX/XXXXXXXX-X/XX/XXX/XXXX, 8 formats in total** For example, XXXX-XXXXXXX represents 0731-8784888 or other 11-digit number

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 avmcu\.(\d{1,10})@(xiamen.yealinksfb\.com), and the regex replace string is (\d{1,10}@(xiamen.yealinksfb\.com).

Adding a Call Routing Rule

Procedure

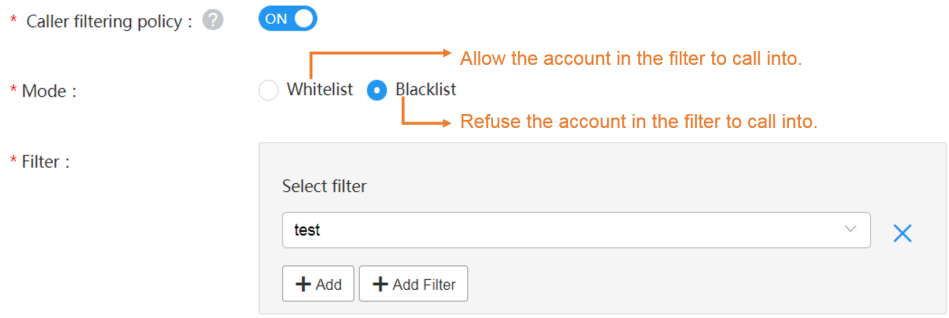
1. Click **Call Configuration** > **Call Routing**.
2. Add a call routing rule.

3. Set the parameters.

Table 27: Parameters of the Call Routing Rule

Parameter	Description
Enabled	Enable or disable the call routing rule. **Default**: enabled.
Name	Specify the name of the call routing rule.
Priority	Specify 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.
Destination regex match	Specify the desired regular expressions or the number field to match the target call number. **Note:** 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 filter, refer to Add a Number Filter



5. Configure the parameter of the outgoing location.

Table 28:

Parameter	Description
Call target	Specify the call target. • **Reject** • **IP Call** • **Federation service** • **Peer Trunk** • **PSTN** • **SfB** • **Register Trunk** • **H.323 GW** •

Parameter	Description
Outgoing location	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.
7. Optional: If you want to test whether there is a conflict between the number resource and the call routing, you can enter the number and click **Start Verification**. If there is a conflict, the page displays the matched call routing. Otherwise, the page prompts no matching route.

Related tasks

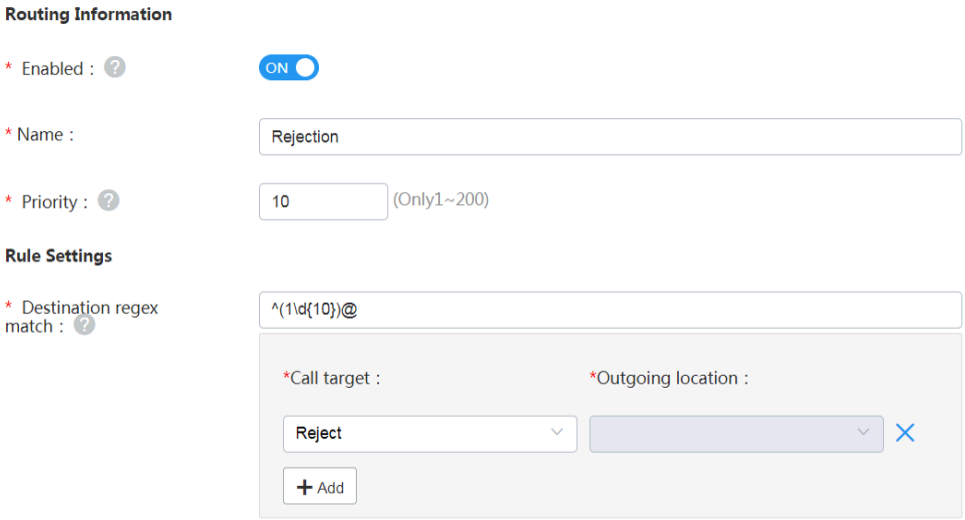
Add a Number Filter

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

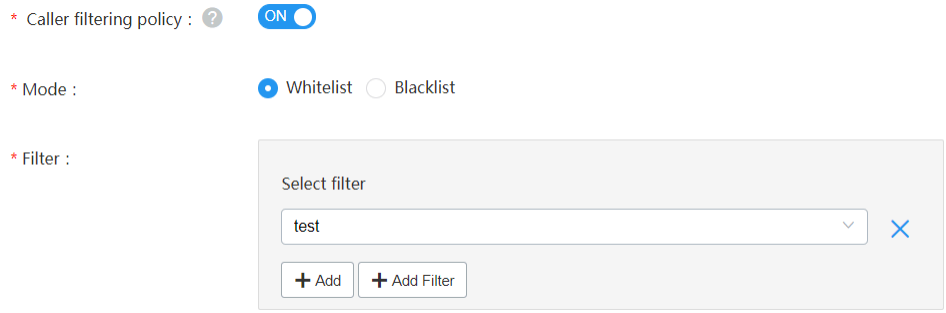
1. Click **Call Configuration** > **Call Routing**.
2. Add a call routing rule.
3. Set the parameters.



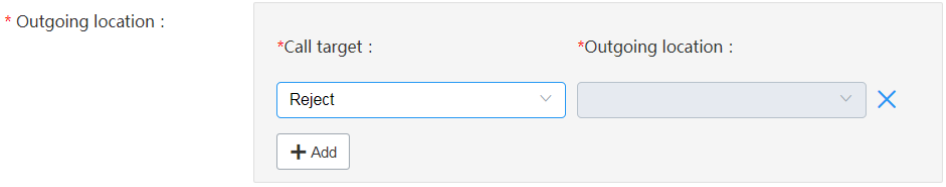
4. To restrict the number you call, enable **Caller filtering policy**, and set the parameters.

   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



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

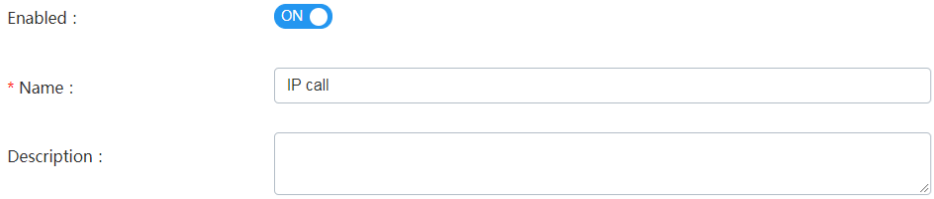


6. Save the configuration.

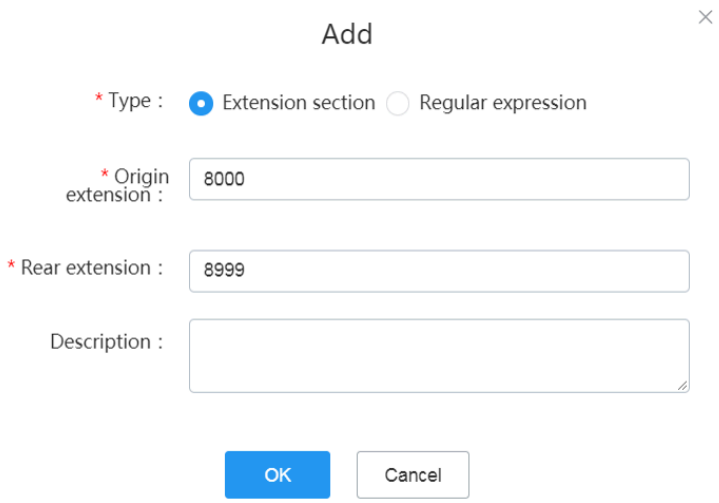
Add a Number Filter

Procedure

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



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



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.	

Type	Description	Note
Other account	The devices that you add by entering the IP address or URI via the SIP, H.323, RTSP, or RTMP. 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

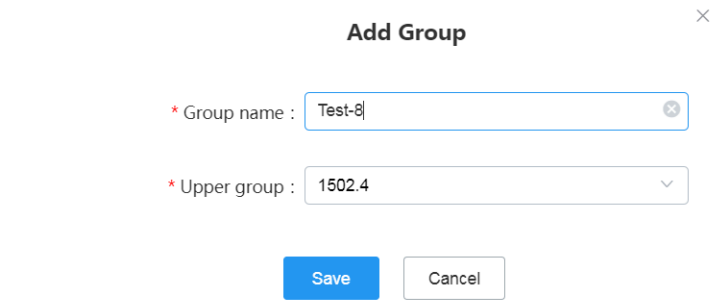
Managing Accounts by Group (Optional)

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.

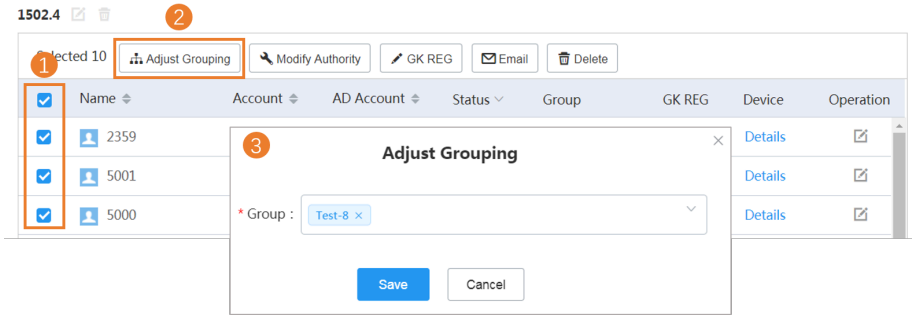
- **Adding a Group**

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



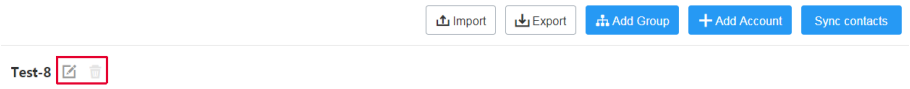
- **Adjusting the Group**

  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
Common parameters	
AD Account	If you select **Obtain from AD server**, 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.
Authority	The authorities owned by this account. The available authorities are as below: • **A**: this account can see all user accounts, room system accounts, VMRs (synced to the directory) and other accounts. • **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. If the user is in the root node, the range that he can see is the same as A. • **C**: this user account/room system account can see only the user accounts/ room system accounts in his group. • **D**: this account can only see himself. • **Custom**: you can customize the visible range for this account.
Enable schedule	Allow or refuse this account to schedule meeting rooms and conferences. **Default:** enabled.
Enable Meet Now	Allow or refuse this account to create Meet Now conferences. **Default:** enabled.
Enable call authority	If you enable this feature, this account can only call the contacts, which are visible to him. **Default:** disabled.
Enable live caption privilege	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. **Default:** disabled. The voice transfer server should support this feature. For more information about it, contact Yealink technical support engineers.

Parameter	Description
The parameters only owned by the user accounts	
Enable Schedule Virtual Meeting Room	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. **Note**: only when you contact Yealink technical support engineers to enable this feature can you see this configuration.

Related concepts
User Account, Room System Account and Other Accounts
Related tasks
Add a User Account
Importing a Batch of Accounts
Configuring the LDAP
Allocating the Number Resource
Related information
#unique_173

Add a User Account

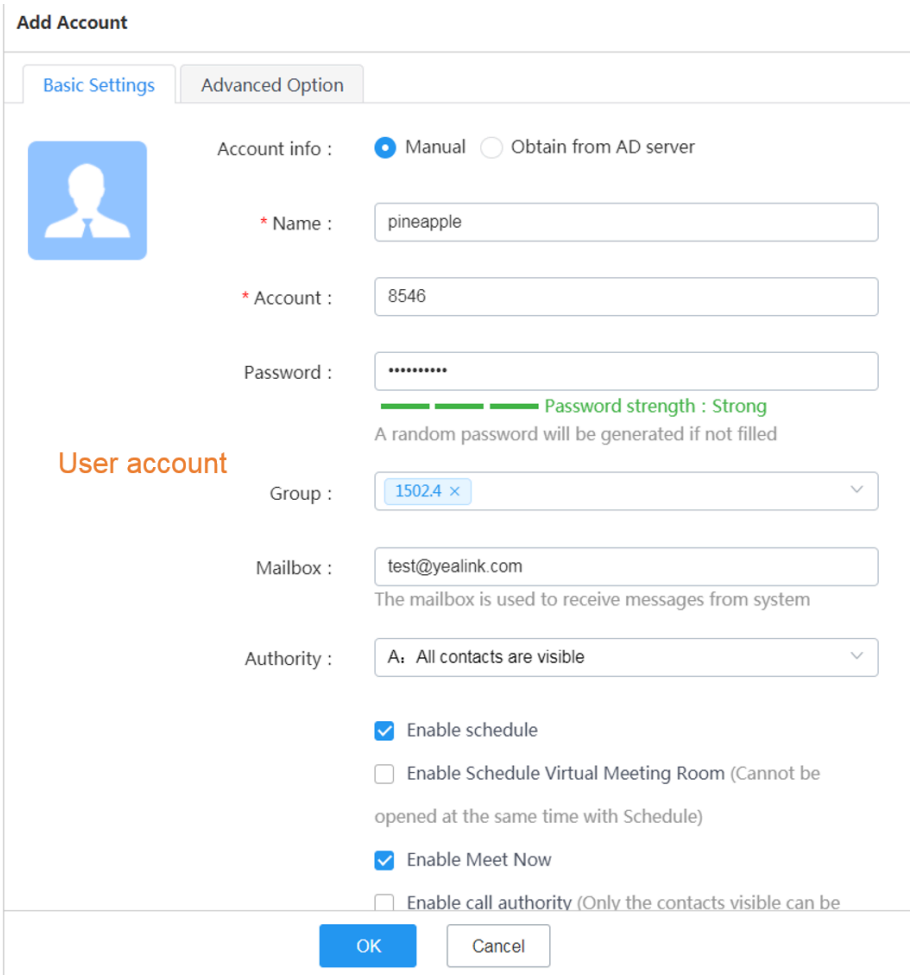
About this task

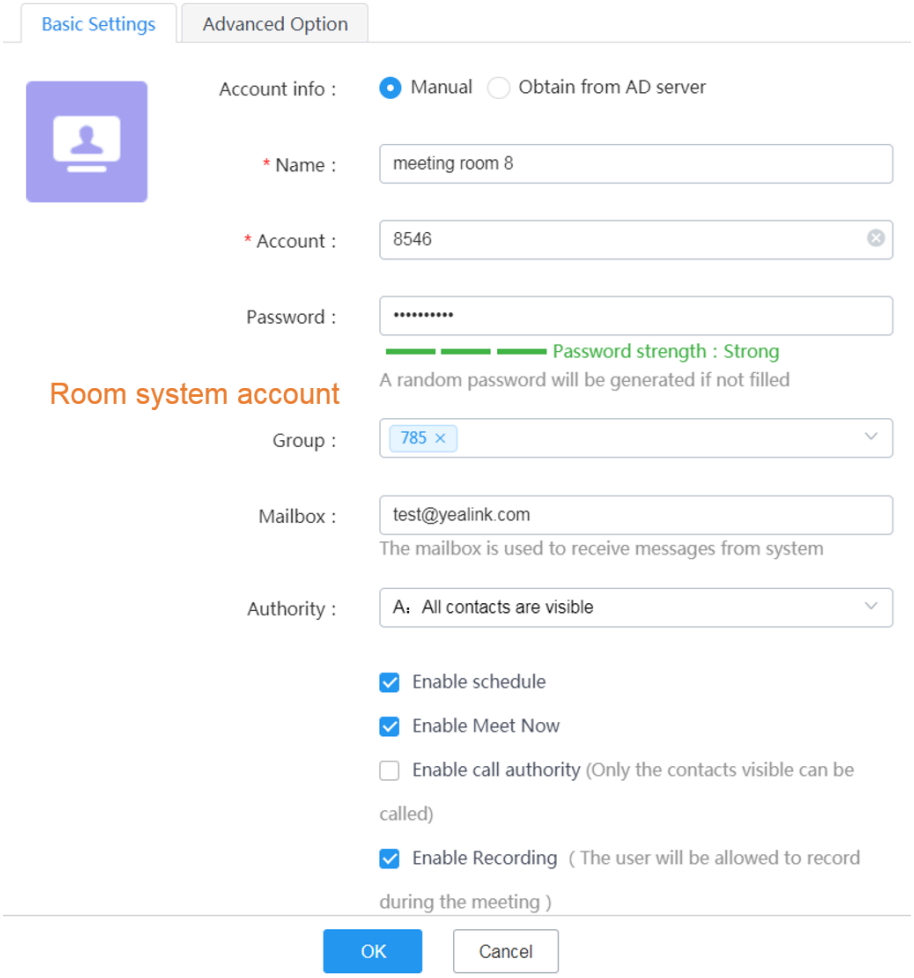
Note: For adding an AD Account, refer to LDAP.

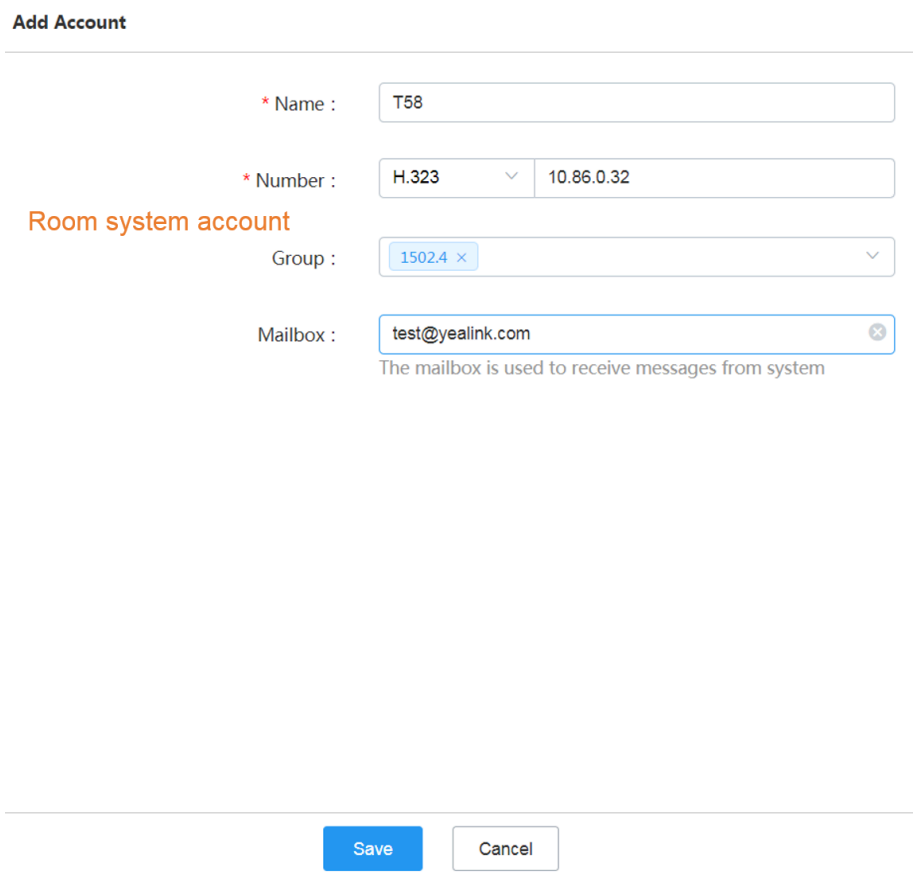
Procedure

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

2. Add an account.




Basic Settings
Advanced Option
Account info :
Manual
Obtain from AD server
* Name :
meeting room 8
* Account :
8546
Password :
Password strength : Strong
A random password will be generated if not filled
Room system account
Group :
785 ×
Mailbox :
test@yealink.com
The mailbox is used to receive messages from system
Authority :
A: All contacts are visible
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)
OK
Cancel



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

Allocating the Number Resource

Related information

#unique_173

Importing a Batch of Accounts

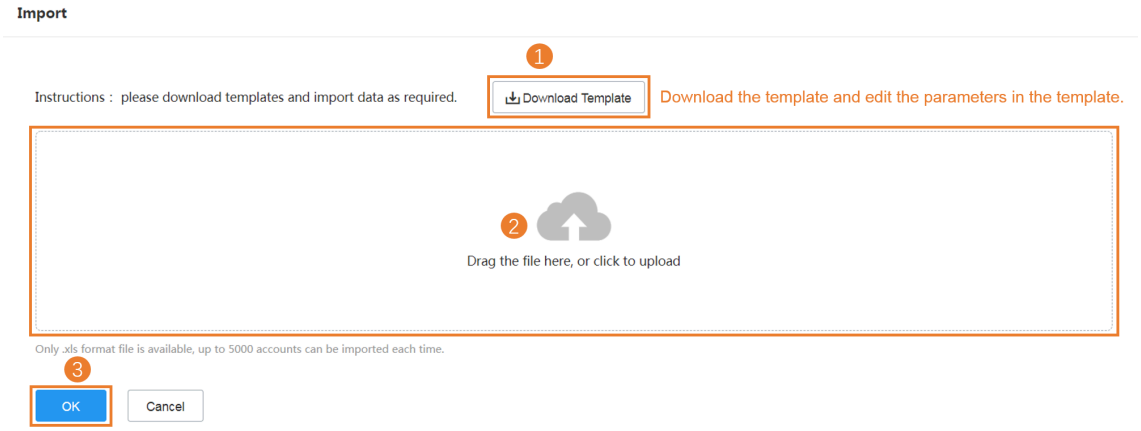
You can import a template to add a batch of accounts. Before that, you need to download the template first.

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
- Setting the Auto Synchronization
- Enabling Logging into YMS via AD Account with Priority
- Synchronizing LDAP Accounts

Configuring the LDAP

Procedure

1. Click **Account** > **LDAP**.
2. Add a LDAP server.

   You can add up to two LDAP servers. If two LDAP servers have the same account, YMS only synchronizes the accounts of the first added LDAP server.

3. Set the parameter and save it.

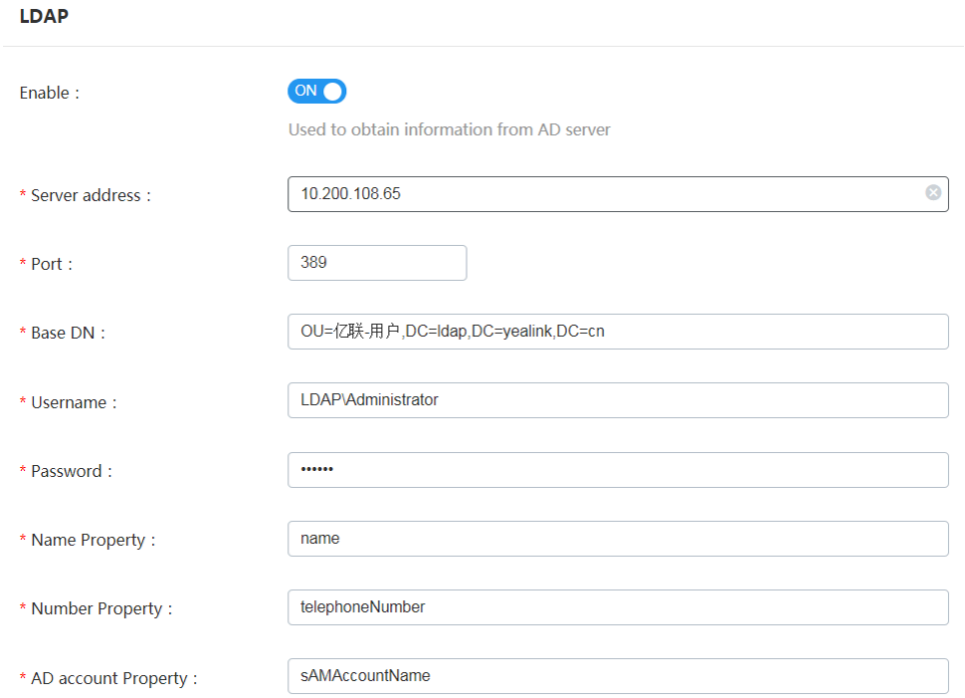
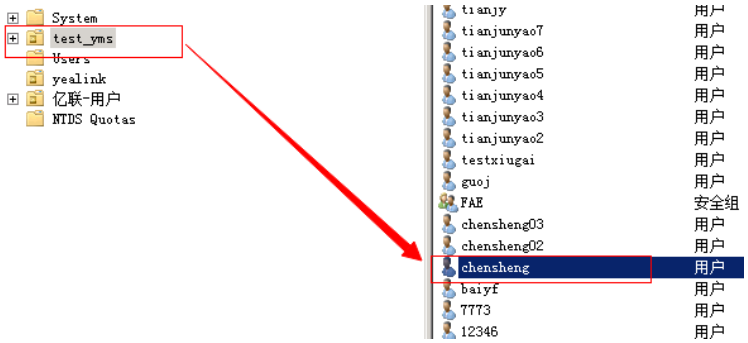


Table 30: LDAP parameters

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

Parameter	Description
Base DN	Set the root path for YMS to obtain the LDAP accounts. **For example**, OU=test_yms,DC=ldap,DC=yealink,DC=cn **Obtaining method**: the directory of AD server is shown as below. If YMS wants to obtain the user information under this contents, right click test_yms->Attribute->Attribute Editor, view the attribute value *OU=test_yms,DC=ldap,DC=yealink,DC=cn*, and fill this value in the **Base ND** field on YMS. 
Username	Specify the username used to log into the LDAP server. **Note**: The username is provided by the AD server administrator. For example, the “chensheng” account in the test_yms contents. The user in the *test_yms* directory is acceptable. The username is *chensheng@ldap.yealink.cn*. 

Parameter	Description
Password	Specify the password used to log into the LDAP server. **Note**: The password is provided by the LDAP server administrator. For example, the AD username is *chensheng@ldap.yealink.cn* Enter the password of this username.
Name Property	Set the name property of the returned LDAP account. **For example**, 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.
Number Property	Set the number property of the returned LDAP account. **For example**, 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 Allocating the Number Resource) 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.
AD account Property	Set the account property of the returned LDAP account. **For example**, sAMAccountName
Mailbox Property	Set the property name of the mailbox in the LDAP server. **For example**, mail or email.

4. Click **Connection Test**.
   If the configuration is correct, the prompt “Connection successful” will pop up.
5. 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

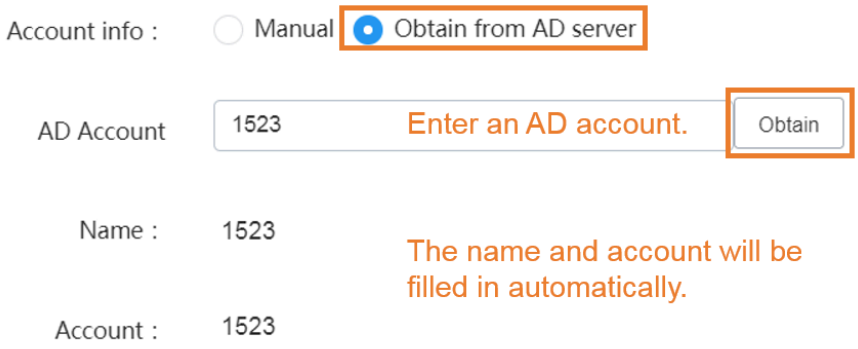
Before you begin
Configuring the LDAP

Procedure

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

2. Add the account and save the configuration.

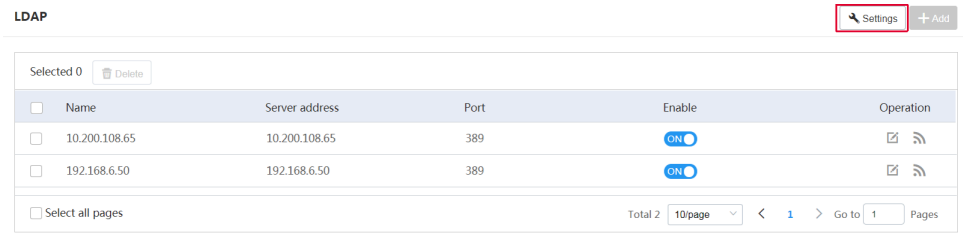
   The account number should be within the number field (see Allocating the Number Resource). Otherwise, the page prompts that the account is invalid.



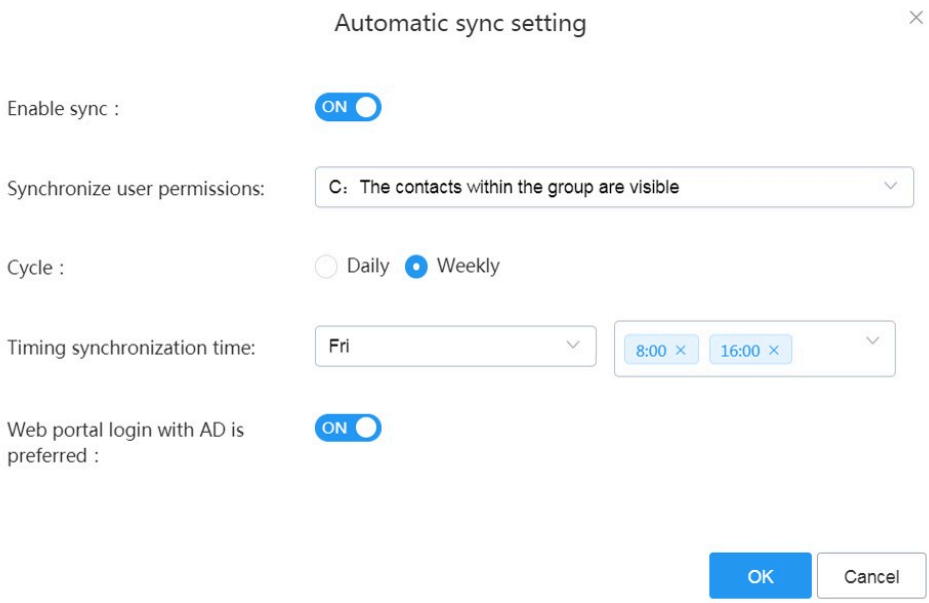
Setting the Auto Synchronization

Procedure

1. Click **Account** > **LDAP**.
2. Click **Settings**.



3. Set the parameter and save it.

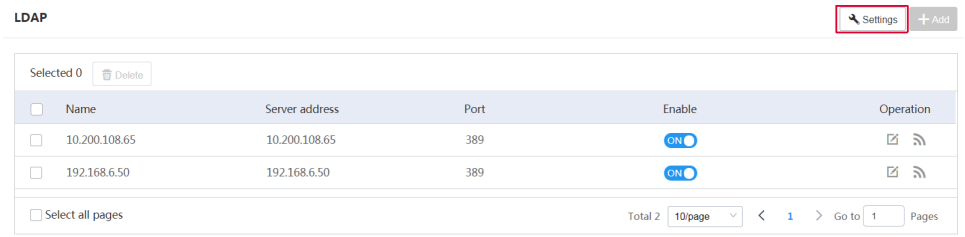


Enabling Logging into YMS via AD Account with Priority

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.

Procedure

1. Click **Account** > **LDAP**.
2. Click **Settings**.



3. Enable **Web portal login with AD is preferred** and save it.

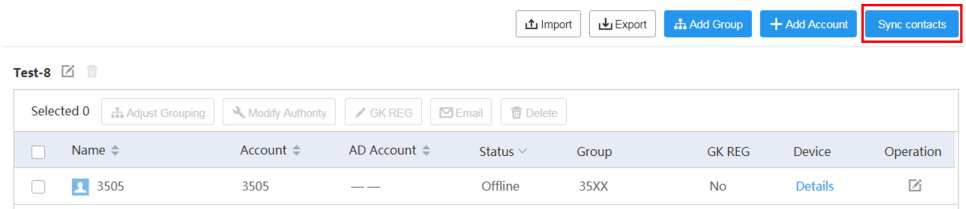
Synchronizing LDAP Accounts

Before you begin

- Configuring the LDAP
- To enable the feature of synchronization, refer to Setting the Auto Synchronization

Procedure

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



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: If the account is outside the number field of the system account, you can also succeed in synchronizing, but you cannot use the account to log in to YMS. You need to add the corresponding number field to use the account for login (refer to Allocating the Number Resource).

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

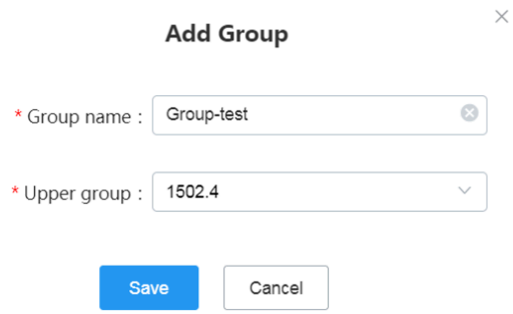
Adding a VMR

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.

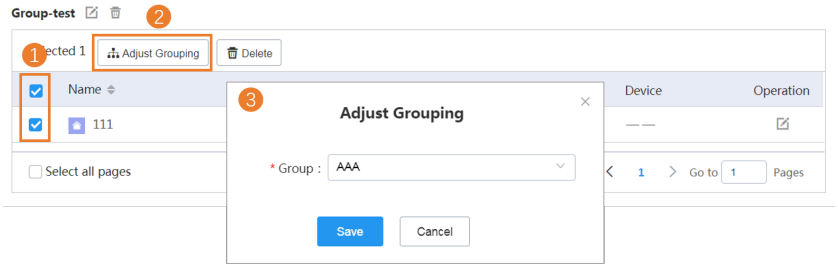
- **Adding a Group**

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



- **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

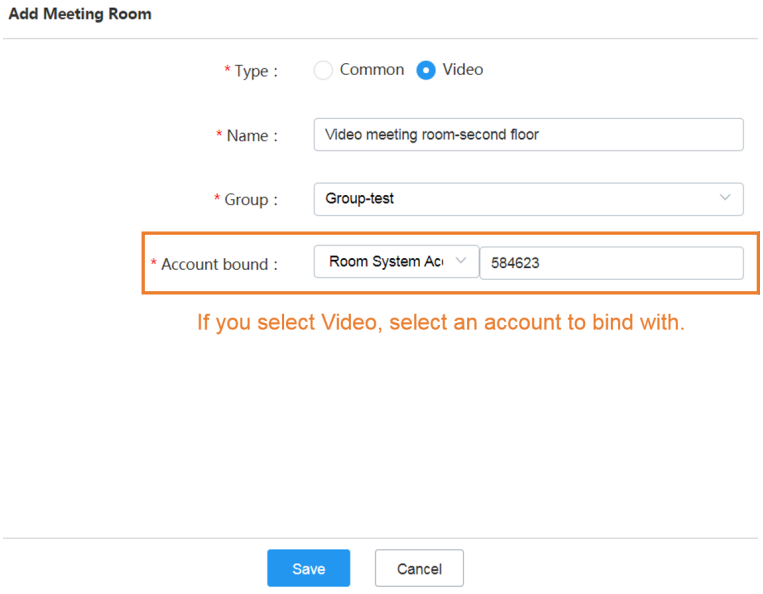
You can add entity meeting rooms for users to schedule conferences.

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.



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.

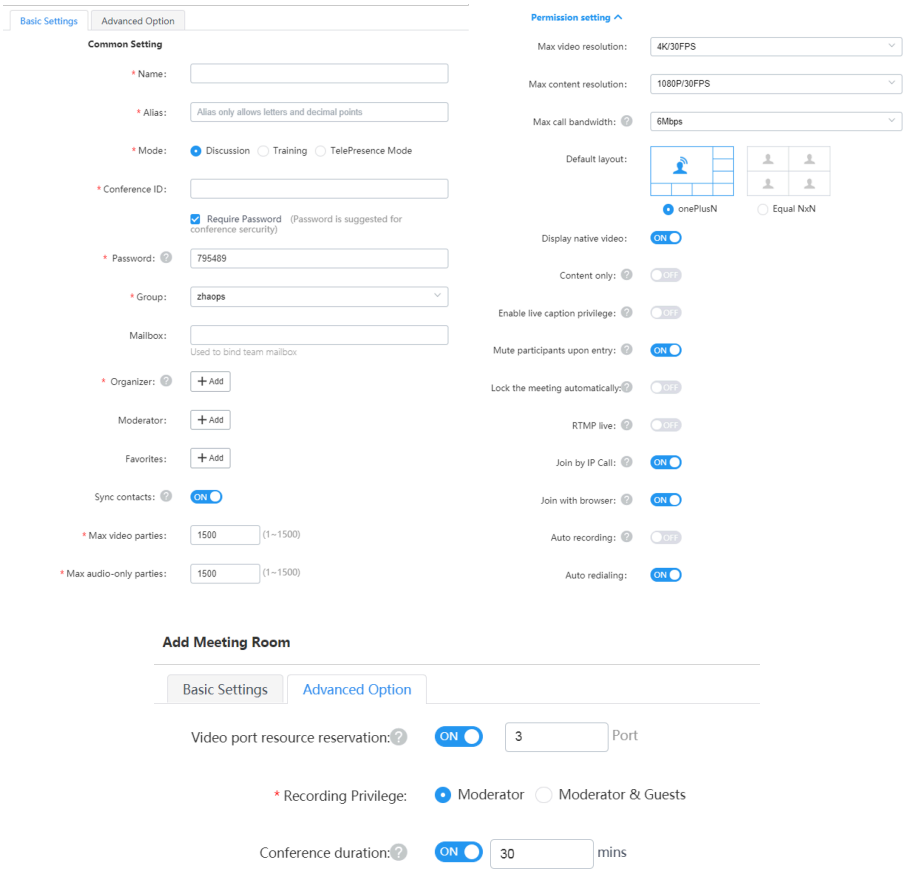


Table 32: Introduction of the corresponding parameters

Parameter	Description
Alias	The call rules based on the alias will be generated after you create the VMR. **Prerequisite**: Setting the IP Call and H.323 Gateway 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.

Parameter	Description
Enable live caption privilege	If you enable this feature, the live caption is available on this VMR. You need to contact Yealink technical support engineers to enable this feature. **Note**: it is disabled by default. The voice transfer server should support this feature. For more information about it, contact Yealink technical support engineers.
Join by IP Call	If it is enabled, the user can join the conference by IP call.
Join with browser	If it is enabled, the user can join the conference by Yealink Web app.
Lock the meeting automatically	If it is enabled, the conference is locked by default. The moderators and the invited people can join the conference directly, and other people will go to the conference lobby when they call into the conference.
Video port resource reservation	To ensure that important conferences can proceed successfully without being occupied by other conferences, you can enable this configuration to reserve video ports. **Note:** The default value is 3. The maximum number of the video port resource reservation cannot exceed the total number of the video ports and the broadcasting ports that are available in the license.
Conference duration	Enable this feature and set the time. If you enable it, when the set time is up, the conference ends automatically. During the conference, the countdown appears on the device screen and disappears after a specific time. Besides, a reminder pops up when the countdown begins and 3 minutes before the countdown ends. **Note:** The countdown starts when the first participant joins the conference.
Open voting	If you enable this parameter, you can set the voting information in advanced. **Note:** The participants can vote online by sending the DTMF tones using their devices.
Set voting content in advance	If you do not set the voting information in advance, you can set it on the Conference Control page.

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

<table>
<tr><th>Difference</th><th colspan="2">Discussion Mode</th><th colspan="2">Training Mode</th></tr>
<tr><td rowspan="3">Participant Role</td><td>Moderator</td><td>You can set any participants in the enterprise directory as moderators.</td><td>Moderator</td><td>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.</td></tr>
<tr><td rowspan="2">Guest</td><td rowspan="2">It refers to the participants who join the VMR but are not set as moderators.</td><td>Lecturer</td><td>Moderators can set any moderators or guests as lecturers during the conference.</td></tr>
<tr><td>Guest</td><td>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.</td></tr>
<tr><td rowspan="3">Feature Privilege</td><td colspan="2">Moderators can configure the layout during the discussion mode conferences or Meet Now conferences.</td><td colspan="2">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.</td></tr>
<tr><td colspan="4">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.</td></tr>
<tr><td colspan="4">Other participants can only view the conference details.</td></tr>
</table>

Difference	Discussion Mode	Training Mode
Layout	Moderators and guests can view all participants. You can set the default layout, refer to Setting the Default Layout.	• The moderators can view all participants by default. You can set the default layout, refer to Setting the Default Layout. If the broadcasting interactive feature is enabled, the moderators can view all interactive parties by default. • 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. 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.
Speaking Rule	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.
Contents	All moderators and guests can share content by default.	Only moderators and lecturers can share content. Guests cannot share content.

Related tasks

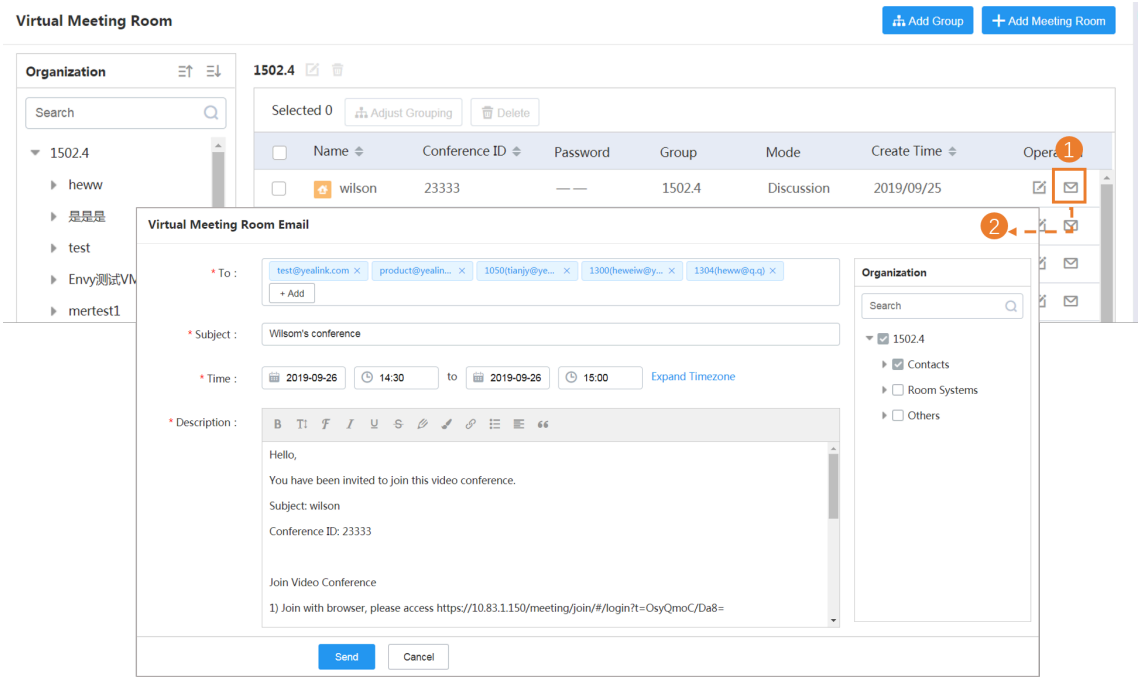
Adding a VMR

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
- Ending the Video Conference Beforehand

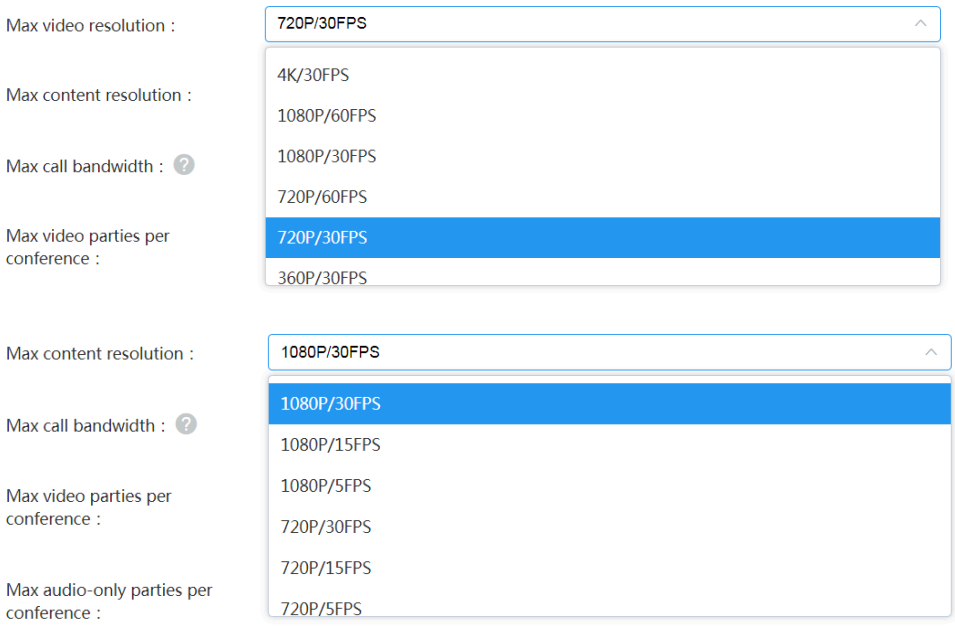
- Setting the Last Participant Backstop Timeout
- Setting the Auto End Conference Without Moderator
- Enabling Content Only
- Setting the Join with APP Awakened by Browser
- Enabling Receiving Ringtone Receipt
- Enabling External/Internal Network Access WebRTC Authentication
- Enabling the Roll Call
- Setting the App Push Address
- Setting the QoS
- Enabling Password for Meet Now Conferences
- Setting the Default Layout
- Displaying the Participant Name
- Displaying Participant Status
- Displaying the Participant Quantity
- Displaying the Audio-Only Participant
- Displaying the Speaker Reminder
- Setting the Codec

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.



- **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**.

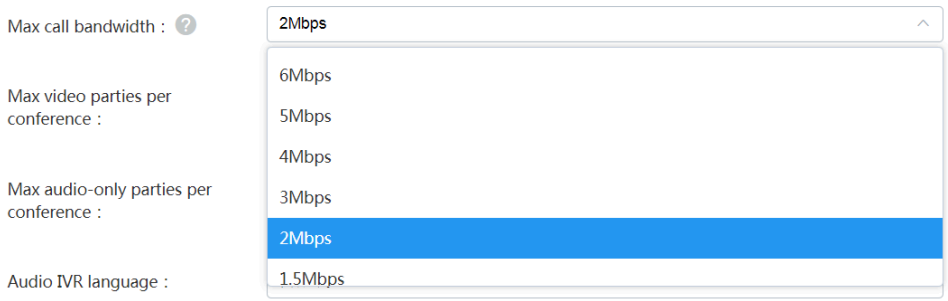
       In the **Permission setting** field, set the maximum content and video resolution, and save it.
     - If you want to edit a VMR, click  .

       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.



- **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 auto dialing feature. When the scheduled conference begins, YMS will automatically place invitation calls to the invited participants.

About this task

If you disable this feature, it is invisible to users when they schedule conferences.

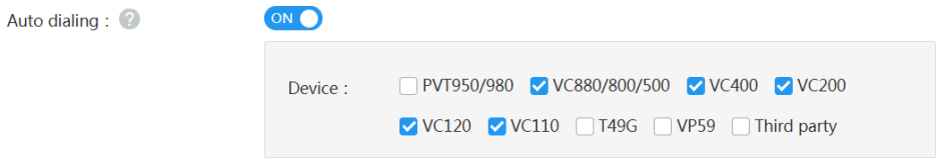
Procedure

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-party participants, select the check box of **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:

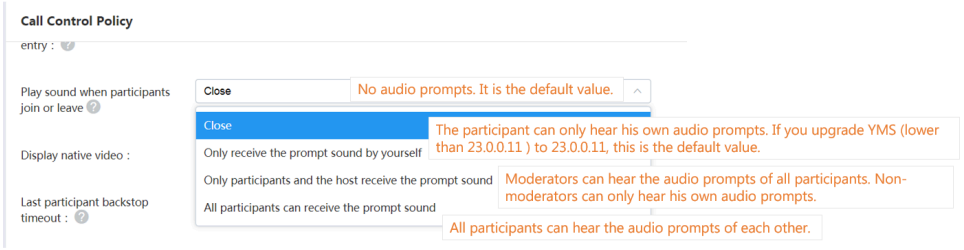
- When users schedule conferences or create Meet Now conferences, if you set the audio prompt in the Global Setting as **Close**, this configuration is invisible on the Conference Control page.
- During the conference, if you change the audio prompt in the Global Setting, it affects the newly scheduled 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.



- **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.

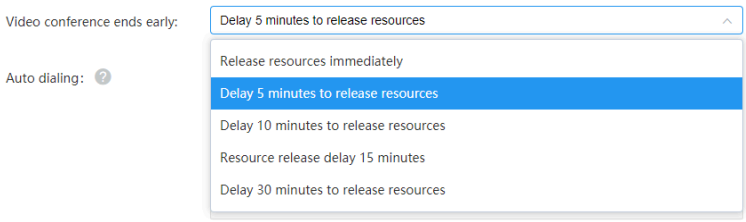
Ending the Video Conference Beforehand

After you set this feature, the server will end the conference to release the port license according the time you set, for better resource usage.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.

2. Set the parameter and save it.



- **Release resources immediately**: after the conference is ended, the port license will be released immediately and the conference ID becomes invalid.
- **Delay N minutes to release resources**:
  - For upcoming conferences, if you or moderators end them, the port licenses will be released immediately and the conference IDs become invalid.
  - For ongoing video conferences but not reaching the conference end time, if you or moderators end them, the server will decide whether to release port licenses after N minutes and the conference IDs are still available within N minutes.

    Within N minutes, if no participant joins the video conference, the port licenses will be released immediately after N minutes and the conference IDs become invalid.

    However, if one or more participants join the video conference, the server will decide whether to release the port license after another N minutes when all participants leave the conference.
  - Within another N minutes, if the conference reaches the conference end time and no participant joins the conference, the port licenses will be released immediately and the conference IDs become invalid. If the conference reaches the conference end time and still has participants, the server will re-decide.

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.

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.

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 .

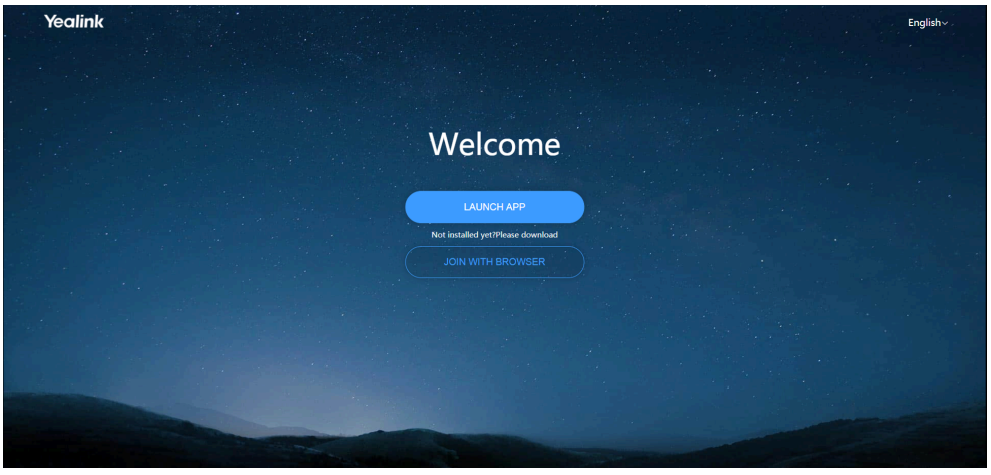
       In the **Permission setting** field, enable **Enabling Content Only, account and save.**, and save it.

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

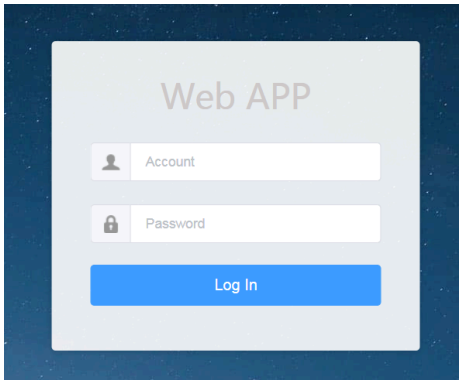
1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Receiving ringtone receipt** and save it.

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 flaw 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.

Enabling Password for Meet Now Conferences

If you enable **Password**, the Meet Now conference created by users will generate a password randomly and automatically. If you disable **Password**, the Meet Now conference will not generate any password.

Procedure

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

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.

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**.

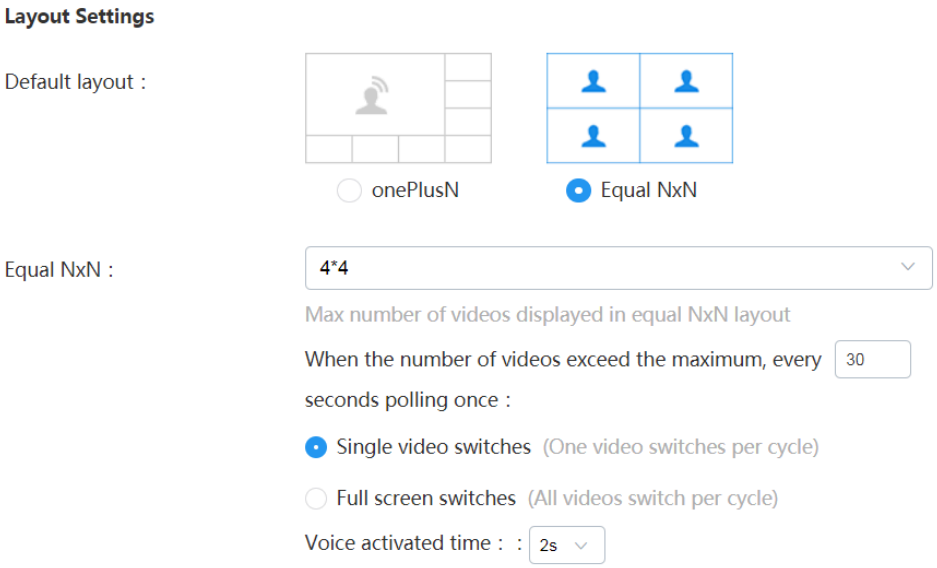


Table 34: Introduction of the corresponding parameters

Parameter	Description
1+N	In the video layout of 1+N, if current participants exceed the maximum number of the video images per screen, the video carousel is enabled by default and the system will switch among the video images of participants automatically.

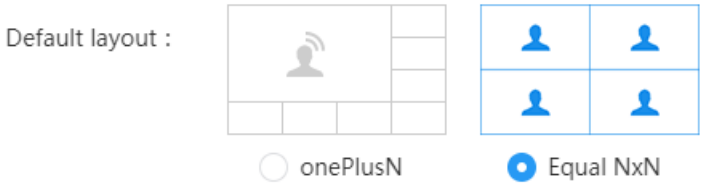
Parameter	Description
Equal N×N	In the video layout of Equal N×N, if current participants exceed the maximum number of the video images per screen, the video carousel is enabled automatically and the system will switch among the video images of participants automatically.
Voice activated speaker	The 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

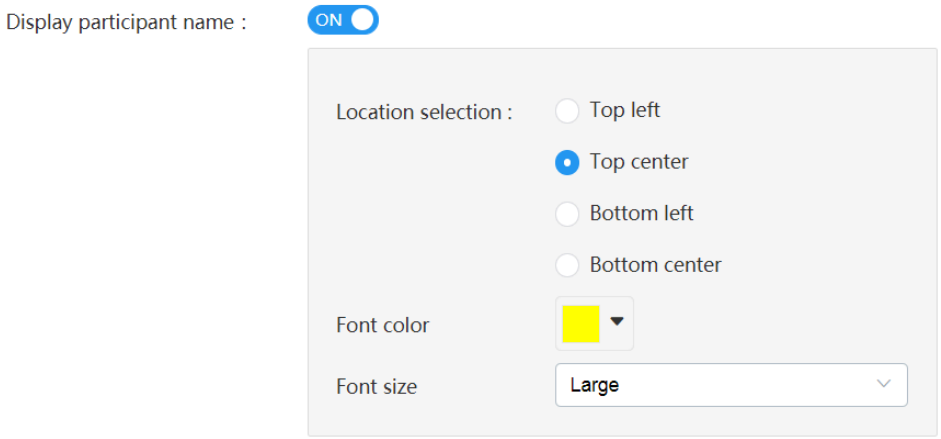
- When users schedule conferences or create Meet Now conferences, if you disable this feature, this configuration is invisible to the Conference Control page, and the participant name will not be displayed in the MCU video image.
- During the conference, if you enable this feature, the configuration will be displayed on the Conference Control page.
- During the conference, if you disable this feature, this configuration is invisible to the Conference Control page, and the participant name will not be displayed in the MCU video image.
- During the conference, if you edit the display position of the participant name, it affects the newly-created scheduled conference, Meet Now conferences and 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.



Displaying 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

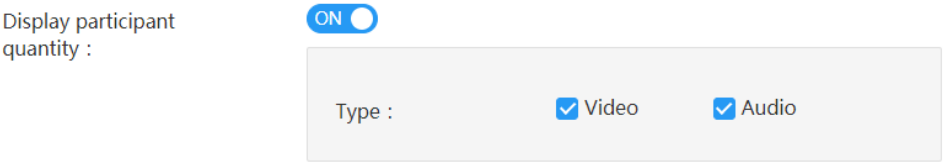
1. Click **Call Configuration** > **Video Display Policy**.
2. Enable **Display participant name** and save it.

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.



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

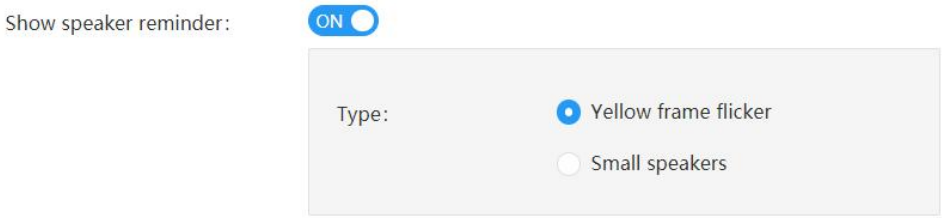
1. Click **Call Configuration** > **Video Display Policy**.
2. Enable **Display the audio-only participants** and save it.

Displaying the Speaker Reminder

In Equal N×N mode, you can enable the speaker reminder so a loudspeaker icon or a flickering yellow frame will be displayed on the video image of the speaking participant. Also, you can disable the reminder.

Procedure

1. Click **Call Configuration** > **Video Display Policy**.
2. Set the reminder type.



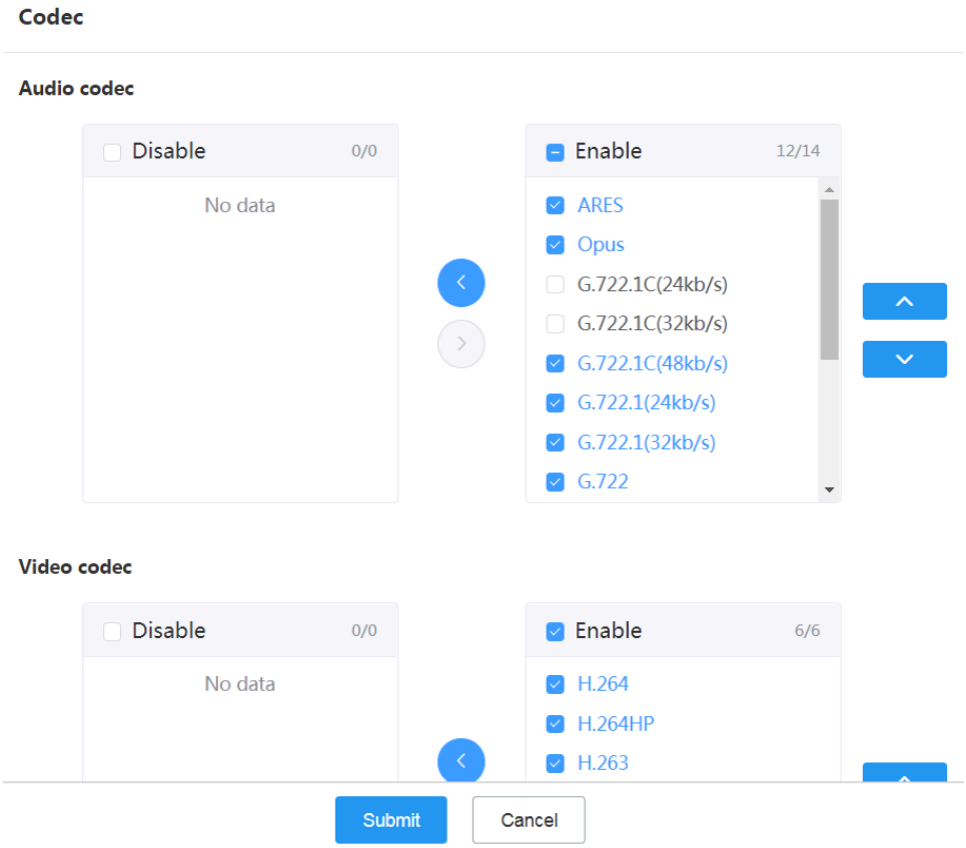
Setting the Codec

Some third-party systems might experience issues if they are sent a large SDP from YMS. You can reduce the size of the SDP by disabling specific, unwanted codecs. If devices join the conference actively, YMS uses the highest priority codec carried by the device (it depends on the device mechanism). However, if the devices are invited to the conference, YMS uses its highest priority codec.

Procedure

1. Click **Call Configuration** > **Codec**.

2. Enable or disable the codec and save the change.



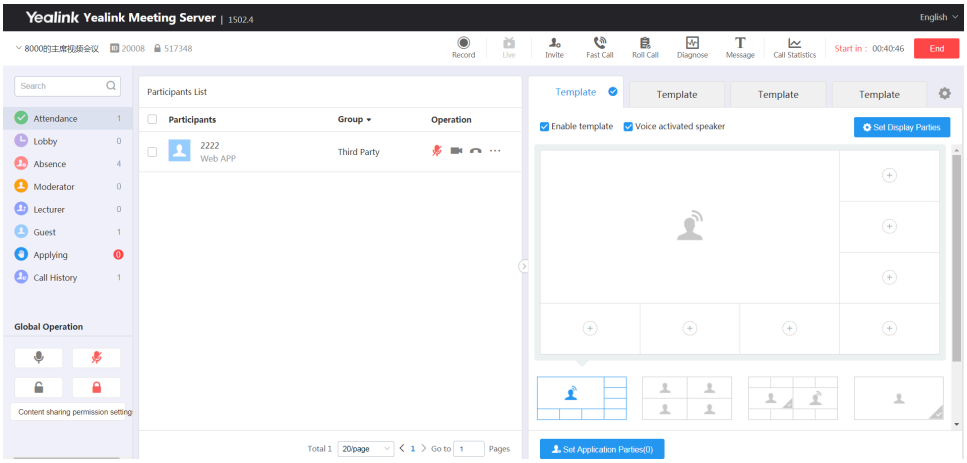
Controlling Conferences

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

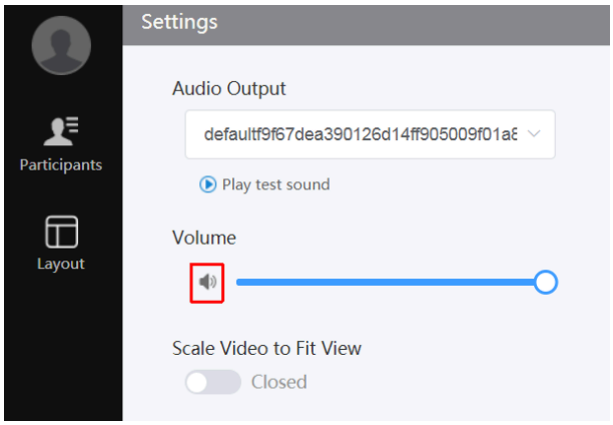
Before you begin

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

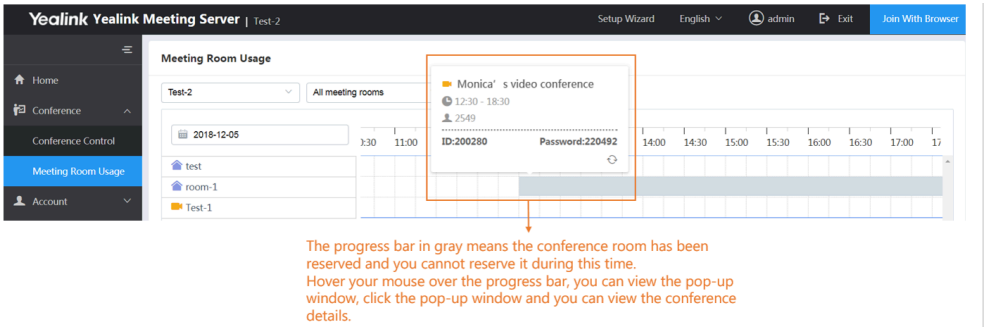
1. Click **Conference** > **Conference Control** > **Ongoing/Scheduled**.
2. On the right side of the desired conference, click .
3. If you want to delete the recurrence conference, click **Cancel occurrence/Cancel series**.
4. If you want to delete a single conference, click **OK**.

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**.



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

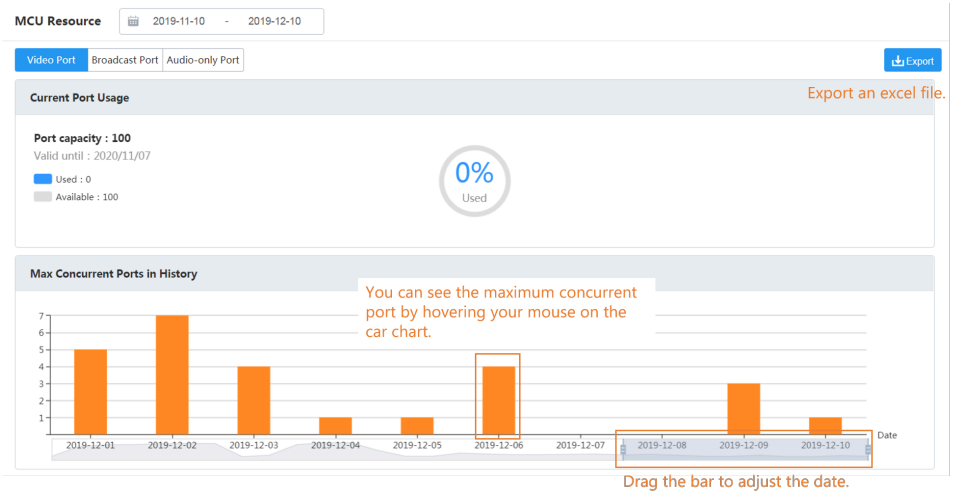
- Viewing the Conference Statistics
- Viewing the Call History

Viewing the MCU Resource

You can view the maximum number of the concurrent ports and the usage of the video, the broadcast, and the audio-only ports.

Procedure

Click **Statistics** > **MCU Resource**.

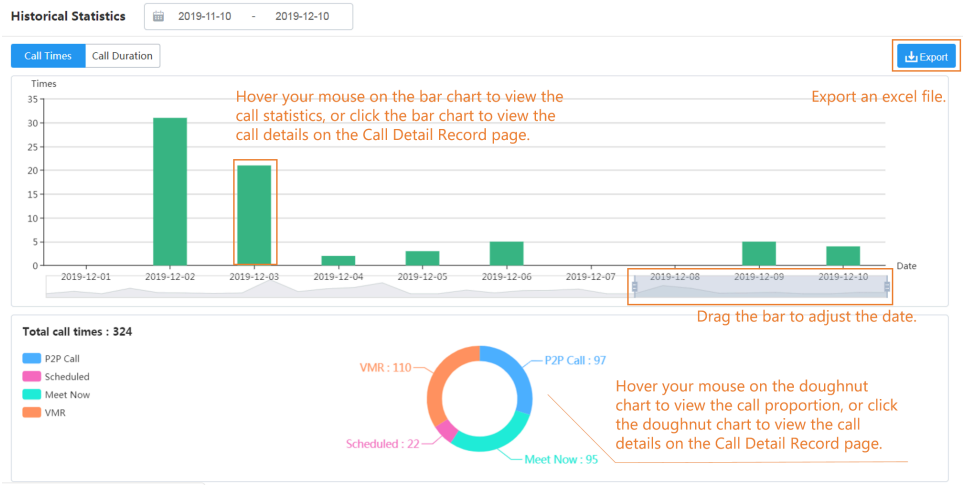


Viewing the Conference Statistics

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, viewing the list of the executed list 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
- Viewing the Statistics of the Executed Tasks

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	
YMS Version	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.
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
	VC210/VC210 Pro/VC200-E: 118.50.0.10 or later
	PVT920
	MeetingEye 800
	MeetingEye 400/MeetingEye 600: 120.43.0.5 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.

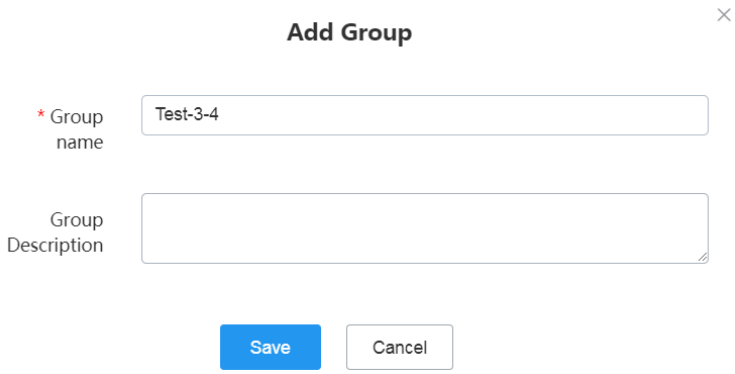
Managing Devices by Groups (Optional)

If you are used to managing the devices by groups, you can create groups.

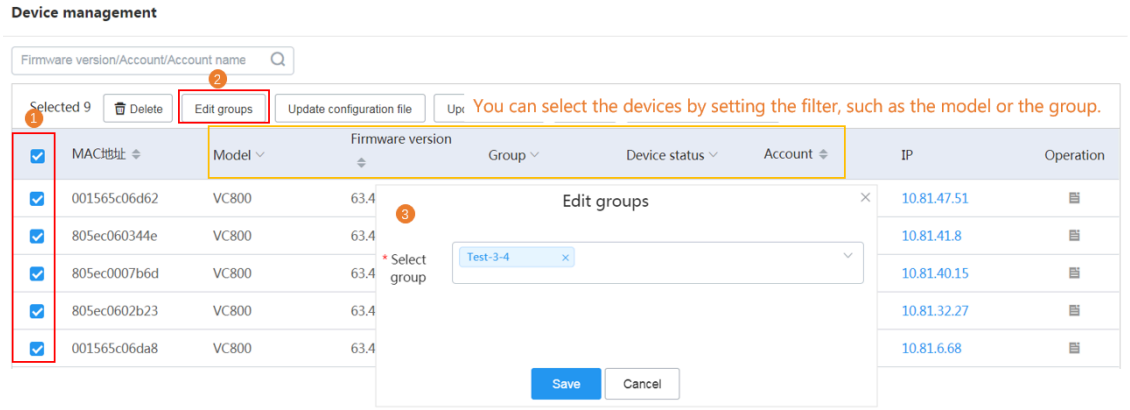
Procedure

1. Click **Device management** > **Group management**.

2. Add a group.



3. Go to the **Device management** page.



Pushing the Configuration

About this task

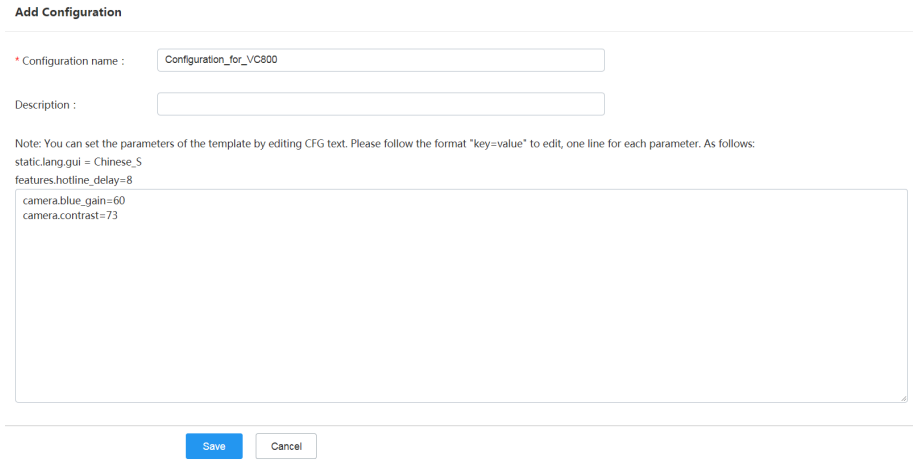
Before pushing the configuration, you need to know the device status first (Device Status):

- 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

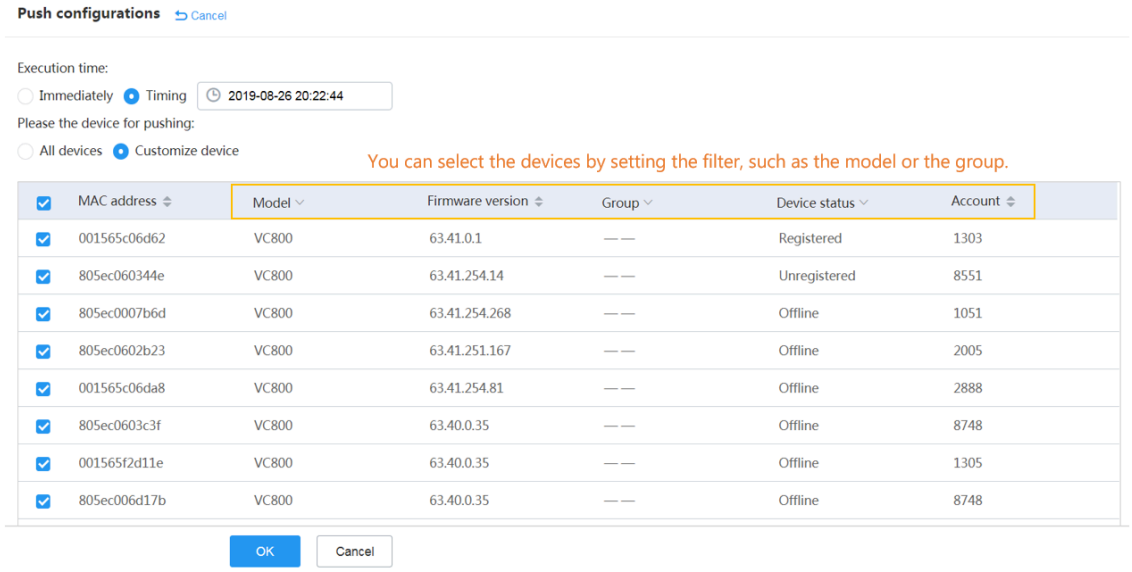
1. Click **Device management** > **Configuration management**.

2. Add the configuration.

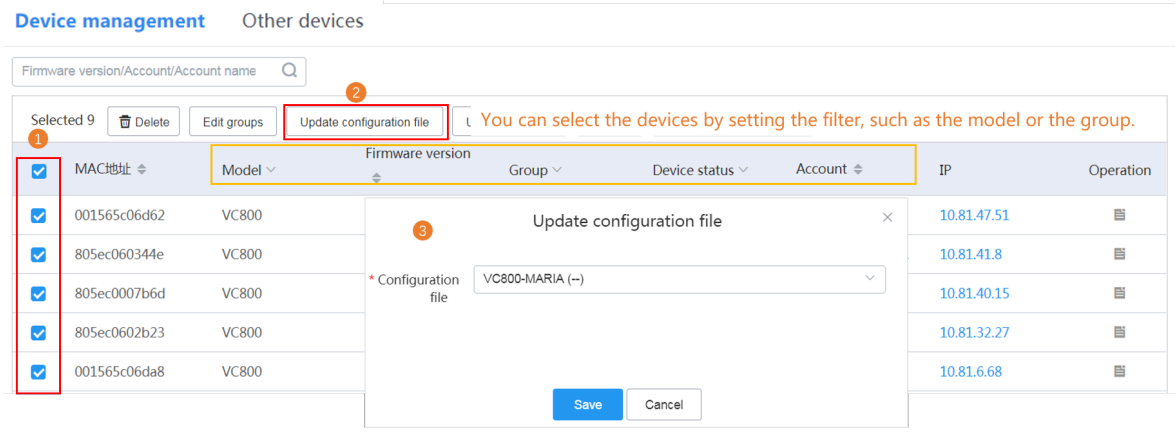


3. Do one of the following:

   - On the list of **Configuration management**, click **Push configurations** on the right side of the added configuration to go to the page of **Push configurations**.



   - Go to the **Device management** page.



4.

Pushing Firmware

You can push a firmware to upgrade an old firmware or downgrade a new firmware.

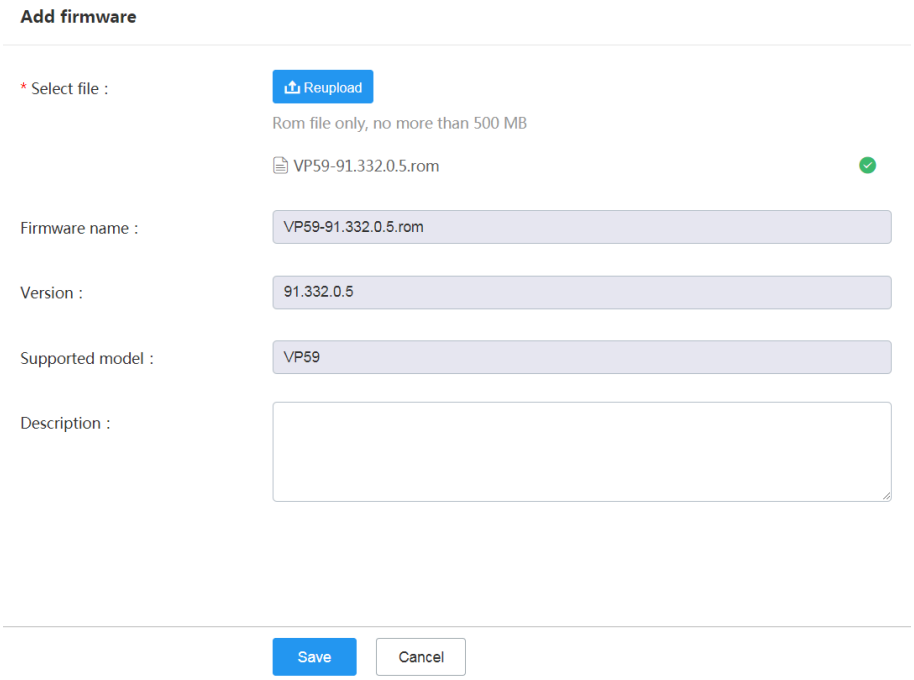
About this task

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.

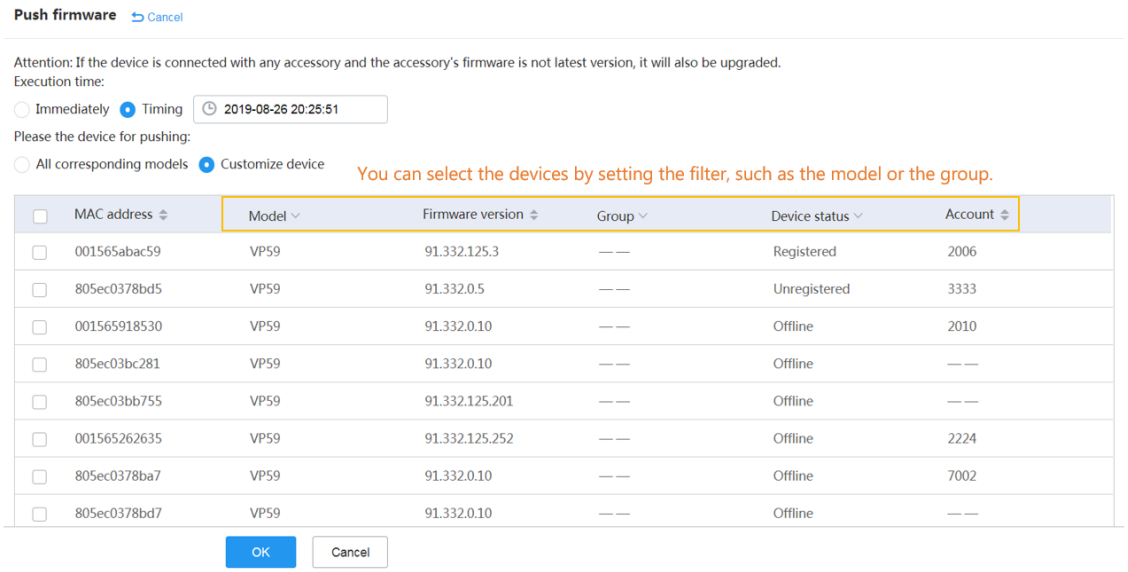
Procedure

1. Click **Device management** > **firmware management**.
2. Add the firmware.

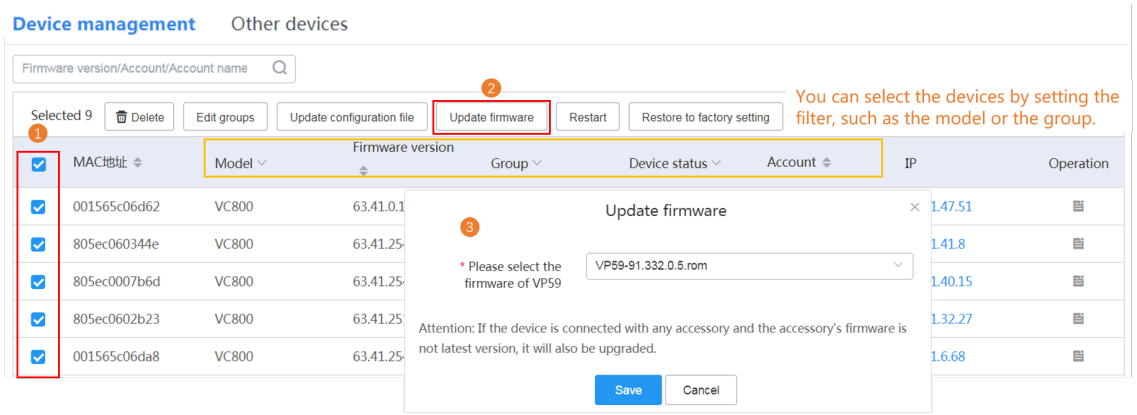


3. Do one of the following:

   - 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**.



   - Go to the **Device management** page.



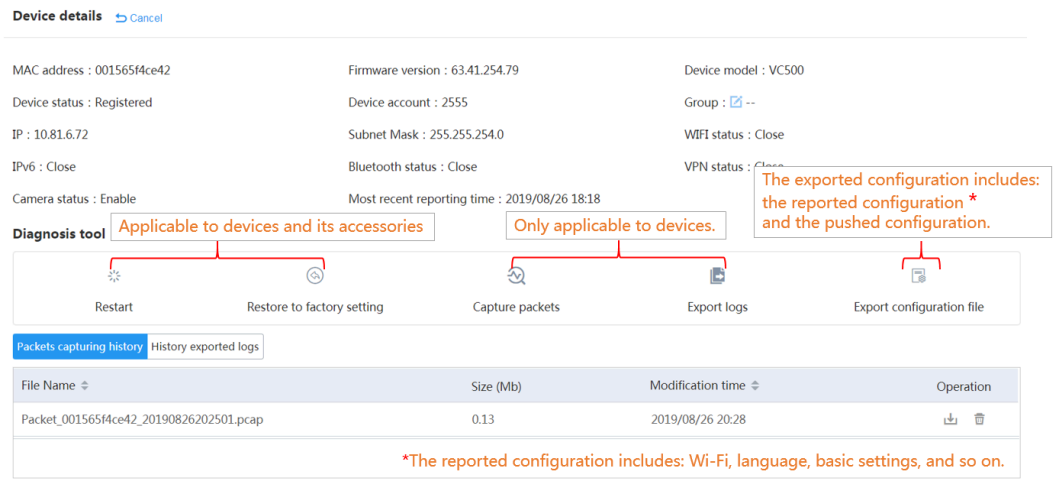
Diagnosing Devices

When problems occur to the devices, you can diagnose the device via YMS.

Procedure

1. Click **Device management** > **Device management** > .

2. In the **Diagnosis tool** field, select the desired method, and click **OK**.

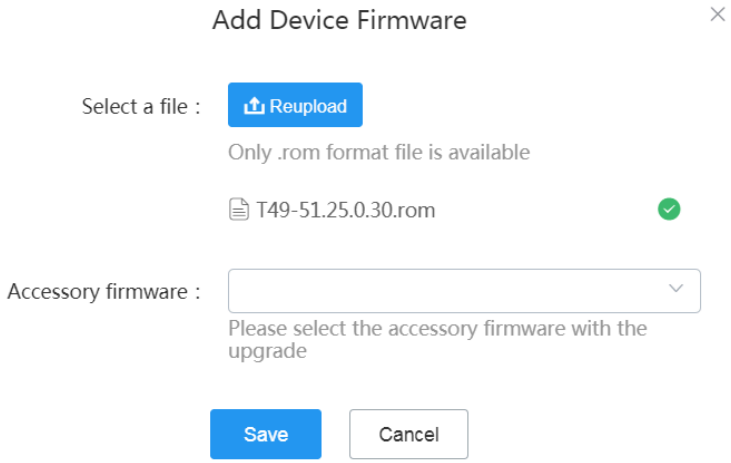


Managing T49 Devices

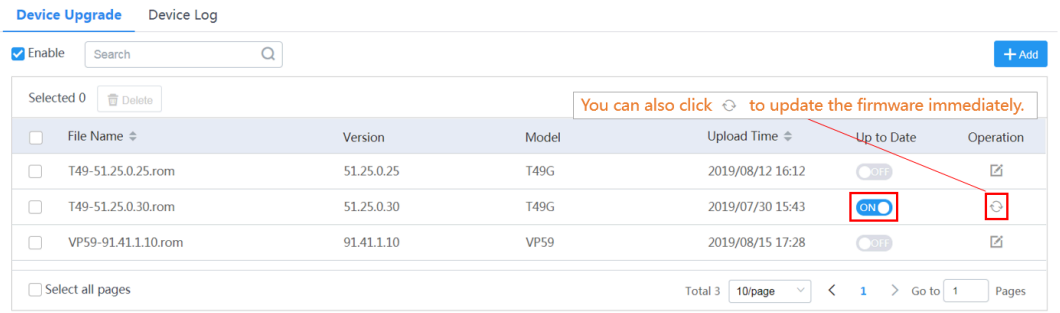
You can upgrade the firmware, enable the device log, or export the device log.

- **Pushing Firmware**

  1. Click **Device management** > **Old device management** > **Device Upgrade**.
  2. Click **Add** to add firmware.



  3. Select the **Enable** check box and enable **Up to Date**.

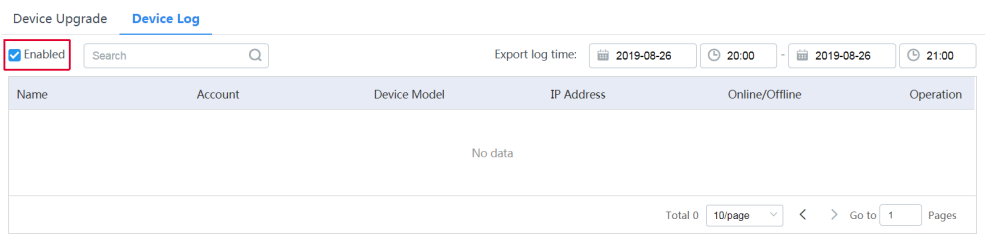


  Results: YMS will push the newest version to the device if the version of the device firmware is lower than the new one.

- **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.



- **Exporting the Device Log**

  1. Click **Device management** > **Old device management** > **Device Log**.
  2. Select the time and click .

     Note:

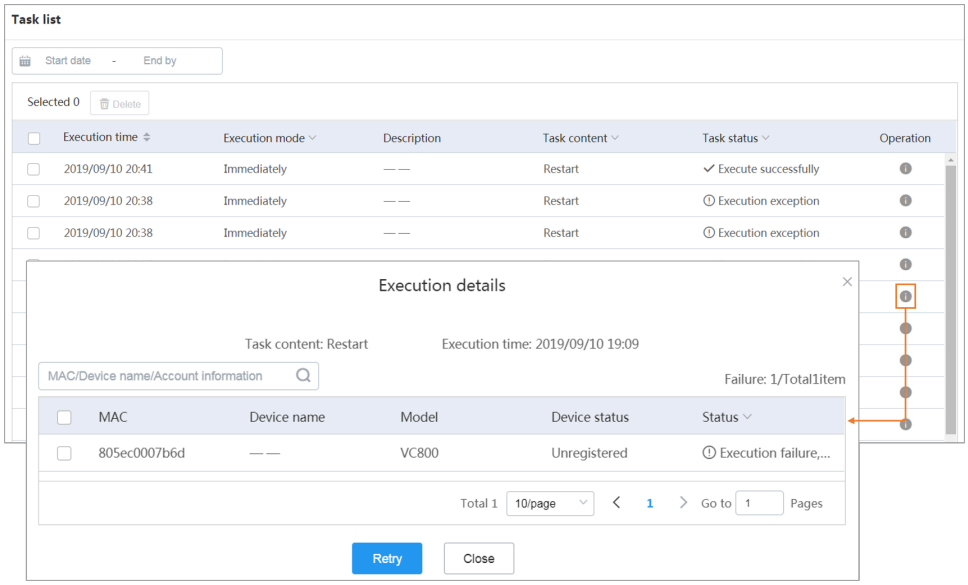
     - Only the logs in the past 7 days will be saved and can be exported. Besides, you cannot select the start date and the end date across two different months.
     - If the page prompts the file does not exist, it means that there is no device log during the time.

Viewing the Statistics of the Executed Tasks

You can view the statistics of the executed tasks, including the execution time, the execution mode (immediately/timing), the MAC, the device name, the model, the task content (updating configuration file/ updating firmware/restarting/restoring to factory settings), the task status (execution exception/execute successfully), and the details of the exceptional task.

Procedure

Click **Device management** > **Task list**.



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

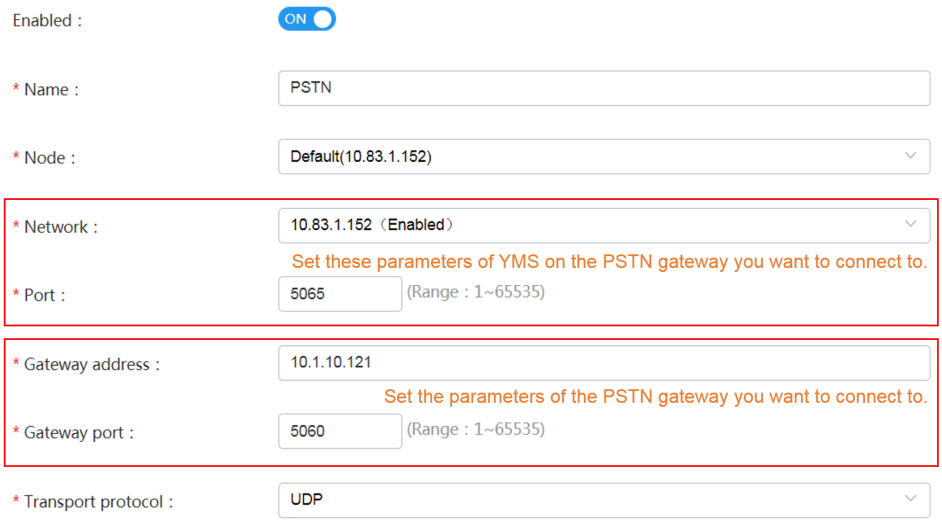
Related concepts

Common Regular Expressions and Replacement Strings

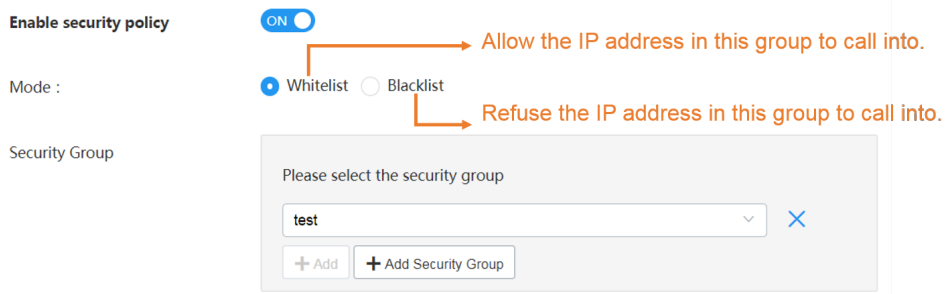
Setting the PSTN Gateway Service

Procedure

1. Click **Service** > **SIP Service** > **PSTN Gateway Service**.
2. Add a PSTN gateway service.
3. Configure the basic parameters.

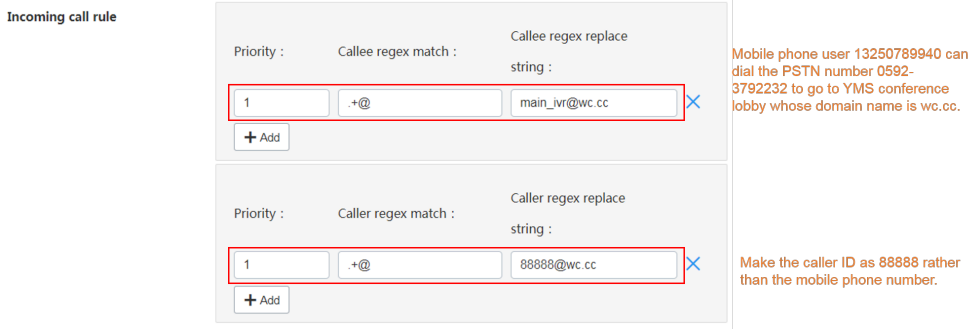


4. Optional: Configure the security policy.
   For adding a security group, seeAdding a Security Group



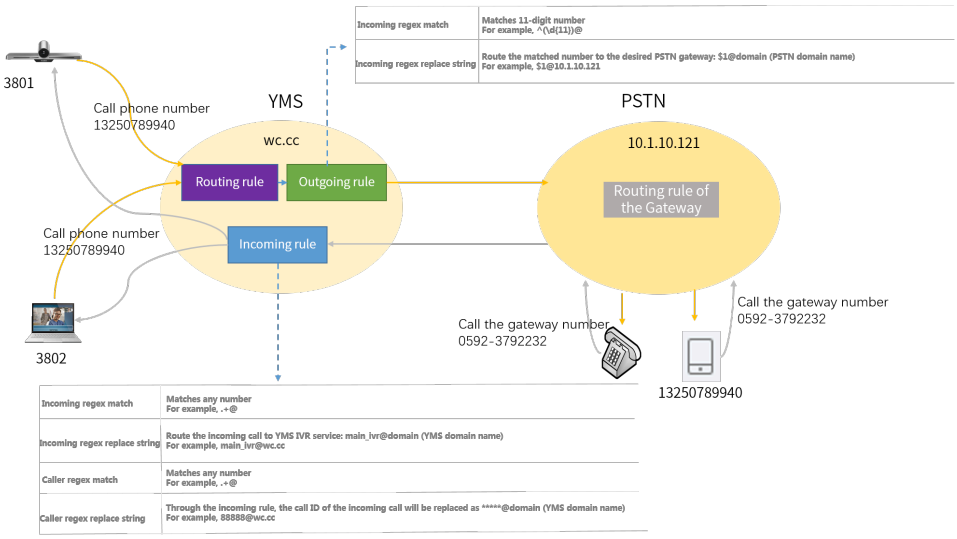
5. Configure the outgoing call rule.

6. Configure the incoming call rule.



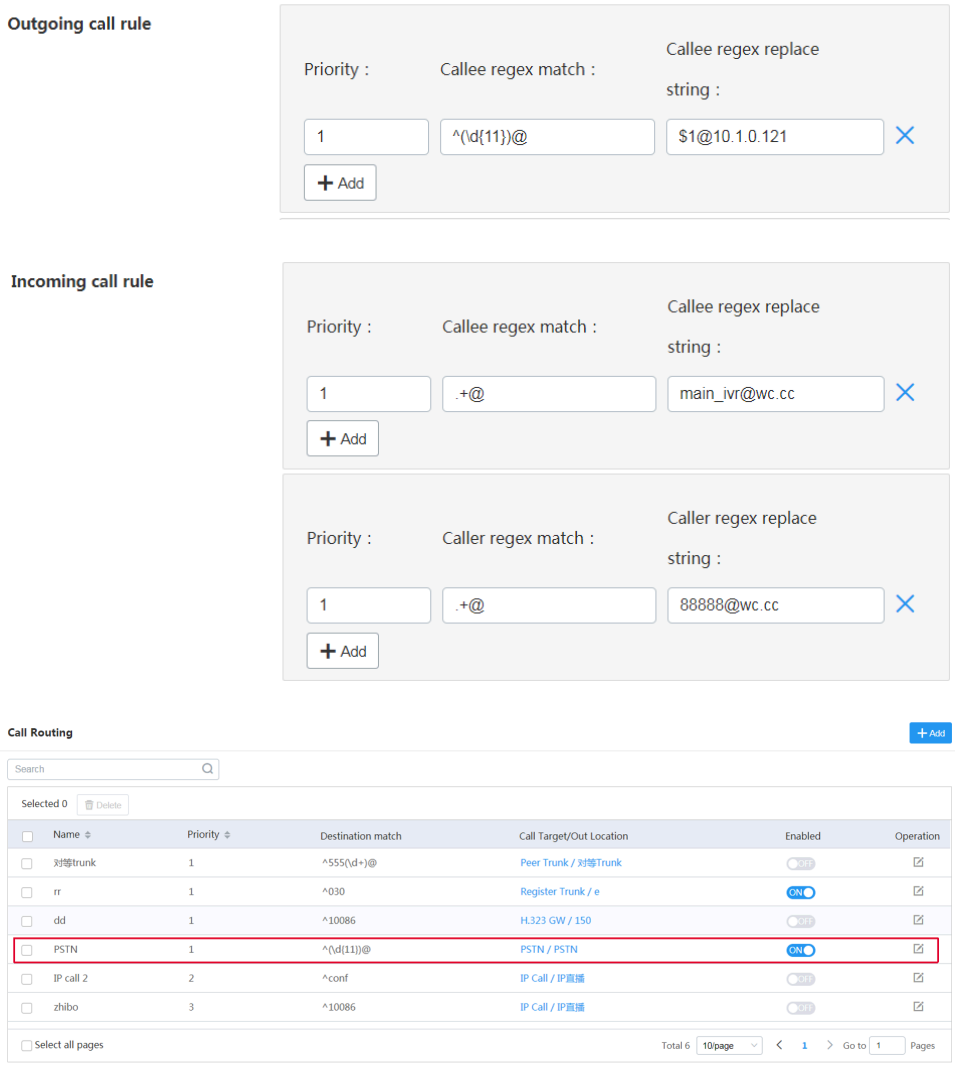
7. Save the configuration.

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



- 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.

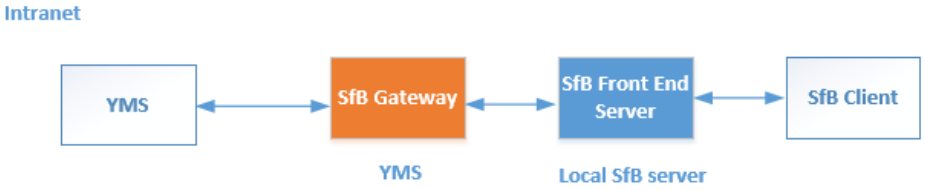
For more information about the configuration and the usage of YMS and Skype for Business server, refer to Yealink Meeting Server and Skype for Business Deployment Guide.

- 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 *sfb1.5060.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
2. Add YMS into the trusted application pool created by the SfB server.	New-CsTrustedApplicationPool **-Identity** <YMS DNS FQDN > **-ComputerFqdn** < YMS DNS FQDN > **-Registrar** <Front End Pool DNS FQDN> **-Site** < Site ID> **-RequiresReplication** $false **-ThrottleAsServer** $true **-TreatAsAuthenticated** $true **Example command:** New-CsTrustedApplicationPool **-Identity** sfb1.5060.space **-ComputerFqdn** sfb1.5060.space **-Registrar** xiamenpool.xiamen.yealinksfb.com **-Site** 5 **-RequiresReplication** $false **-ThrottleAsServer** $true **-TreatAsAuthenticated** $true	**Syntax explanation:** **-Identity**: defines the DNS FQDN of the YMS group that belongs to the trusted application pool. **-ComputerFqdn**: defines the DNS FQDN of the YMS which communicates with the SfB in the trusted application pool. 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. **-Registrar**: defines the DNS FQDN of the SfB Front-End Pool to which this trusted application pool belongs. **-Site**: defines the SfB Site ID to which this trusted application pool belongs. Run command **Get-CsSite** to get the Site ID. Others are the same as the default value. **Note**: 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: **"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."** This warning can be safely ignored as YMS is non-domain-joined, and you should answer Yes to this warning.

Procedure	Command	Syntax description
3. Add other trusted applications to the trusted application pool.	New-CsTrustedApplication **-ApplicationId** <Application ID> **-TrustedApplicationPoolFqdn** <YMS DNS FQDN> **-Port** <Available Port> **Example command:** New-CsTrustedApplication **-ApplicationId** sfb1 **-TrustedApplicationPoolFqdn** sfb1.5060.space.space **-Port** 5067	**Syntax explanation:** **-ApplicationId**: defines a friendly identifier for the YMS devices. You can customize the name and it is unique. **-TrustedApplicationPoolFqdn**: defines the trusted application pool to which this YMS belongs. **-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.
4. View the trusted application to ensure that YMS is added to the trusted application pool.	Get-CsTrustedApplication	None
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.	Get-CsStaticRoutingConfiguration	None
6. Create a new static routing configuration for the desired registrar.	New- CsStaticRoutingConfiguration –**Identity** "Service:Registar: <Front End Pool DNS FQDN>" **Example command:** New- CsStaticRoutingConfiguration –**Identity** "Service:Registrar:xiamenpool.xiamen.yealinksfb.com"	**Syntax explanation:** **-Identity**: defines the registrar to which we want to apply the static route object.

Procedure	Command	Syntax description
7. Create the static SIP domain route, and associate this route with a trusted application.	$newroute = New-CsStaticRoute -TLSRoute **-Destination**<YMS DNS FQDN> **-Port** <YMS Port> **-MatchUri** < YMS DNS FQDN> **-UseDefaultCertificate** $true **Example command:** $newroute = New-CsStaticRoute -TLSRoute **-Destination** "sfb1.5060.space" **-Port** 5067 **-MatchUri** "sfb1.5060.space" **-UseDefaultCertificate** $true	**Syntax explanation:** **-Destination**: defines the YMS DNS FQDN where SfB should send SIP requests matching the domain specified in **-MatchUri**. **-Port**: defines the source port on YMS that communicates with SfB server. It can be any unoccupied port from 0 to 65535. The default port is 5067 in YMS, and we recommend that the Port you configure is consistent with the port in YMS. **-MatchUri**: defines the matched YMS DNS FQDN.
8. Apply your required static route to your registrars' static routing configuration.	Set-CsStaticRoutingConfiguration **-Identity** "Service:Registar: <Front End Pool DNS FQDN>" -Route @{Add=$newroute} **Example command:** Set-CsStaticRoutingConfiguration **-Identity** "Service:Registrar:xiamenpool.xiamen.yealinksfb.com" **-Route** @{Add=$newroute}	**Syntax explanation:** **-Identity**: defines the registrar to which we want to apply the static route object. Others are the same as the default value.
9. View all routes in your static routing configuration to ensure that your required static route is added successfully.	Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty Route	None
10. Enable the new topology.	Enable-CsTopology	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

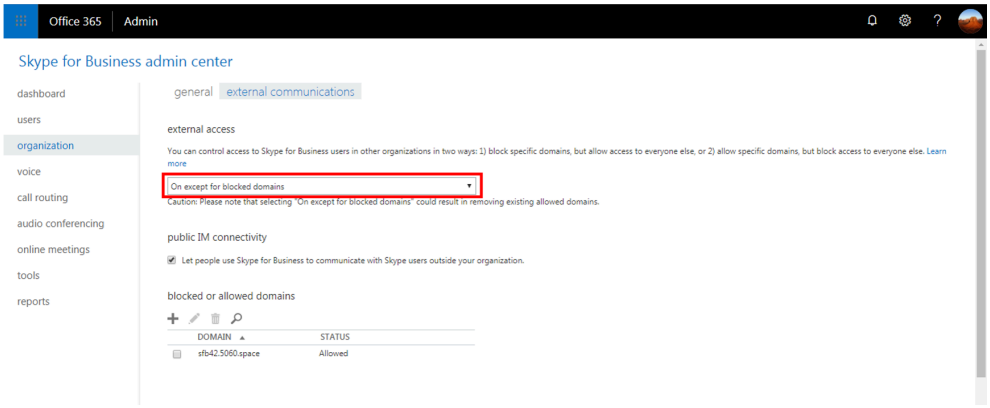
Procedure

1. Make sure that the SRV record and the A record of YMS and SfB are configured on the public DNS server.

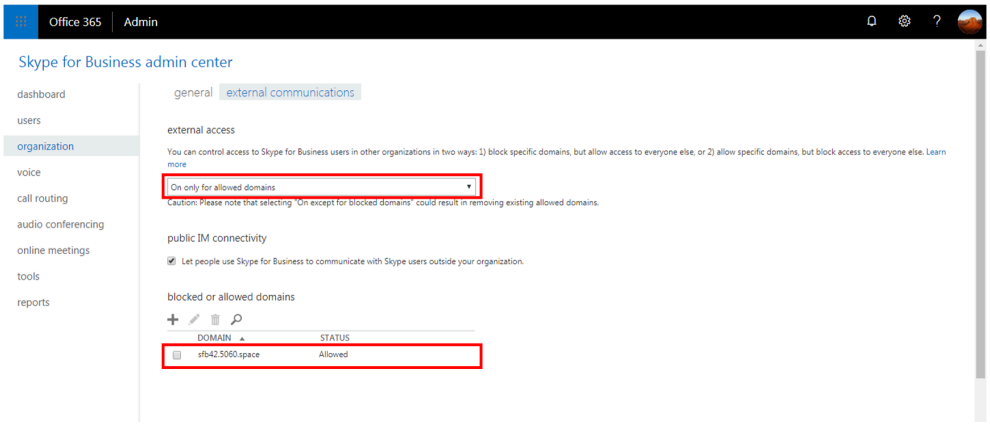
2. If you add a domain name in Office 365, and use the suffix of the added domain name to build a federation with YMS, you need to add CNAME record and SRV record to the DNS server which the added domain belongs to.

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:

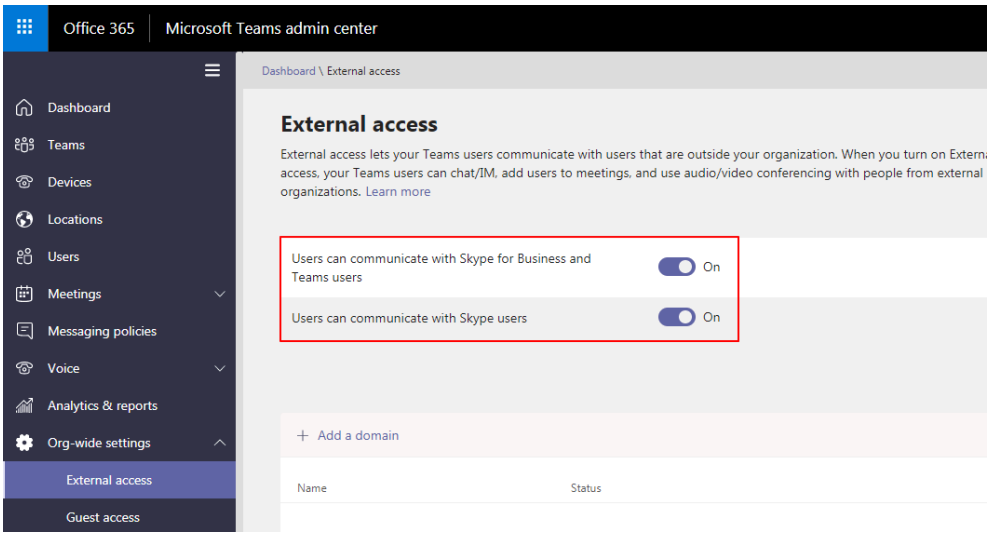
   - If you use the legacy portal of Office 365 and want to create the federation between Office365 and all the external YMSs, you need to select **On except for blocked domains** in the **External access** field on Office 365.

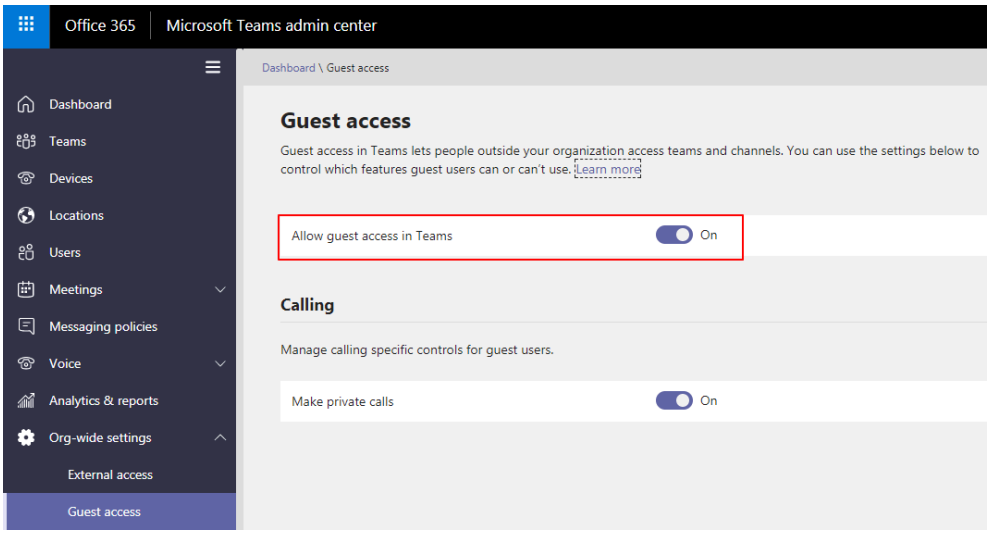


   - If you use the legacy portal of Office 365 and want to create the federation between Office 365 and one YMS, you need to select **On only for allowed domains** in the **External access** field on Office 365. Besides, the DNS FQDN of YMS is added to the allowed domain.

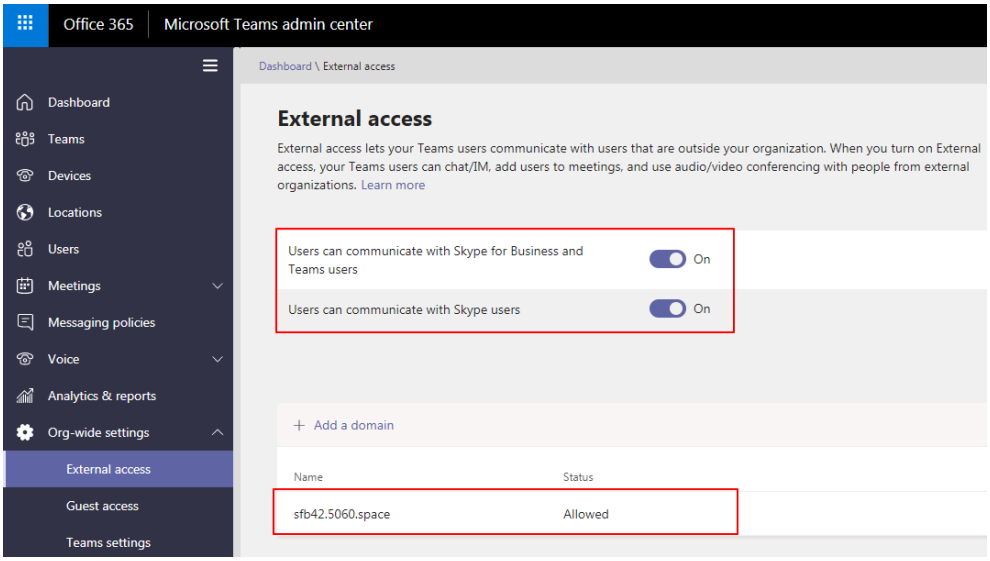


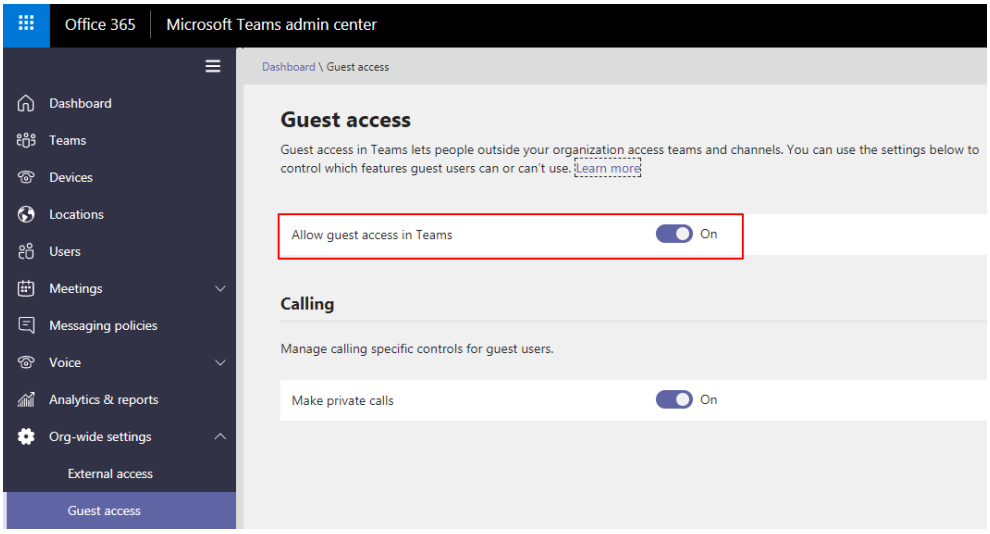
   - If you use the new Office 365 and want to build the federation between Office 365 and all the external YMSs, you should turn on the switches displayed as below:





- 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.



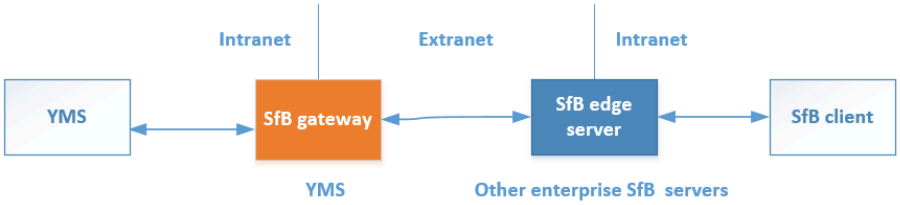


Communicating with Other Enterprise SfB Servers

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.



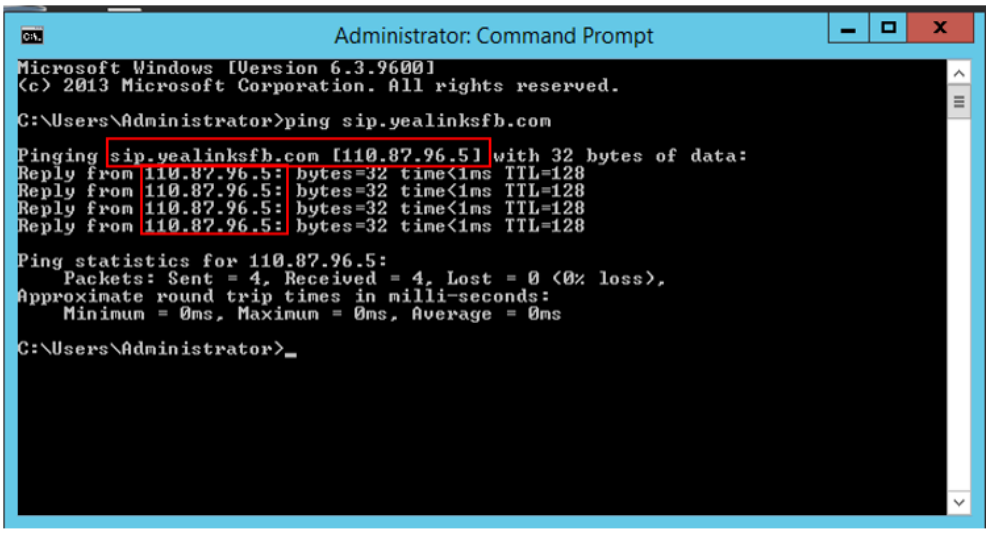
- Configuring Other Enterprise SfB Servers

Configuring Other Enterprise SfB Servers

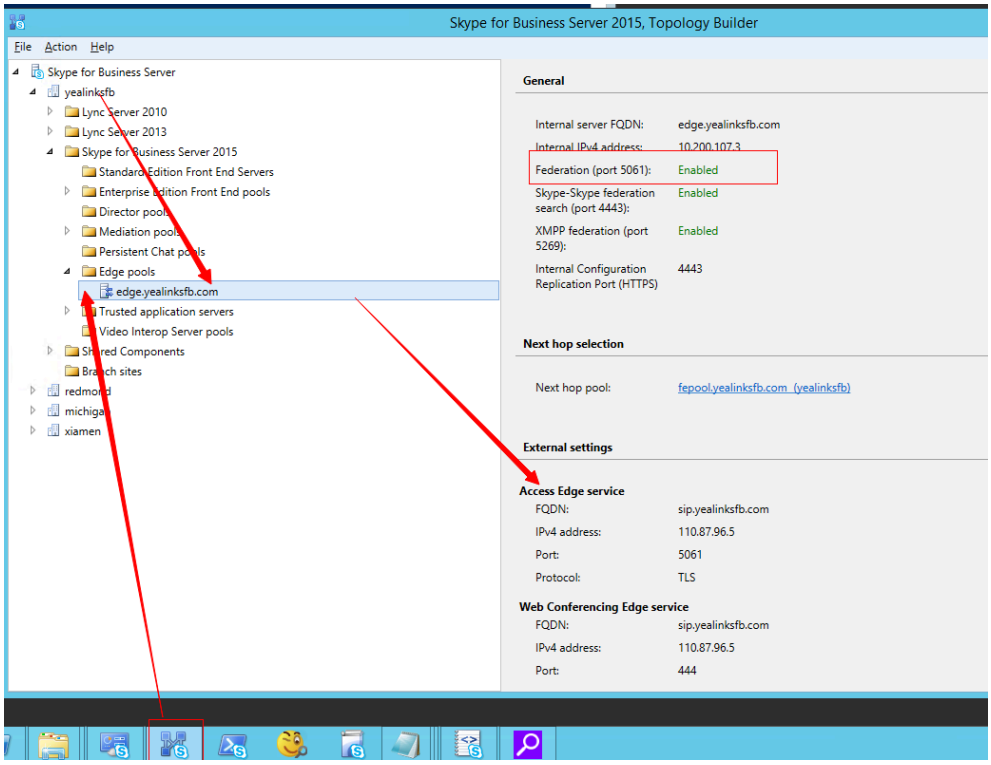
Procedure

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.



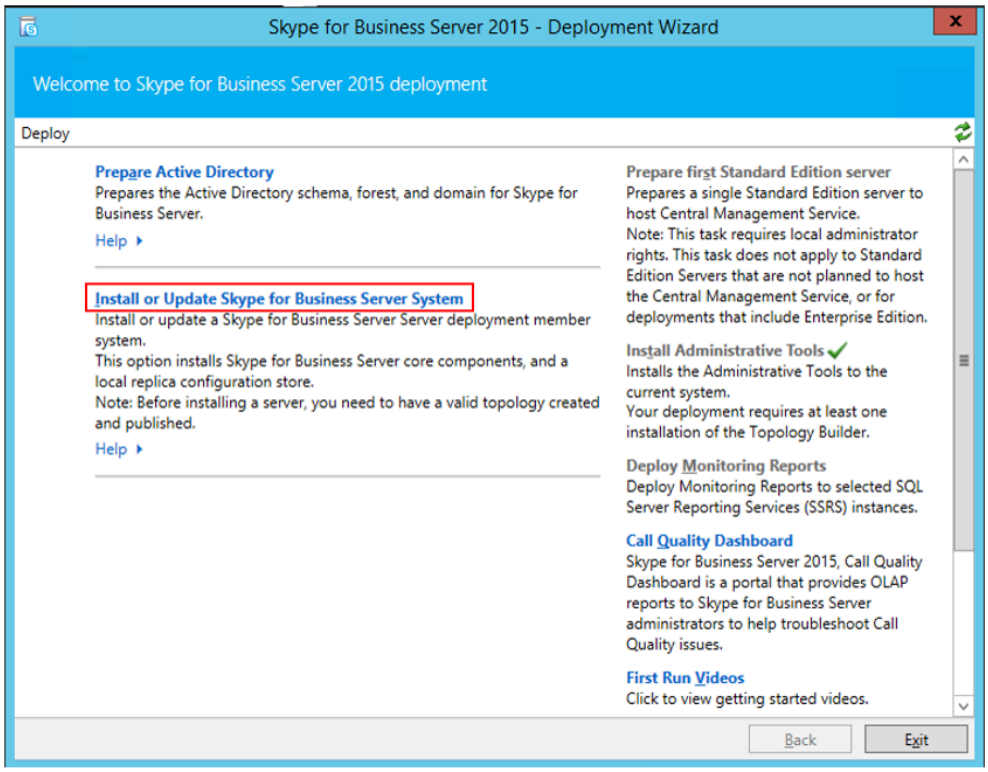
   - View the information of the SfB edge server in the Front End topology. The information includes whether or not the federation is enabled on the SfB edge server.



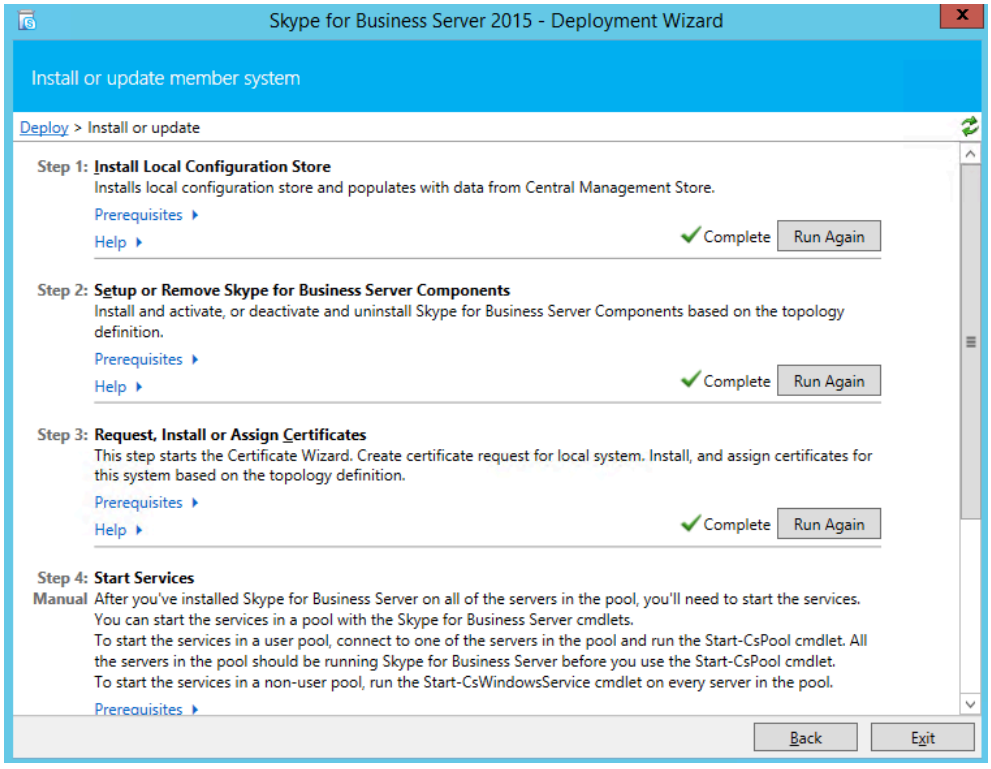
2. Make sure that the SRV record and the A record of YMS and SfB are configured on the public DNS server.
   - Log into the public DNS server where the SfB edge server is located to view the SRV record and the A record. The host record must be_sipfederationtls_tcp in the SRV record.

   - 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.

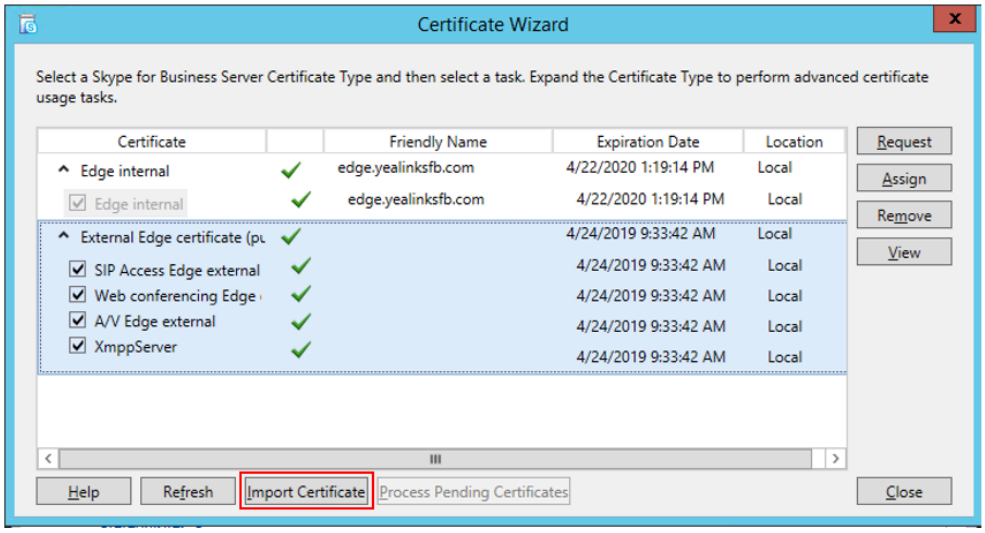
3. Check if you purchase the certificate of the SfB edge server from a trusted third-party organization. The procedure of importing the certificate is described as below:
   a) Go to the Deployment Wizard of the Lync Server, and click **Install or Update Skype for Business Server System**.



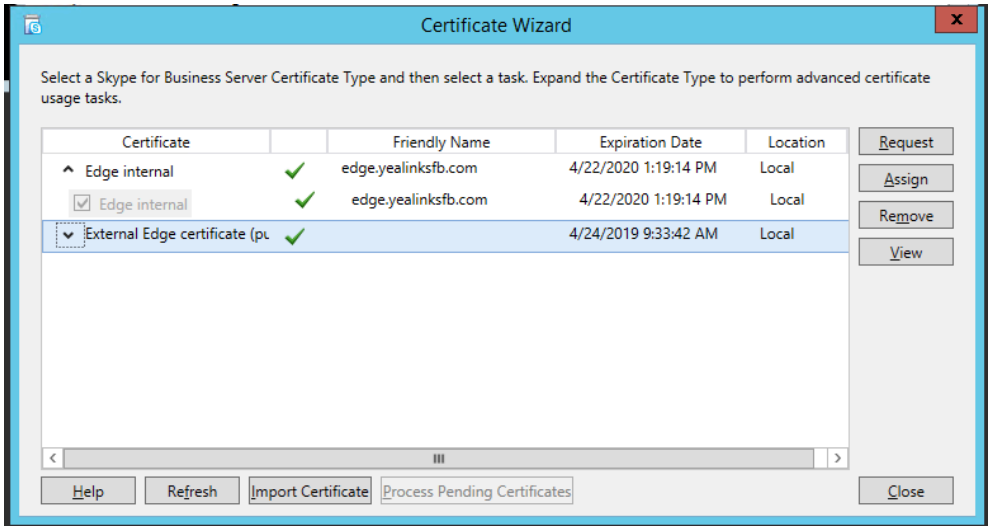
   b) Click **Run Again**.



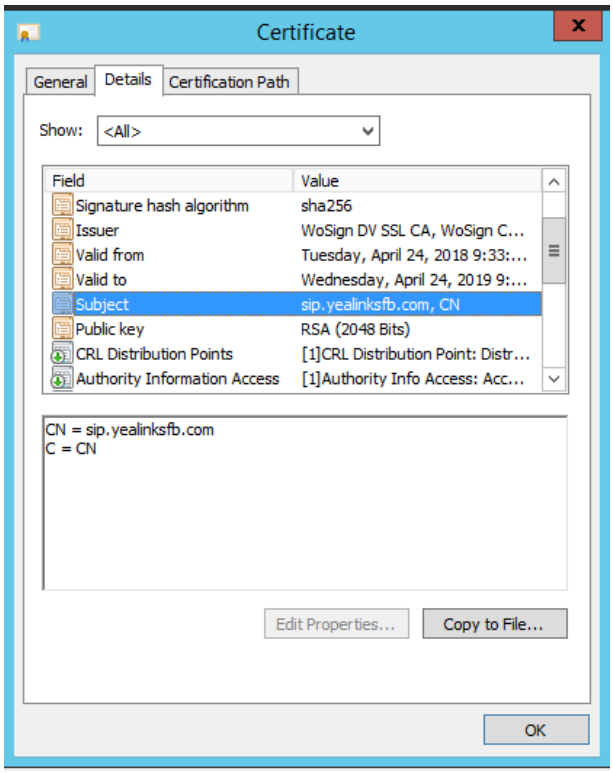
   c) Click **Import Certificate** and import the external edge certificate.



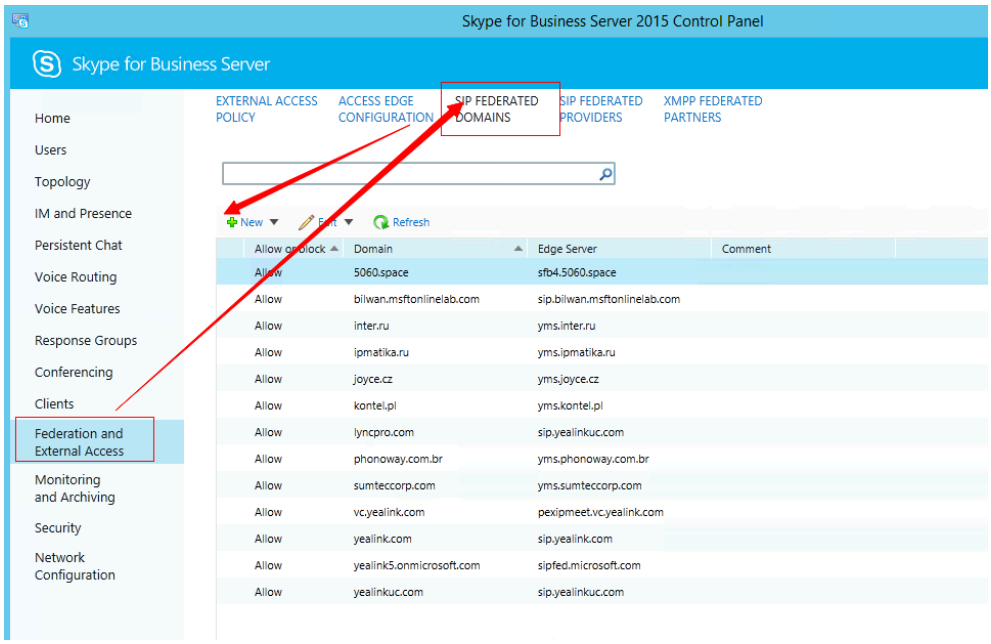
After importing, the page is shown as below:

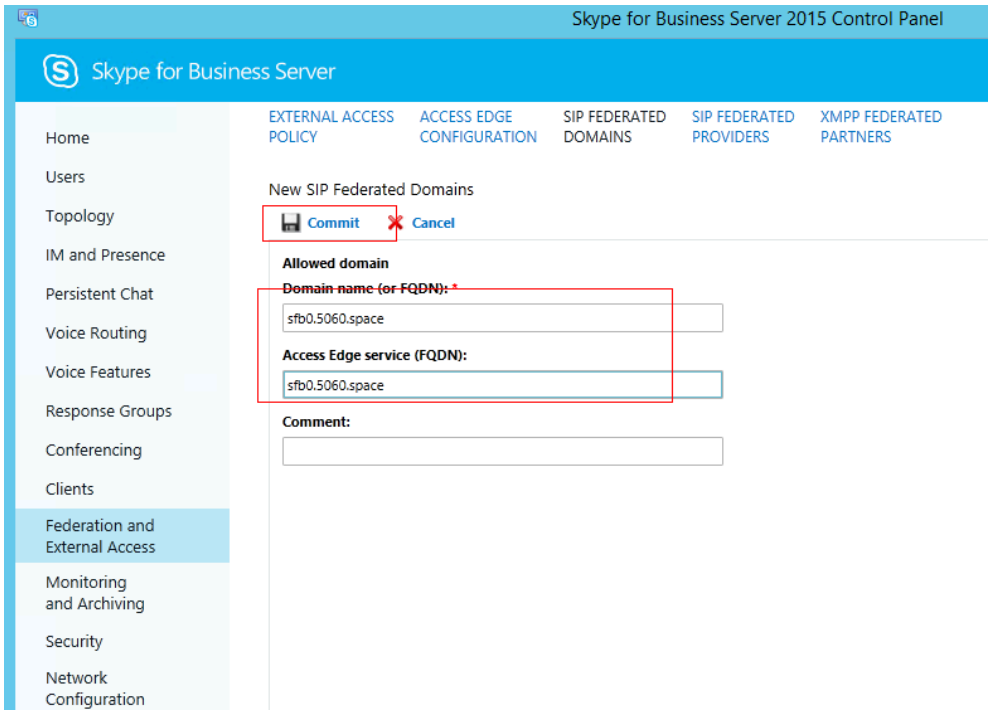


d) Select the imported edge server certificate, click **View**, and make sure that the user name (commonName attribute) or the user optional name (altNames attribute) contain the FDQN name of the edge server.


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Signature hash algorithm
sha256
Issuer
WoSign DV SSL CA, WoSign C...
Valid from
Tuesday, April 24, 2018 9:33:...
Valid to
Wednesday, April 24, 2019 9:...
Subject
sip.yealinksfb.com, CN
Public key
RSA (2048 Bits)
CRL Distribution Points
[1]CRL Distribution Point: Distr...
Authority Information Access
[1]Authority Info Access: Acc...
CN = sip.yealinksfb.com
C = CN
Edit Properties...
Copy to File...
OK

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

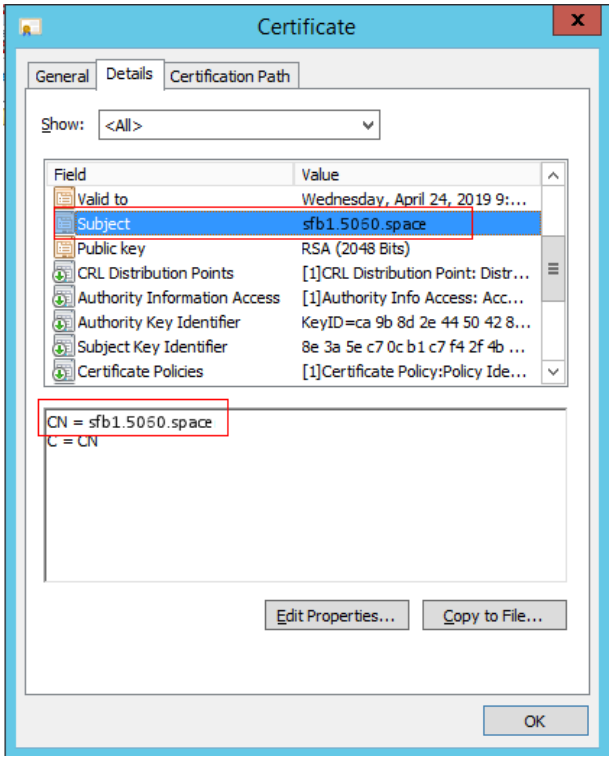
Make the SfB server trust this YMS by Importing the TLS Certificate on this YMS.

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-----
MIIEczCCA1ugAwIBAgIJALSYl2RyrkNWMA0GCSqGSIb3DQEBBQUAME8xEzARBgoJ
kiaJk/IsZAEZFgNjb20xGjAYBgoJkiaJk/IsZAEZFgp5ZWFsaW5rc2ZiMRwwGgYD
VQQDExN5ZWFsaW5rc2ZiLUFELUNBLUNBMB4XDTE3MTIyODAyMTI0MloXDTI3MTIy
NjAyMTI0MlowgZAxCzAJBgNVBAYTAkNOMQ8wDQYDVQQIEwZGdWppYW4xDzANBgNV
BAcTBlhpYW1lbjEQMA4GA1UEChMHWWVhbGluazELMAkGA1UECxMCSVQxHzAdBgNV
BAMTFnBleGlwMm1lZXQueWVhbGluay5jb20xHzAdBgkqhkiG9w0BCQEWEG1pbG9A
eWVhbGluay5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCephdy
ddIJJ9Rh/Ykx7kksD4bxK+qz50LLcIwY/qPI7ZcPUd0kf+zzd07/AQQkjza/cZgF
36R3oUBwrqJRRUZhdyHhxRYr/+wOCHrmcCkKPKLSmpKezjxTzd/x3EqlMyM4jD8j
TbTbRLjt3dZumZ03a5gBzjaj2wnFwexQ7Pmb6e4EnViW7PNfDfrtrlsQEcNUCDbc
bO+7LIPPDpP/trpYDB8U4fNuVHjko455jwTz3/wdsTwbosDISX46nywn01K8QpEB
9QlfKglA6/Tzp5yNhoT6Zx0szADdOVZ6EBh0dZc8fduNiS8rIrVj+8Bfjl4VktG2
eOJubaQcxHtZQ7k3AgMBAAGjggEOMIIBCjAMBgNVHRMEBTADAQH/MIHNBgNVHREE
gcUwgcKCFnBleGlwMm1lZXQueWVhbGluay5jb22CD1NGQjAuNTA2MC5zcGFjZYIP
U0ZCMS41MDYwLnNwYWNlgg9TRkIyLjUwNjAuc3BhY2WCD1NGQjMuNTA2MC5zcGFj
ZYIPU0ZCNC41MDYwLnNwYWNlgg9TRkI1LjUwNjAuc3BhY2WCD1NGQjYuNTA2MC5z
cGFjZYIPU0ZCNy41MDYwLnNwYWNlgg9TRkI4LjUwNjAuc3BhY2WCD1NGQjkuNTA2
MC5zcGFjZTAdBgNVHQ4EFgQUxXmjM3vh1JEgQX2WpmFTpNEJZoowCwYDVR0PBAQD
AgXgMA0GCSqGSIb3DQEBBQUAA4IBAQBtp42PO5TXqPNvEqn1O4QcEBXbukKmErOq
CqxksUVyudOQ/5qqyd6x9K1M/6BmAS2Fi/1463PaoiQEZDAbDHw0UyAvisOyUDDw
WYEAYa2vIe2tvE/NW7TFysWgHPWcvjLN91wtLNDVjJkb7r4Et7//TnRc5oHL5ok9
En43cfZ3inev1HgFhne3C6iHVip5X4T7rZO5j9G5lQYp9Jw4GwiCT2syP2DOl0u/
Yf6h/yIwnYLE3s4MFwqkD4fRJh8p+aCjabhjxUPWvk7PCctmaceWUg1VRDIgZB4L
xSzPAeywK+qgvrYfAQFTB2OpAxVBXHuBswo/6oPmtvJso50R+Qdt
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAnqYXcnXSCSfUYf2JMe5JLA+G8Svqs+dCy3CMGP6jyO2XD1Hd
JH/s83dO/wEEJI82v3GYBd+kd6FAcK6iUUVGYXch4cUWK//sDgh65nApCjyi0pqS
```

Procedure

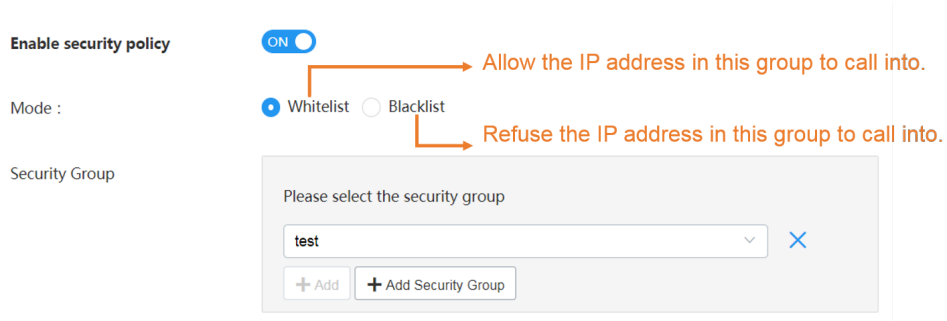
1. Click **Service** > **SIP Service** > **Skype for Business**.
2. Add a SfB gateway service.
3. Set the parameters.

Table 37: Basic Parameters

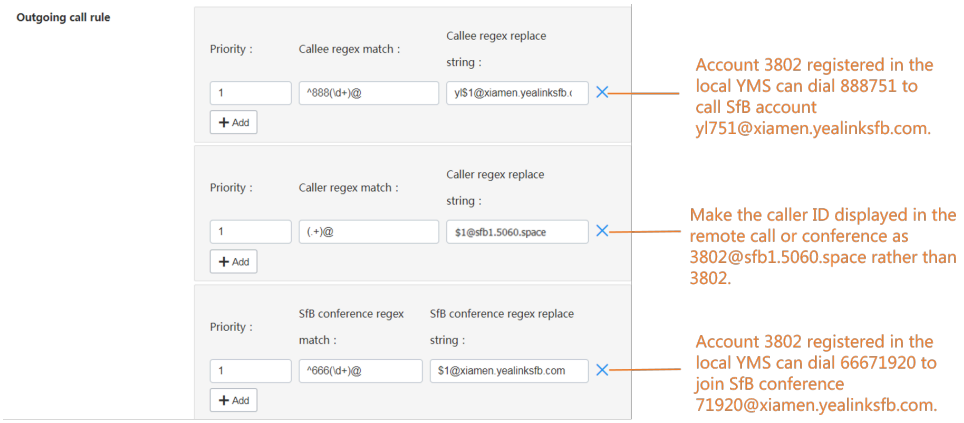
Parameter	Description
Enabled	Enable or disable the SfB gateway server. **Default**: enabled.
Name	Specify the name of SfB gateway.
Node	Specify the node used by this SfB gateway.
Network	Specify the IP address of this node.
Transport protocol	Only TLS is available if communicating with SfB.
FQDN	Specify the name of YMS. Example: sfb1.5060.space **Method**: add this domain name on DNS server which the A record of YMS is added to.
Port	Specify the source port on YMS to communicate with SfB server. **Note**: 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. **Default**: 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.
Domain	Specify the domain name of SfB server. For example, xiamen.yealinksfb.com.
Port	Specify the source port of the SfB server to communicate with YMS. **Default**: 5061.
Federation	Enable or disable the federation. **Default**: disabled. According to different SfB servers, you can enable or disable the federation in one of the following scenarios: • If the SfB server is the local SfB server, you can disable the federation. • If the SfB server is Microsoft Office 365 or other enterprise SfB servers, you can enable the federation.
Outbound proxy	Enable or disable it to allow the SfB server to send requests to the outbound proxy server. **Default**: disabled.
Proxy address	Specify the IP address or the domain name of this outbound proxy server.

Parameter	Description
Proxy port	Specify the port of this outbound proxy server. **Note**: the value can be any integer from 0 to 65535.
Support video	If you enable this, you can place video calls to the remote that supports video calls. **Default**: enabled.

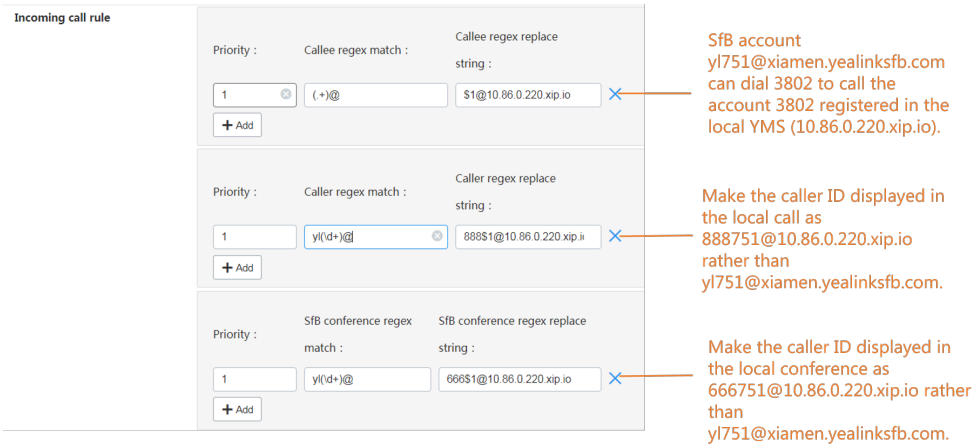
4. Configure the security policy.
   For adding a security group, seeAdding a Security Group



5. Configure the outgoing call rule.



6. Configure the incoming call rule.



7. In the **SfB certificate** field, select the desired certificate to make the SfB server trust this YMS.
8. Save the configuration.

Related concepts

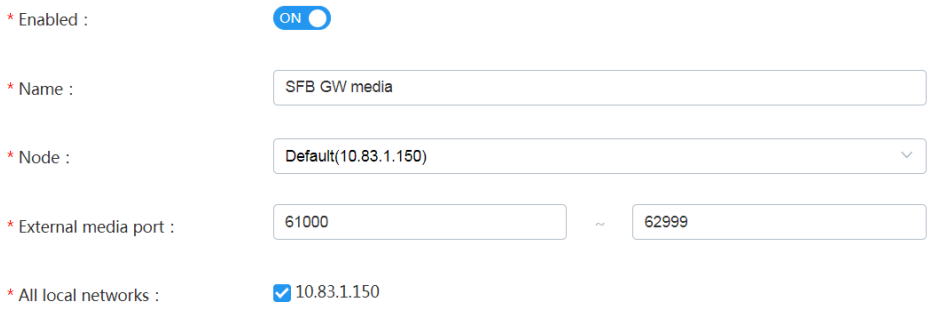
Common Regular Expressions and Replacement Strings

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.



4. Save the configuration.

Communicating with Another YMS or Third-Party PBX (Peer Trunk)

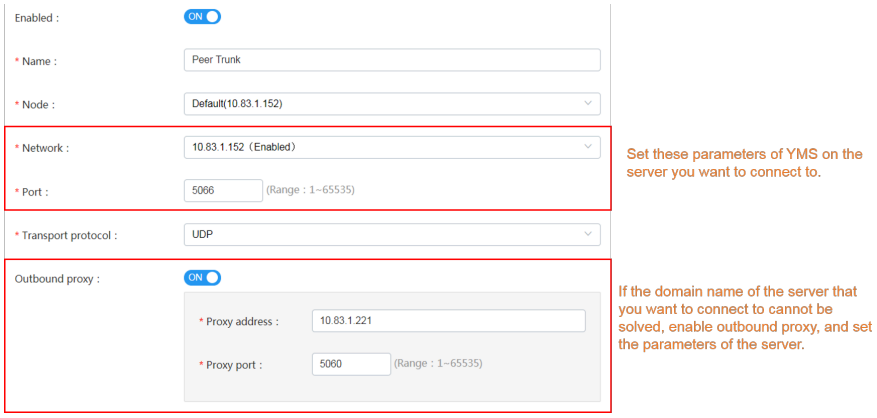
To route calls between accounts registered in two different servers (for example, CUCM accounts and YMS accounts), Setting the Peer Trunk Service and Adding a Call Routing Rule need to be done.

- 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.



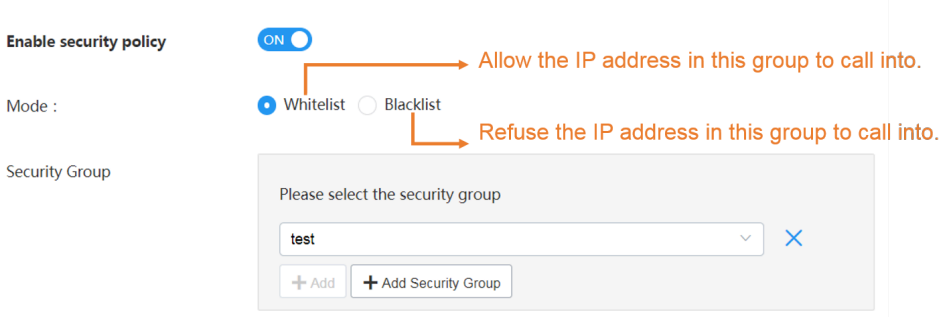
4. Enable **Media Bypass** to improve the server performance and to support a larger number of participants in the conference. Note that the third-party devices have lower compatibility.

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

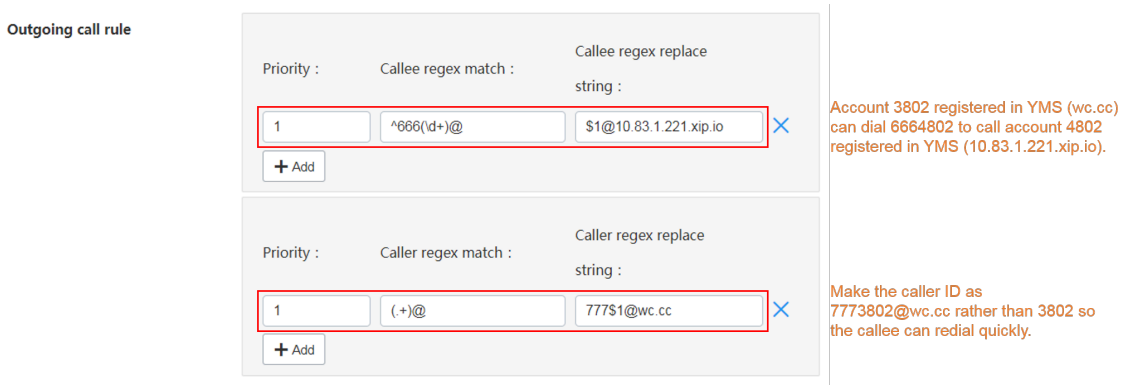
   If **Media Bypass** is enabled, Media bypass service should be enabled too. For more information, refer to Configuring the Media Bypass Service.

5. Optional: Configure the security policy.

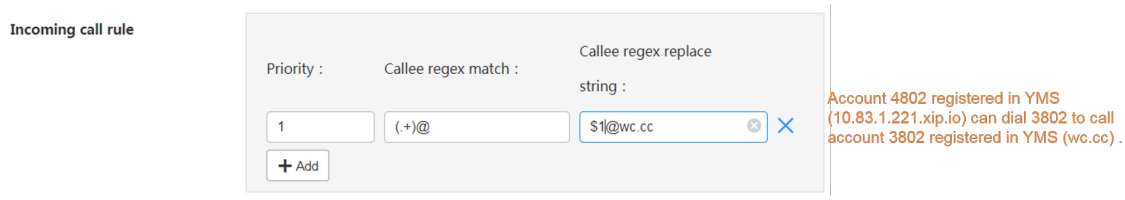
   For adding a security group, seeAdding a Security Group



6. Configure the outgoing call rule.



7. Configure the incoming call rule.

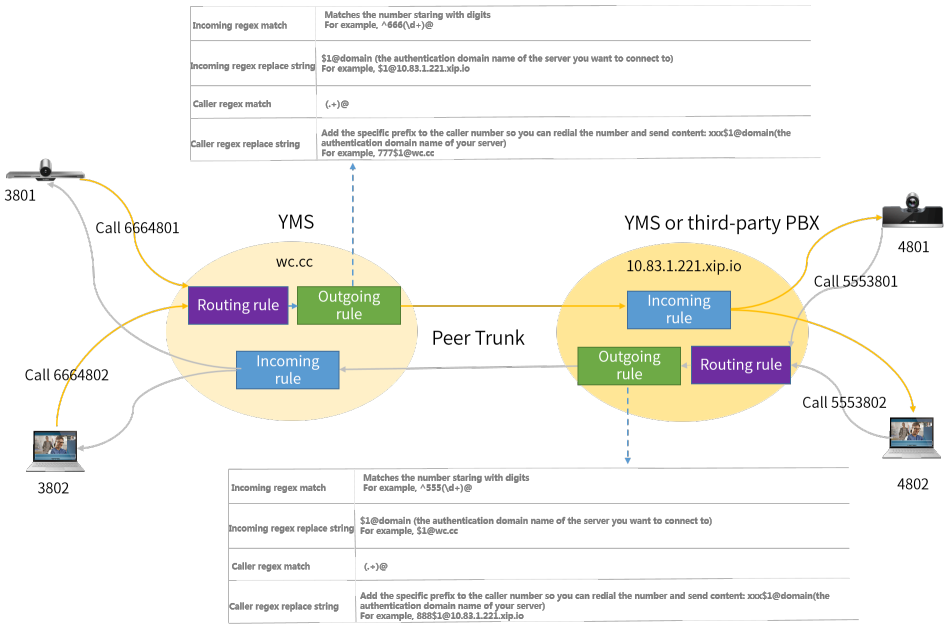


8. Save the configuration.

Related concepts

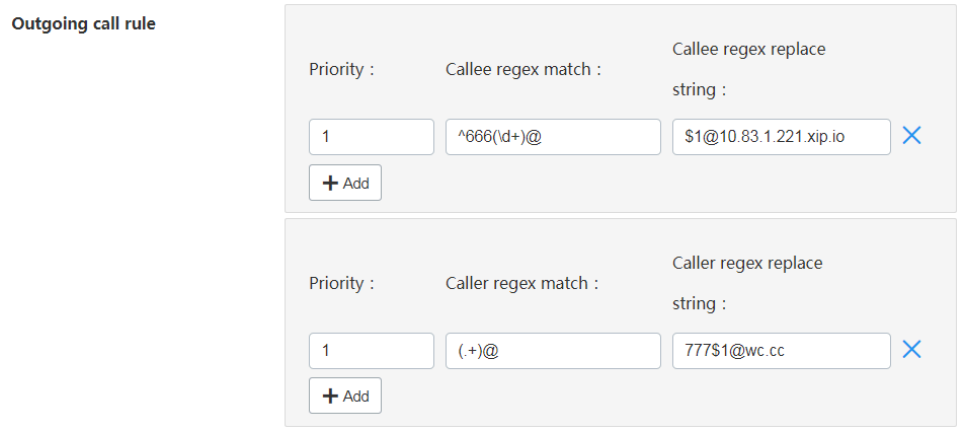
Common Regular Expressions and Replacement Strings

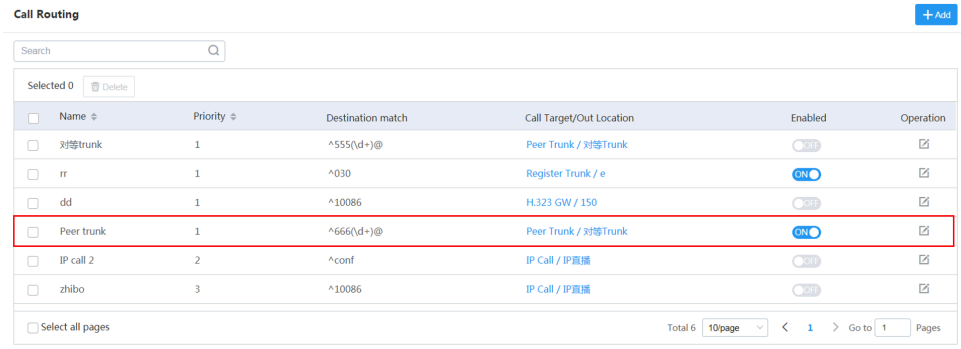
Peer Trunk Example



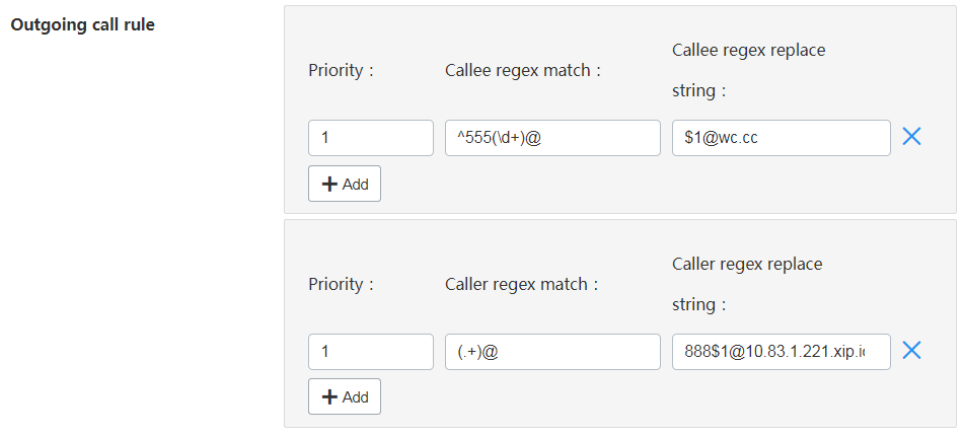
- **Situation**
  - YMS SIP account 3802 can dial 6664802 to call another YMS SIP account 4802. You can make the caller ID as 7773802 rather than 3802, and the callee can redial 7773802 to call 3802.
  - YMS SIP account 4802 can dial 5553802 to call YMS SIP account 3802. You can make the caller ID as 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.

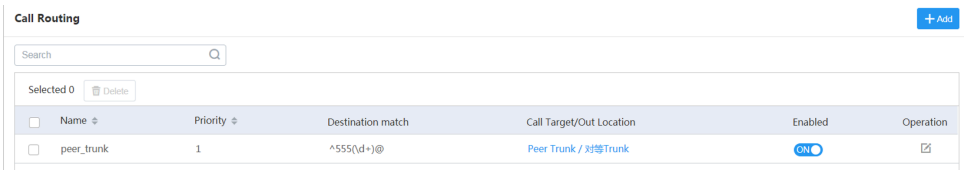
- **The configurations are as below:**
  - Enable the peer trunk service on both servers
  - Set the outgoing call rule and the call routing on server wc.cc





  - Set the outgoing call rule and the call routing on server 10.86.1.221.xip.io





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.

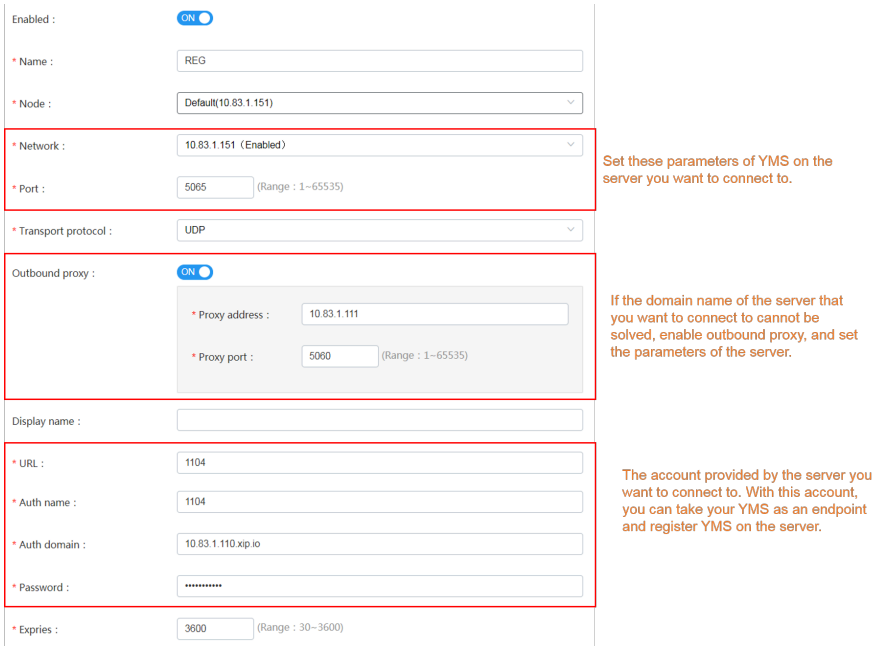
YMS accounts can call third-party accounts directly, while third-party accounts can only call into YMS conferences but cannot place P2P calls to YMS account. Besides, the P2P call can only be transmitted by third-party accounts registered in YMS.

- 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.

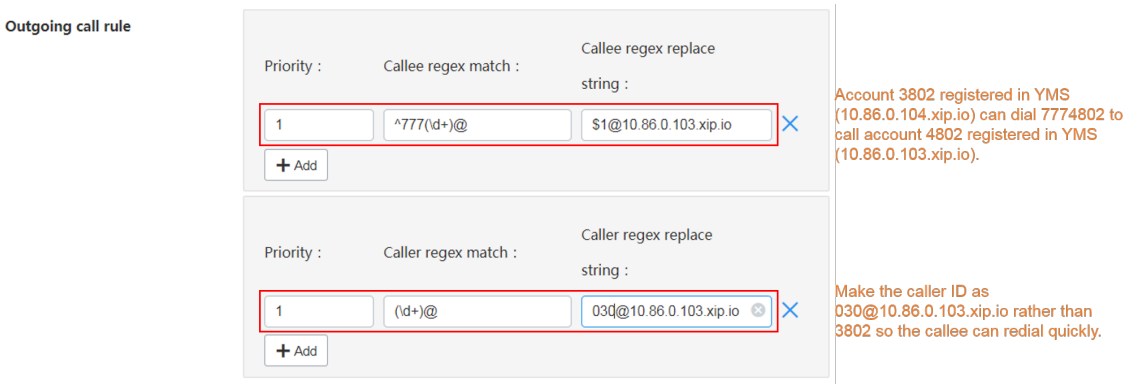


4. Enable **Media Bypass** to improve the server performance and to support a larger number of participants in the conference. Note that the third-party devices have lower compatibility.

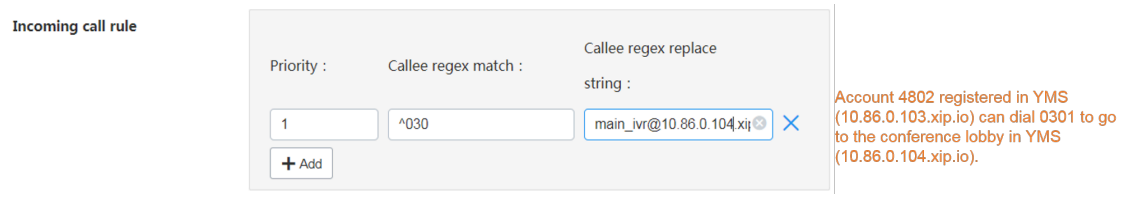
   If **Support video** is enabled, **Media Bypass** is recommended to be enabled.

   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.



6. Configure the incoming call rule.

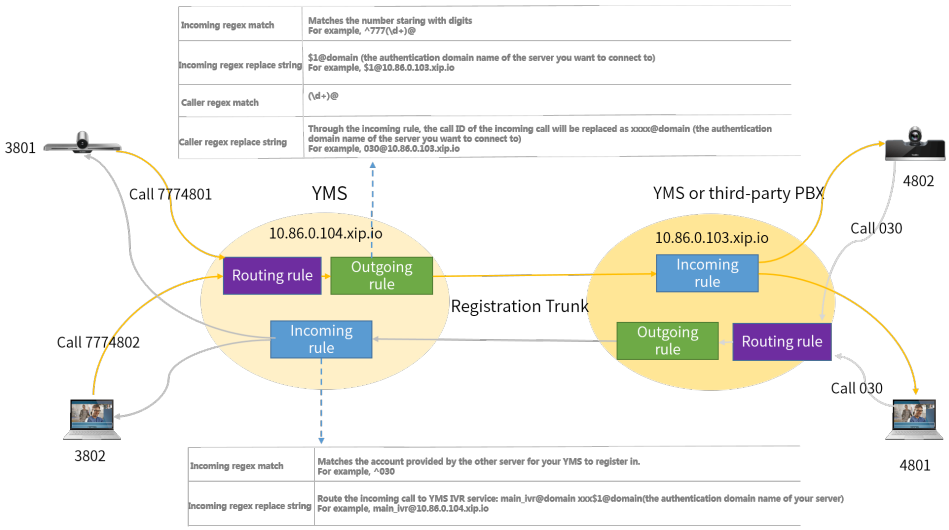


7. Save the configuration.

Related concepts

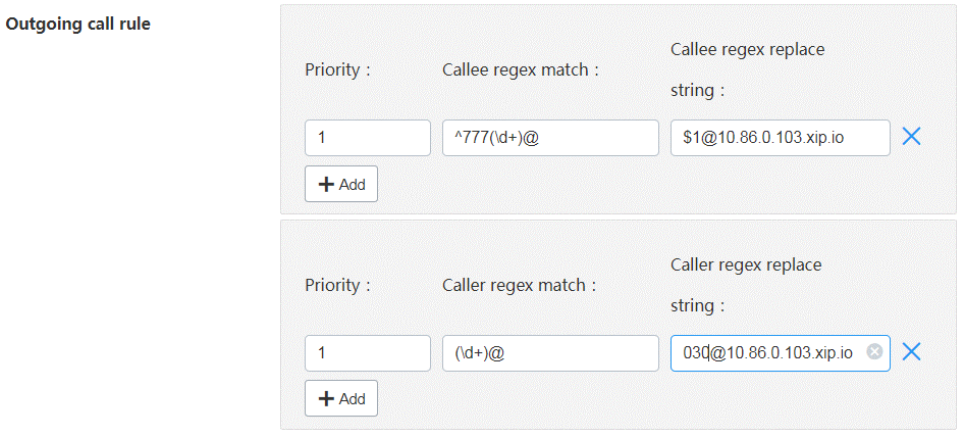
Common Regular Expressions and Replacement Strings

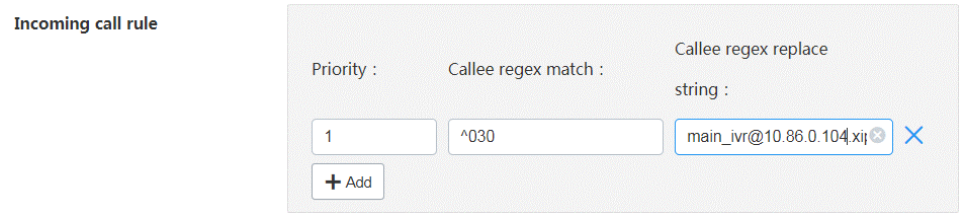
Registration Trunk Example

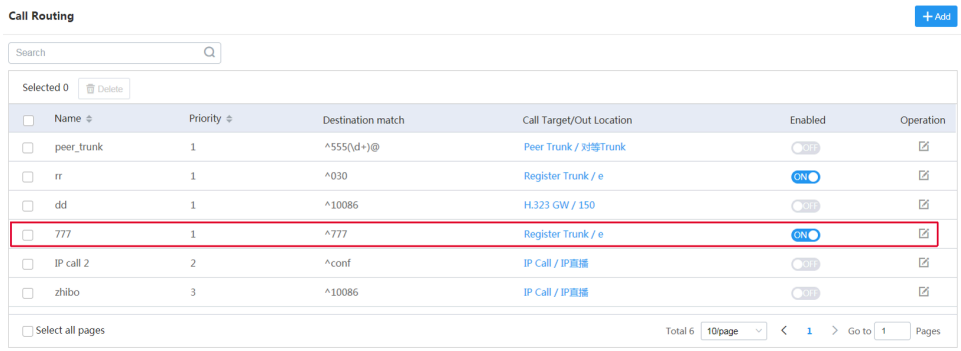


- **Situation**
  - YMS SIP account 3802 can dial 7774802 to call another YMS SIP account 4802.
  - YMS SIP account 4802 can dial 030 to go to the conference lobby of another YMS (SIP trunk IVR). YMS SIP account 4802 can dial the extension number or join the conference according to the prompts.

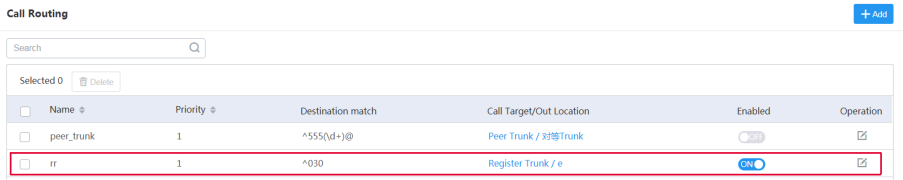
- **The configurations are as below:**
  - Enable the registration services on both servers
  - Enable the third party registration service on server 10.86.0.103.xip.io (the outbound proxy of the registration service on server 10.86.0.104.xip.io directs to this node).
  - Set the outgoing call rule, the incoming call rule, and the call routing on server 10.86.0.104.xip.io







- Set the call routing on server 10.86.0.33.xip.io



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.

YMS uses the RTMP live service and the interface provided by Alibaba. 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**.

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 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 You Tube 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.

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
Organizer Logo	Specify the logo displayed on the Webcast page.
Domain	Specify the domain name of the server.
Application name	Specify the application name in the authentication URL.
Live domain	Specify the domain name.
Edge Ingest	Specify the streaming method. **Note**: if your domain name for watching is added after February 21, 2019, you cannot use the Live Center Ingest method.
Enable authentication	Enable or disable the authentication. **Default:** disabled.
Authentication key	Specify the authentication password.

4. Click **Save**.
5. Operate according to the prompts, and click **OK**.

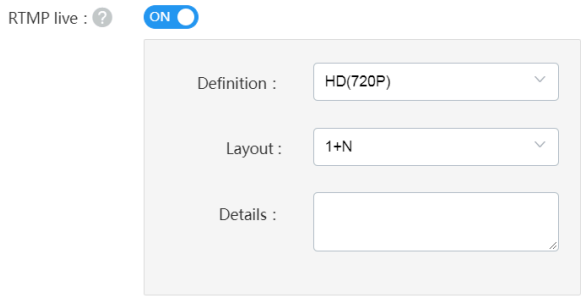
Related tasks

Configuring the RTMP Media Service

Setting the RTMP Live for VMRs

Procedure

1. Click **Meeting Room** > **Virtual Meeting Room**.
2. Do one of the following:
   - If you want to add a VMR, click **Add Meeting Room**.
   - If you want to edit a VMR, click .



3. In the **Permission setting** field, set the parameters.

Table 39: 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. **Default**: disabled.
Definition	It refers to the video resolution that the MCU sends to a public streaming services. The supported video resolution is as below: • 1080P(1080P) • HD(720P) **Default**: HD.
Layout	Configure the video layout displayed in the webcast. The supported layouts are as below: • **1+N**: 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. • **Picture in picture**: 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. • **Selected speaker**: 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. • **Default controlled layout**: the audience can see the same video layout as the conference participants. Besides, this layout will change as the conference moderator changes the video layout.
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.

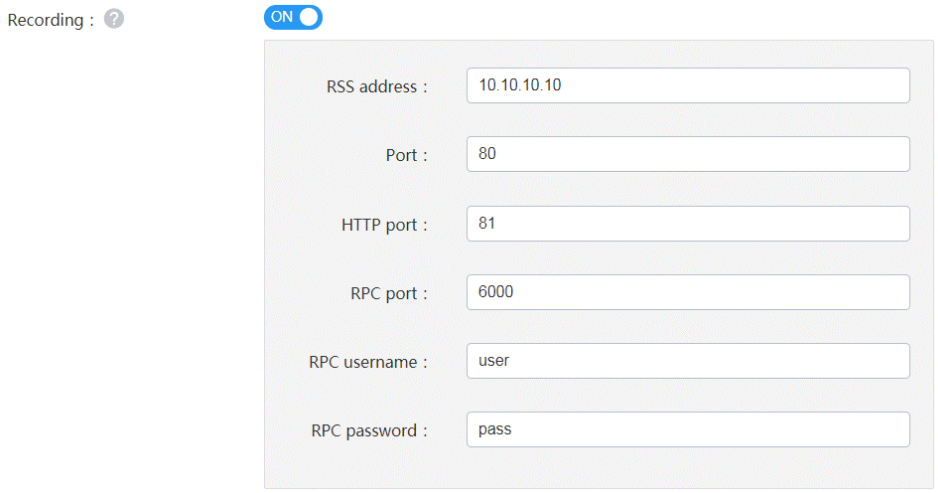
About this task

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.



3. Save the configuration.

Immersive TelePresence

With the immersive TelePresence, YMS allows you to use the following features:

- Any venue can call into the TelePresence meeting room to establish TelePresence conferences.
- In a multi-party immersive TelePresence conference, every venue can see the real-time video images of other venues, and adjust the video layout.
- In a multi-party immersive TelePresence conference, every venue can switch the video images of other venues.
- When a participant of a venue is speaking, you can send the video image of this venue to other venues.
- Collaboration
- Recording

Note: You can subscribe to this service from Yealink technical support. For more information about using the immersive TelePresence, refer to Immersive TelePresence User Guide.

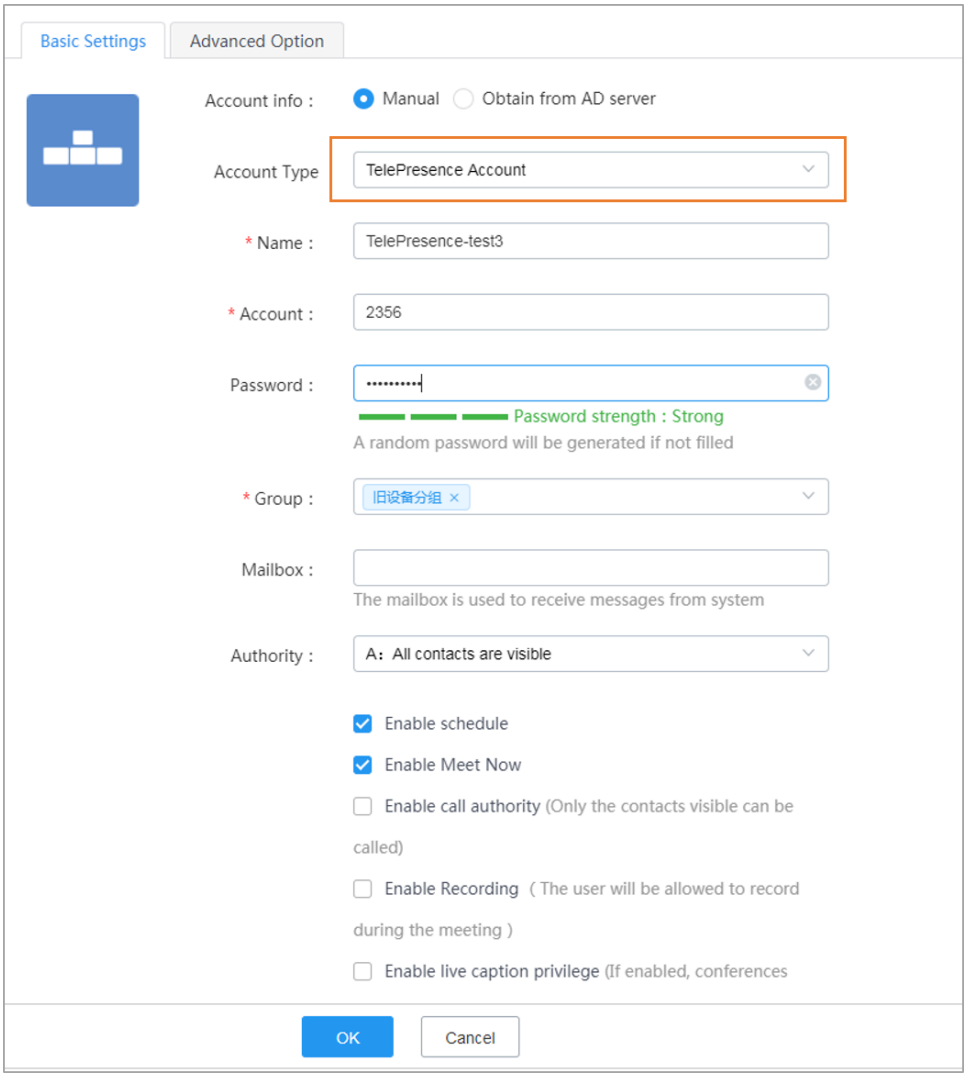
- Adding TelePrence Accounts
- Adding TelePresence Meeting Rooms
- Introduction of the TelePresence Recording
- Controlling Conferences

Adding TelePrence Accounts

Procedure

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

2. Add an account.



Adding TelePresence Meeting Rooms

About this task

By default, YMS allows up to 4 participants using TelePresence devices to join the conference. If the number of participant using TelePresence devices is not larger than the maximum number, other participants using general devices can still join the conference. The details are as below:

- 4 TelePresence device: 12 videos + 1 content
- 3 TelePresence device + 1 general devices: 10 videos + 1 content
- 2 TelePresence device + 2 general devices: 8 videos + 1 content
- 1 TelePresence device + +3 general devices: 6 videos + 1 content
- 4 general devices: 4 videos + 1 content

Note: A TelePresence meeting room can hold up to 40 participants using TelePresence and general devices. If you want to subscribe to this service or know more specific information, contact Yealink technical support.

Procedure

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

2. Add a meeting room.

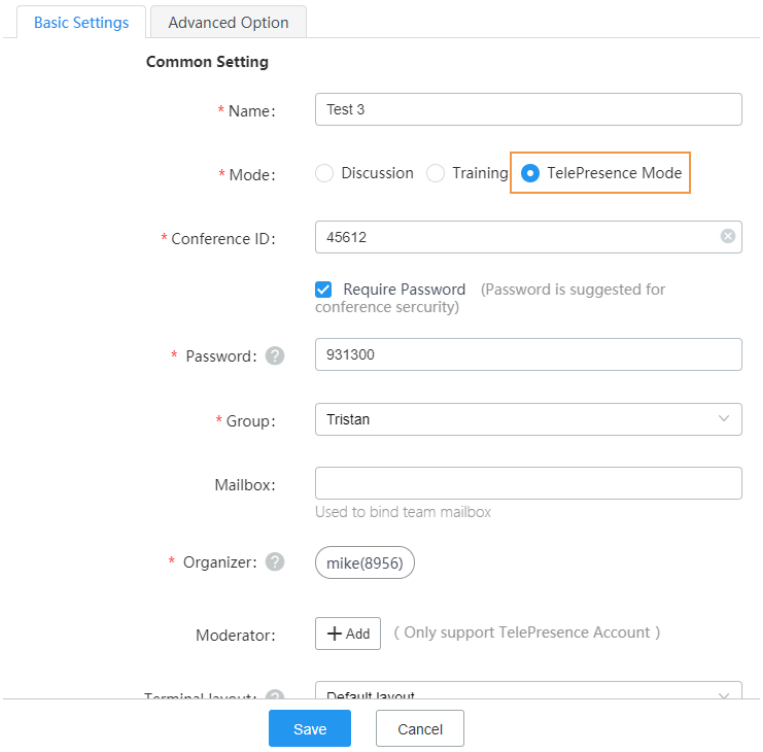
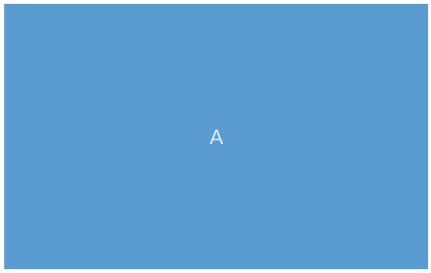
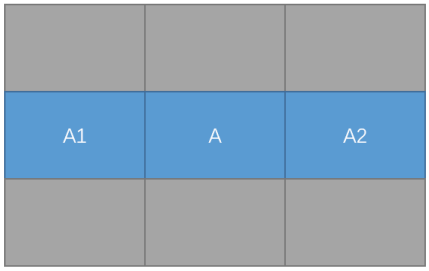


Table 40: Parameter Introduction

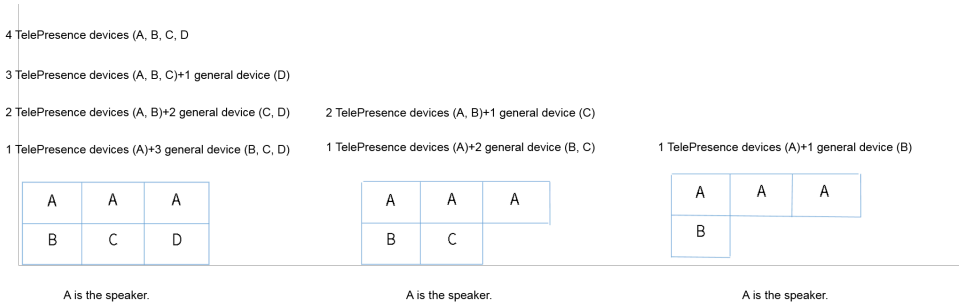
Parameter	Description
Terminal layout	Set the layout displayed on the general devices as default layout or three screen layout. • Default layout If the speaker is the participant using TelePresence device, participants using general devices can see the middle screen of the speaker like below:  • Three screen layout If the speaker is the participant using TelePresence device, participants using general devices can see three screens of the speaker like below:  **Note:** If the speaker is the participant using general devices, participants using general devices can see the speaker as their large video images.
Screen polling settings	Enable or disable it.
Polling time setting	Set the time from 5 to 60 seconds.

Introduction of the TelePresence Recording

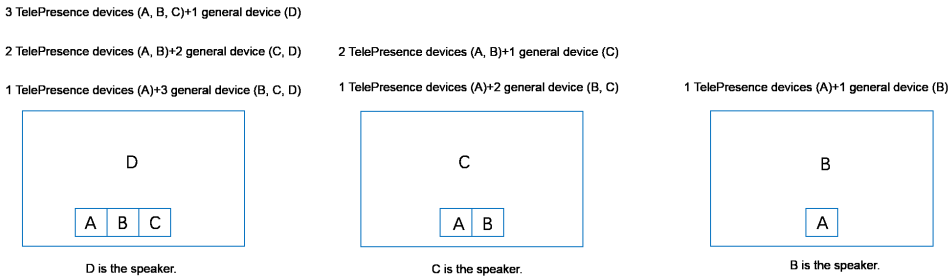
The process of enabling TelePresence recording is similar to the one of conference recording, you can refer to Yealink Recording Service. Here are some differences:

- The TelePresence accounts are associated with the TelePresence template by default and this association cannot be modified.
- You cannot configure the layout of the TelePresence template.
- When there is no shared content, the recording layout is as below:
  - If the speaker (the voice-activated feature is enabled and the voice-activated time is 2 seconds) is a participant using the TelePresence device, you can see the left, the right, and the middle screens of

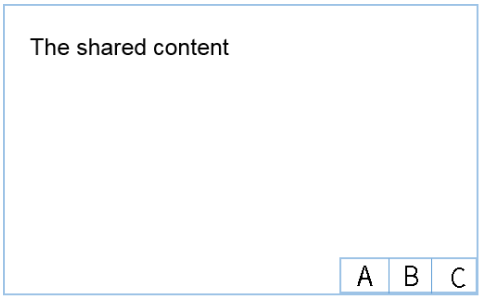
the speaker displayed in three video images respectively. For other participants using TelePresence devices, you can only see the middle screens of their devices.



- If the speaker (the voice-activated feature is enabled and the voice-activated time is 2 seconds) is a participant using the general device, you can see the speaker as your large video image. For other participants using TelePresence devices, you can only see the middle screens of their devices in thumbnails in picture-in-picture mode.



- When there is shared content, the recording layout is as below:
  - Only display the shared content and the speaker (the voice-activated feature is enabled and the voice-activated time is 2 seconds). You can see the shared content as your large video image and the video image of the speaker is reduced to a thumbnail in picture-in-picture mode. If the speaker is a participant using the TelePresence device, you can see his video image reduced to three thumbnails in picture-in-picture mode. If the speaker is a participant using the general device, you can see his video image reduced to a thumbnail in picture-in-picture mode.



Controlling Conferences

You can control the Telepresence conference to realize the desired effect.

- Going to the Conference Control page
- Muting/Unmuting Participants
- Turning on/off the Video Image
- Removing Participants
- Viewing Call Statistics

- Switching the Roles Between the Moderators and Guests
- Controlling the Remote Camera
- Blocking/Unblocking Audio
- Editing the Site Name
- Inviting Contacts
- Inviting Other Participants
- Inviting Participants by Email
- Sharing the Conference Information
- Searching for Participants
- Moving Participants to the Lobby
- Recording Conferences
- Setting Smart Check-in
- Pausing/Stopping the Recording
- Leaving/Ending a Conference
- Conference Settings

Going to the Conference Control page

Procedure

1. Click **Conference** > **Conference Control** > **VMR**.
2. On the right side of the desired Telepresence conference, click to go to the Conference Control page.

Muting/Unmuting Participants

You can mute or unmute a participant to control whether or not other participants can hear this participant's voice.

Before you begin

Going to the Conference Control page

Procedure

Do one of the following:

- If you want to mute/unmute a participant, select the desired participant and then click / .
- If you want to mute/unmute some participants, select them and then click / .
- If you want to mute/unmute all participants, click / in the **Global Operation** field.

Turning on/off the Video Image

You can turn on/off the video image of a participant to control whether or not other participants can see the video image of this participant.

Before you begin

Going to the Conference Control page

Procedure

Do one of the following:

- If you want to turn on/off the video image of a participant, click / .
- If you want to turn on/off the video images of some participants, click / .

Removing Participants

You can remove participants.

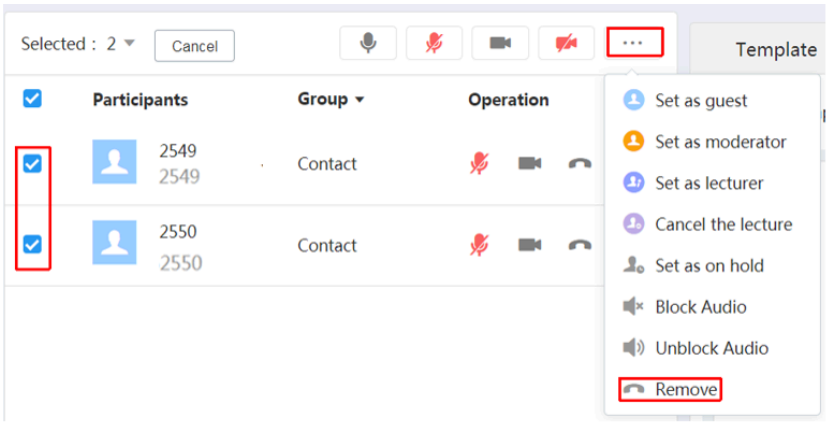
Before you begin

Going to the Conference Control page

Procedure

Do one of the following:

- If you want to remove a participant, click on the right side of the desired participant.
- If you want to remove some participants, select them and click on the top of the page, then select **Remove** from the drop-down menu.



Viewing Call Statistics

During the conference, if the call quality is poor, you can see the call statistics of every participant to find out the reason. Call statistics covers the statistics about the audio, the video, the content and so on. You can know the call quality by checking the codec, the bandwidth, the packets loss and so on. For example, when the call has a delay or there is a mosaic in the video, you can check the package lost rate.

Before you begin

Going to the Conference Control page

Procedure

Do one of the following:

- Click **Call Statistic** in the top-right corner and click the desired participant to view details.
- Select the desired participant, click on the top of the page, and select **Call Statistics** from the drop-down menu.

Switching the Roles Between the Moderators and Guests

You can set a guest as a moderator. If the participant does not want to be a moderator anymore, you can cancel his role as a moderator. The participant using general devices cannot be set as a moderator.

Before you begin

Going to the Conference Control page

Procedure

Do one of the following:

- If you want to set a single participant as the moderator/guest, click ··· on the right side of the desired participant, and select **Set as moderator**/**Set as guest** from the drop-down menu.
- If you want to set several participants as moderators/guests, select them, click ··· on the top, and then select **Set as moderator**/**Set as guest** from the drop-down menu.

Controlling the Remote Camera

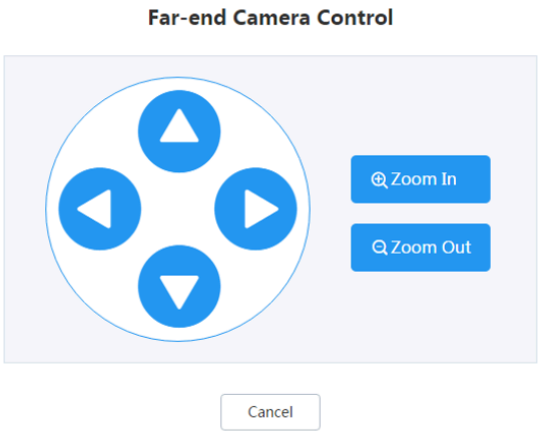
You can control the camera of the participant, including turn it up/down/left/right, zoom it in/out.

Before you begin

- Going to the Conference Control page.
- The devices of conference participants support FECC (Far End Camera Control) feature.

Procedure

1. Click ··· beside the desired participants, and select FECC from the drop-down menu.
2. In the pop-up dialogue, do the corresponding operations:



Blocking/Unblocking Audio

You can block/unblock the audio of a participant to control whether or not this participant can hear the voice of other participants.

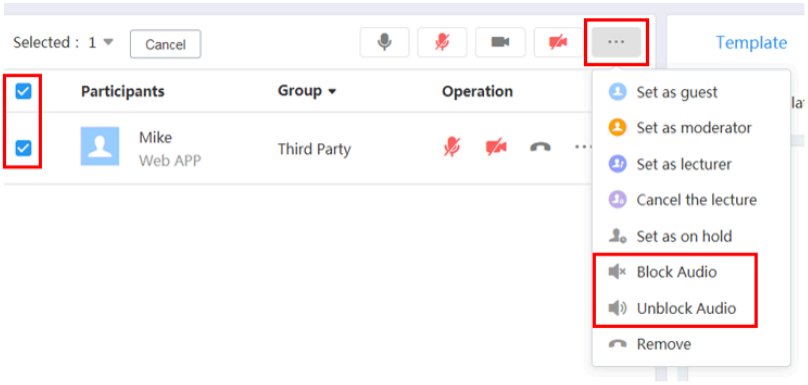
Before you begin

Going to the Conference Control page

Procedure

Do one of the following:

- If you want to block the audio of a single participant, click ··· on the right side of the desired participant, and select **Block Audio/Unblock Audio** from the drop-down menu.
- If you want to block the audio of some participants, select them, click ···, and then select **Block Audio/Unblock Audio** from the drop-down menu.



Editing the Site Name

The you can edit the site name of the participant. Especially, those participants do not have YMS accounts and might join the conference by IP call, browser, VCD, or VCM.

Before you begin

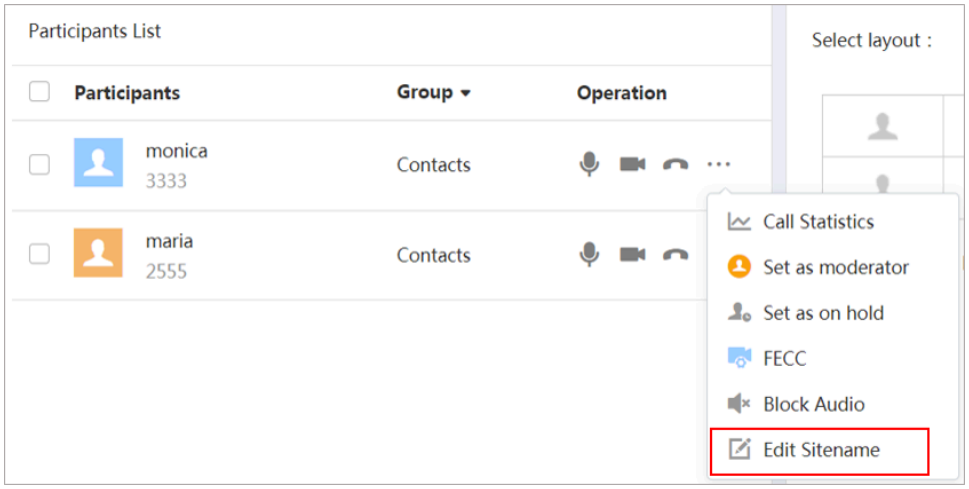
Going to the Conference Control page

About this task

After editing, the new site name will be displayed in the Participant List, in the MCU image, and in the prompts when the participant applies for speaking or leaves the conference. Editing the site name is valid only at this time you join the conference, when the next time you join the conference, your site name will return to the default one. Editing the site name has no influence on the original name.

Procedure

Click ··· beside the desired participants, and select **Edit Sitename** the drop-down menu.



Inviting Contacts

You can place a call to the desired contact in the enterprise directory directly.

Before you begin

Going to the Conference Control page

Procedure

1. In the top-right corner of the page, click **Invite**.
2. Select **Invite Contacts**.
3. Select the desired contact in the enterprise directory.
4. Click **OK**.

Inviting Other Participants

You can use the H.323, SIP, RTSP to invite participants.

Before you begin

- Going to the Conference Control page
- When using RTSP, make sure you have configured Configuring the RTSP Gateway Service

Procedure

1. In the top-right corner of the page, click **Invite**.
2. Click **Invite Others**.
3. Select the desired call protocol from the drop-down menu of **Protocol** and enter the address or number.
4. If you select H.323 or SIP, you can also select the call bandwidth.
   The default value is the one you set in global setting, refer to Setting the Call Bandwidth.
5. Click **Call**.

Inviting Participants by Email

You can use the system mailbox to send emails to invite participants.

Before you begin

- Going to the Conference Control page
- Configuring the SMTP Mailbox

Procedure

1. In the top-right corner of the page, click **Invite**.
2. Click **Email Invitation**.
3. Click **System mailbox**.
4. Edit the email, and click **Send**.

Sharing the Conference Information

You can invite conference participants by sharing conference information with others.

Before you begin

Going to the Conference Control page

Procedure

1. In the top-right corner of the page, click **Invite**.
2. Click **Email Invitation**.
3. Click **Copy invitation information**, paste the information and send it to the participants you want to invite.

Searching for Participants

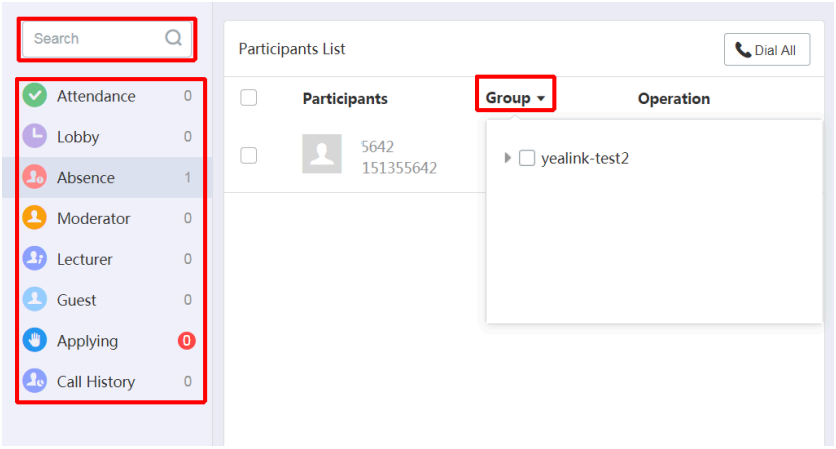
You can search for participants.

Before you begin

Going to the Conference Control page

Procedure

1. Enter the participant name or the account number in the **Search** box to perform the search.
2. Select the participant type below the **Search** box, and the search result will be displayed in the Participant list.
3. Select the desired group from the drop-menu of **Group**, and the participants of this group will be displayed in the Participant list.



Moving Participants to the Lobby

In order to keep the conference order, you can move the participant who has attended the conference to the lobby.

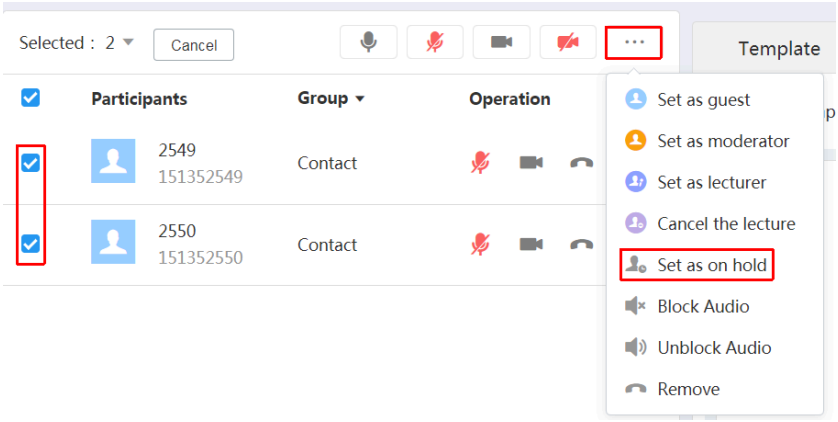
Before you begin

Going to the Conference Control page

Procedure

Do one of the following:

- If you want to move a single participant to the lobby, click ··· beside the desired participant and select **Set as on hold** from the drop-down menu.
- If you want to move several participants to the lobby, select them, click ··· at the top, and select **Set as on hold** from the drop-down menu.



Recording Conferences

Before you begin

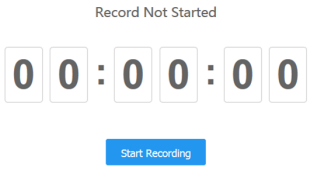
- Going to the Conference Control page
- You have enabled the recording service, refer to Yealink Recording Service

About this task

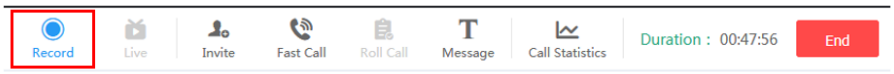
Note: In the same video conference, while a participant is recording, other participants cannot record the conference.

Procedure

1. In the top-right corner of page, click **Record**.
2. Click **Start Recording.**



The page is shown as below:



Setting Smart Check-in

If you enable the face recognition service, you can use this feature.

Before you begin

- Going to the Conference Control page
- You have enabled the face recognition service, refer to Face Recognition Service

Procedure

1. In the top-right corner of page, click **Smart Check-in**.
2. If you want to add participants for smart check-in, click **Edit member**, select the desired participants, and click **Save**.
3. Set the check-in time limit.
4. Click **Sign in** > **Start**.
5. To manually end the smart check-in, click **End**. Also, YMS can automatically end the smart check-in when the time you set is over.

   The attendance result will be displayed on the page.

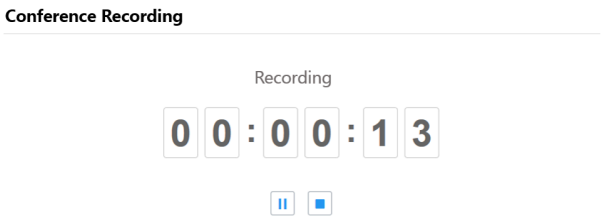
Pausing/Stopping the Recording

Before you begin

Going to the Conference Control page

Procedure

1. In the top-right corner of page, click **Record**.
2. In the pop-up window, click  to pause the recording or click  to stop the recording.



Leaving/Ending a Conference

You can leave or to end a conference.

Before you begin

Going to the Conference Control page

Procedure

1. In the top-right corner of the page, click **End**.
2. Select **End conference** or **Leave, others keep going**.

Conference Settings

Before you begin

Going to the Conference Control page

Procedure

1. In the top-right corner of page, set the following parameters:

   Table 41: Parameter Introduction

Parameter	Description
Play sound when participants join or leave	Enable or disable voice prompt when when participants join or leave the conference. After you enable it, whether or not the participant can hear the voice prompt depends on the one you set in global setting, refer to Setting the Audio Prompt When Participants Join or Leave Conferences.
Electronic nameplate	If you enable it, YMS can automatically recognize the participant face and display the participant name. You can set the frame color. **Note:** For managing face pictures, refer to Registering Faces. If participants whose faces cannot be found in the face database or be identified by YMS, they are called guests. YMS can recognize up to 50 electronic nameplates (The number depend on your YMS performance).
Details of speaker	If you enable it, YMS can automatically present a brief introduction of the participant. **Note:** For more details, refer to Registering Faces. According to the order of recognizing the participant face, YMS can present the brief introductions of the first 3 recognized participants at most.
Real-time subtitles	Enable or disable the subtitle to be displayed on the video image. **Note:** Default: disabled. This configuration appears only when you enable the subtitle on Adding a VMR.

2. Click **Apply**.

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

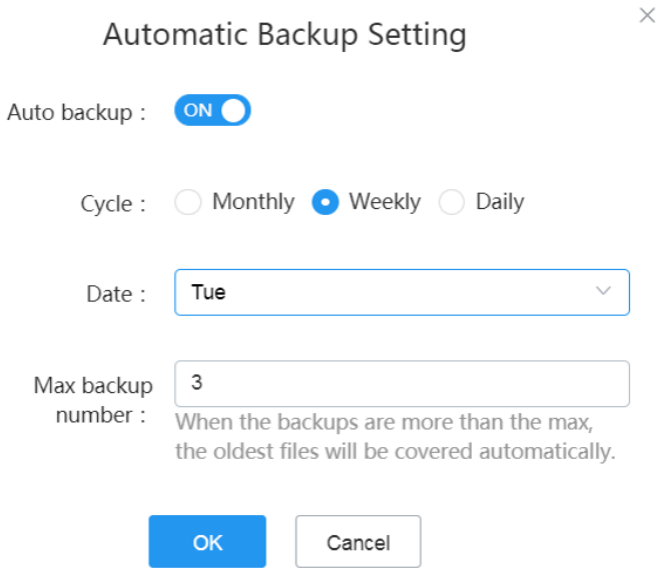
When there is sufficient space for backups, you can make backups for the server data, including the user accounts and the conference information.

- 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.



Creating a Backup Manually

Procedure

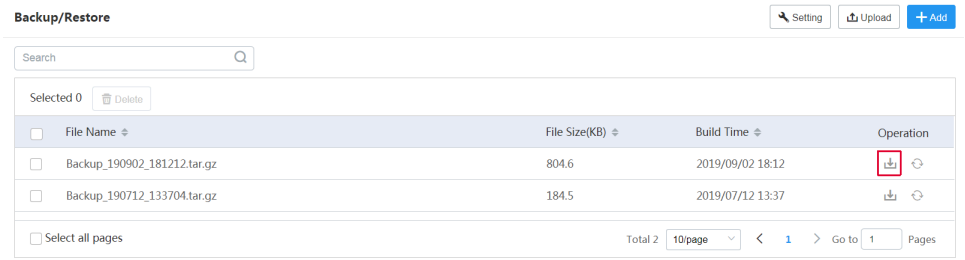
1. Click **Maintenance** > **Backup/Restore** > **Add**.
2. Enter the file name and save the configuration.

Downloading a Backup

Procedure

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

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



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 BackuporCreating 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.

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.

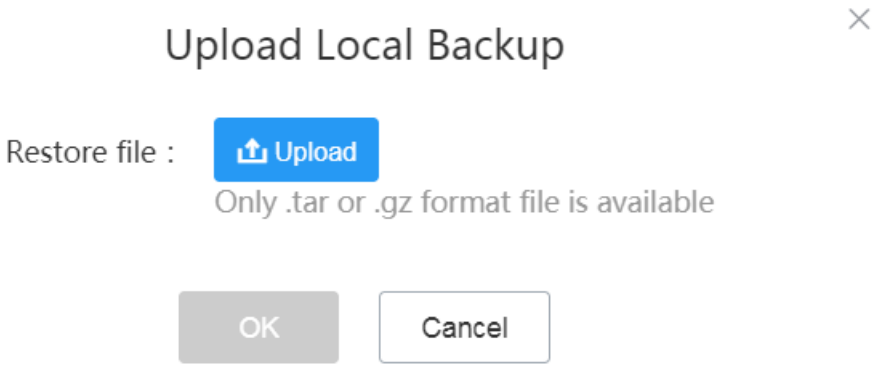
Before you begin

Downloading a Backup

Procedure

1. Click **Maintenance** > **Backup/Restore** > **Upload**.

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



3. 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

1. Click **Maintenance** > **System Restart**.
2. Select a node and reboot the node.

Resetting to the Factory

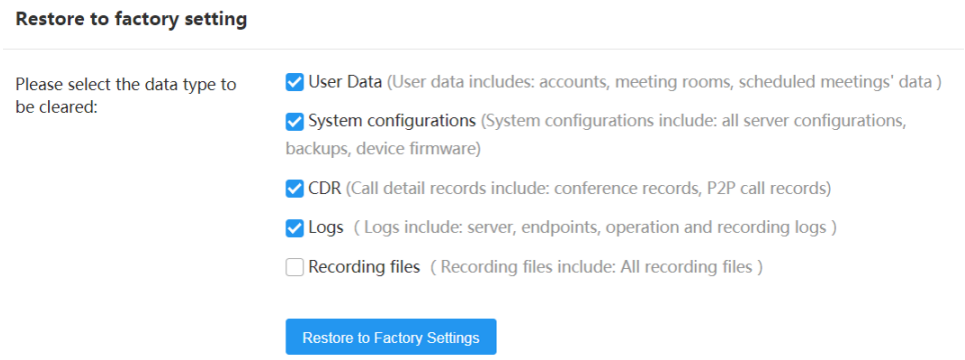
In some situations, you might need to clear up the entire user data, the system configuration, the call records, the logs, and the recording files to solve the problem that occurred to the YMS.

Procedure

1. Click **Maintenance** > **Restore to factory setting**.

2. Select the data type, and reset the server to the factory.

   If you choose to clear up the system configuration, some customization settings might be saved. For example, the web and conference theme, the email template, SIP trunk IVR, the audio IVR, DTMF, the watermark on the recording setting, and others.

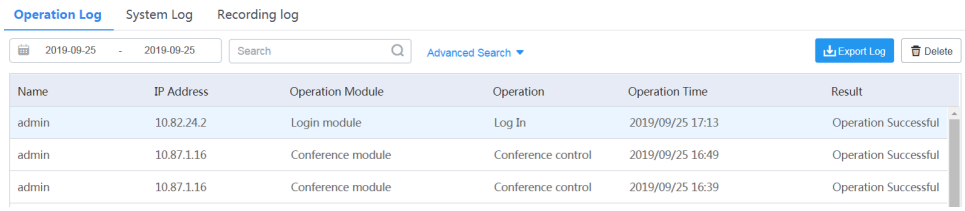


Viewing Operation Logs

The operation log keeps a record of the changes, including the visit record and the configuration record.

Procedure

Click **Maintenance** > **Operation Log** > **Operation Log**.



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

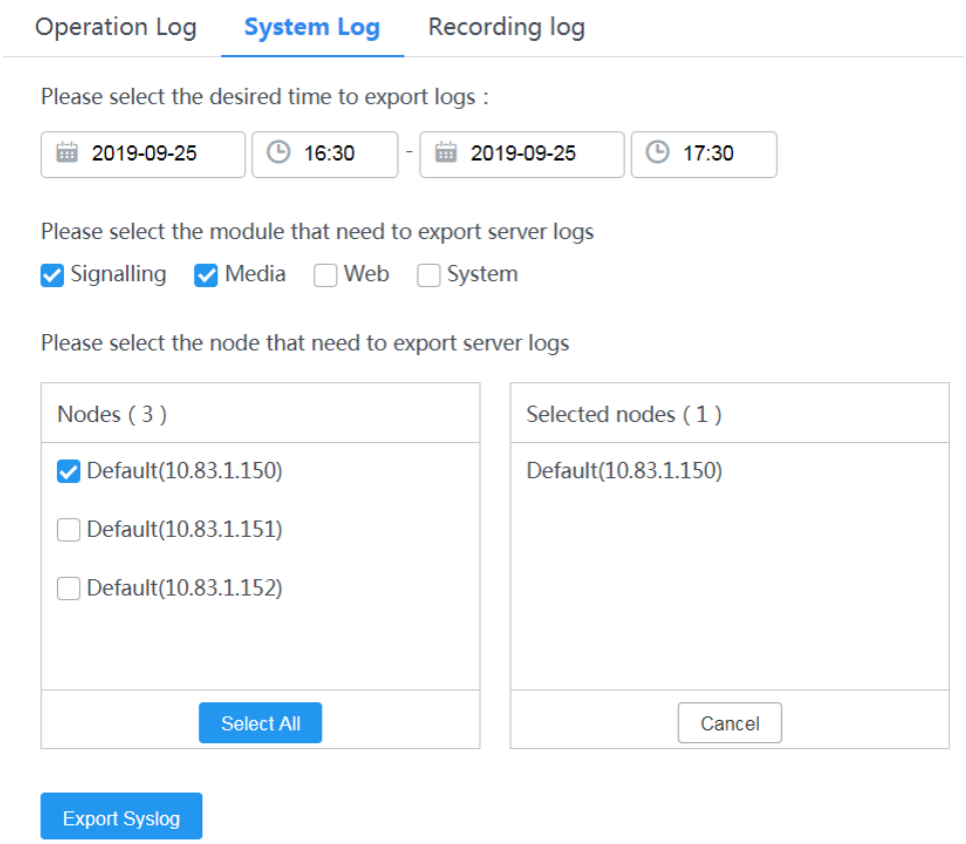
Exporting System Logs

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.



3. Click **Export Syslog**.

Using Tools

Ping and packetcapture are available on YMS to test the network.

- Pinging the Network
- Capturing Packets

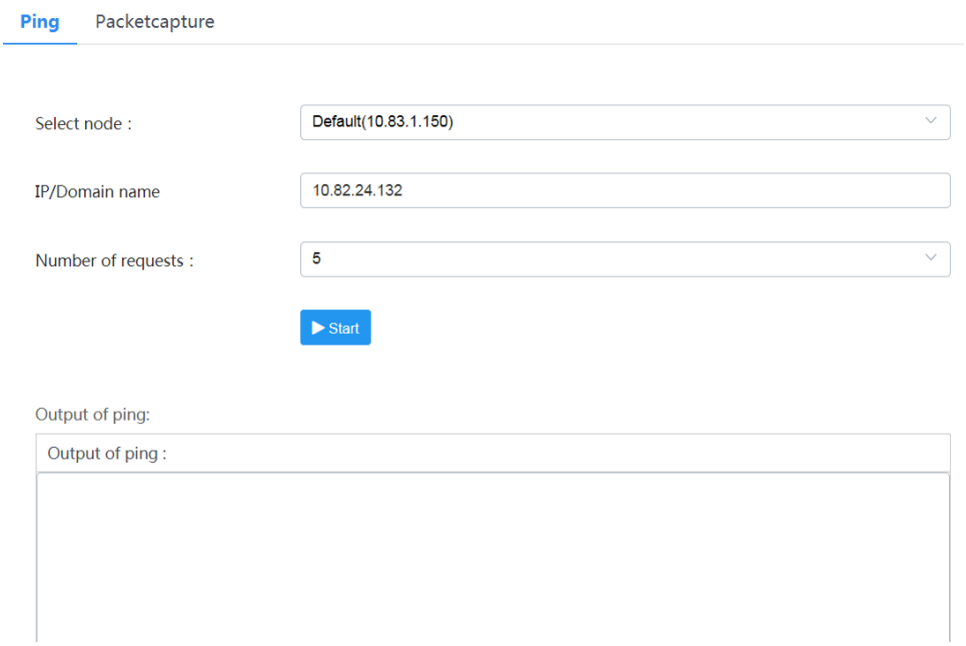
Pinging the Network

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**.



Capturing Packets

You can capture packets to analyze the network traffic sent or received by the nodes.

About this task

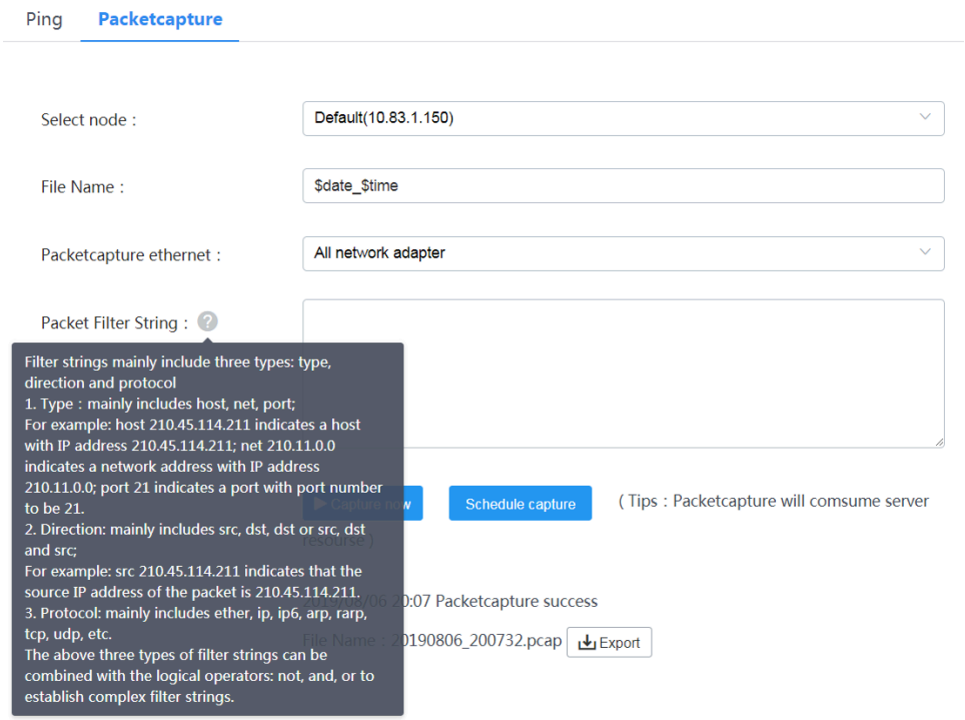
If you encounter problems when using YMS, Yealink technical support engineers will solve the problem with the packets you captured.

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**.



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.

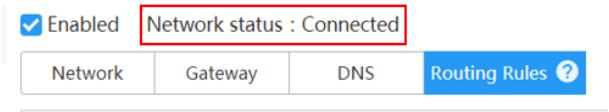
Cause:

- 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**.