Yealink Meeting Server
Administrator Guide V21.0.0.10

Contents

About This Guide..... 7
Targeted Audience..... 7
Related Documents..... 7
Introduction of Yealink Meeting Server..... 8
Introduction of the Deployment Structure..... 8
Basic Concepts..... 8
Browser Requirement..... 9
Router Port Requirements..... 9
Icons Introduction..... 10
In This Guide..... 11
Summary of Changes..... 11
Changes for Release 21, Guide Version 21.0.0.10..... 11

Basic Operations of the Enterprise Administrator..... 12
Logging into YMS..... 12
Setting the Setup Wizard..... 12
Introduction of the Home Page..... 13
Account Management..... 14
Editing the Login Password..... 14
Editing the Registered Email..... 14
Logging out of YMS..... 14

System Setting..... 14
Setting the Primary Domain Name..... 15
Setting the Web Service Address..... 16
Setting the Log Service Address..... 16
Configuring the Port..... 17
Configuring the Time..... 17
Setting the Data Space..... 18
Configuring the SMTP Mailbox..... 19
Allocating the Number Resource..... 19
Configuring the Node..... 20
Viewing the Node Information..... 21
Configuring the Address Port Mapping..... 21
Setting the IP Property..... 21
Adding a Sub Admin Account..... 22
Editing the Information of a Sub Admin Account..... 22
Delete the Abnormal IP..... 22
Adding a Security Group..... 23
Configuring Intelligent Security Strategy..... 23
Applying for the Accesskey..... 24
Adding the User-Agent Blacklist..... 24
Adding the User-Agent Compatible List..... 25
Activating a License..... 26
Importing the Server Device License..... 26
Activating a License Online..... 27
Activating a License Offline..... 27

Disassociating the License....28
Importing the Trusted CA Certificate....28
Importing the HTTPS Certificate....28
Importing the TLS Certificate....28
Setting the Display on the Web Page....29
Configuring the Email Template....34
Configuring SIP Trunk IVR....35
Configuring the Audio IVR....35

Service Management....35

Configuring the Registration Service....36
Communicating with Other Devices via IP Call....37
Configuring the IP Call Service....37
Setting the Redirect Service....39
Configuring the Third Party REG Service....40
Communicating with PSTN....41
Configuring the PSTN Gateway Service....42
Setting the Peer Trunk Service....44
Configuring the REG Trunk Service....46
Communicating with Skype for Business Server....48
Communicating with the Local SfB Server....49
Communicating with Microsoft Office 365....52
Communicating with Other Enterprise SfB Servers....55
Configuring the SFB Service....60
Configuring the SfB Gateway Media Service....64
Configuring the GK Service....65
Configuring the H.323 Gateway....67
Configuring the Interactive Media Service....69
Configuring the Broadcast Media Service....70
Configuring the RTMP Media Service....71
Configuring the Media Bypass Service....71
Adding the Recording Service....72
Configuring the Traversal Service....73

Call Settings....74

Call Control Policy....74
Setting the Video and the Content Resolution....75
Configuring the Call Bandwidth....75
Configuring the Max Video Parties per Conference....75
Configuring the Max Audio-Only Parties per Conference....76
Setting IVR language....76
Configuring the Time for Joining Conference Beforehand....76
Enabling Auto Dialing....76
Enabling the Auto Redialing....77
Enabling Play Sound When Participants Join....77
Displaying the Native Video....77
Setting the Last Participant Backstop Timeout....77
Setting the Auto End Conference Without Moderator....78
Enabling the Content Only....78
Enabling Join with APP Awakened by Browser....78
Enabling Receiving Ringtone Receipt....79
Enabling External/Internal Network Access WebRTC Authentication....79
Disabling the Roll Call Setting....79
Configuring the iOS Push Address....79

Enabling the Broadcasting Interactive....80
Configuring the RTMP Live.... 80
Enabling the Conference Recording....81
Setting the QoS....81
Video Display Policy....81
Setting the Default Layout.... 82
Setting Video Layout of 1+N....82
Setting the Video Layout of Equal N×N.... 83
Display participant name....83
Display Participant Status....83
Displaying the Participant Quantity.... 84
Displaying the Audio-Only Participant....84
Restricting the Dialed Number....84
Add a Number Filter.... 84
Call Routing Rule....85
Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings....86
Adding a Call Routing Rule....87
Configuring the Call Routing Rule.... 89

Managing the Recording....89
Showing the Recording Icon During Recording....90
Parameters of the Recording Template.... 90
Editing the Default Recording Template....90
Adding the Recording Template....91
Viewing the Application Object of the Recording Template....91
Deleting the Recording Template....91
Viewing the Usage....91
Editing the Recording Parameters of User Account....92
Managing the Recording Files.... 92
Deleting Recording Files....92
Copying the Sharing Link.... 93
Disabling the Sharing Link.... 93

Managing Accounts.... 93
User Accounts, Room System Accounts and Other Accounts.... 94
Managing Groups....94
Adding a Group.... 94
Editing/Deleting the Group.... 94
Adding Accounts.... 95
Parameters of User Account....95
Parameters of Room System Account.... 97
Parameters of Other Devices....100
Adding an Account Manually.... 100
Adding a Batch of Accounts....100
Sending an Email to a YMS Account.... 101
Adjusting the Account Group.... 101
Editing the Authority....101
Editing the GK Registration Parameter....102
Editing a Batch of Accounts.... 102
Configuring the LDAP.... 102

Managing Meeting Rooms.... 105
The Entity Meeting Room and the Virtual Meeting Room.... 106

Managing Groups of Meeting Room.....106
Adding Groups of Meeting Room.....106
Editing/Deleting the Meeting Room Group.....106
Adding a General Meeting Room.....107
Adding a Video Meeting Room.....107
Discussion Mode and Training Mode.....108
Adding a VMR.....109
Adjusting the Meeting Room Group.....113
Sending Emails About Joining the Conference.....114

Managing Conferences.....114
Viewing the Conference.....114
Viewing the Meeting Room Usage.....114
Monitoring the Conference.....115
Going to the Conference Monitoring Page.....115
Adjusting the Output Volume.....115
Selecting an Audio Output Device.....116
Changing the Display Language.....116
Configure the Video Images in Equal N×N.....116
Setting the Video Carousel.....117
Displaying a Participant in a Full Screen/Exiting the Full Screen.....117
Scaling the Video Image.....117
Changing Video Layouts.....117
Displaying the Conference Monitoring Page in a Full Screen/Exiting the Full Screen.....118
Deleting a Conference.....118
Controlling the Conference.....119

Conference Statistics.....119
Viewing the MCU Resource.....119
Viewing the Conference Statistics.....120
Viewing the Call History.....120

System Maintenance.....120
Viewing the System Version.....121
Upgrading the System.....121
Enabling the Device Upgrade.....121
Adding the Firmware.....122
Updating the Firmware.....122
Setting the Auto Backup.....122
Creating a Backup Manually.....122
Downloading a Backup.....123
Backup/Restore.....123
Restoring a backup by Selecting a Backup Directly.....123
Restoring a backup by Uploading a Backup.....123
Rebooting the System.....123
Resetting to Factory.....124
Viewing the Operation Log.....124
Viewing the System Log.....124
Viewing the Device Log.....124
Viewing the Recording Log.....125

Troubleshooting.....125

Users Do Not Receive Emails.....125
User Fail to register an Account.....126
Failing to Activating a License Online.....126
Failing to Activating a License Offline.....127
Loading the Orgainzation Structure Slowly.....127

About This Guide

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

- *Targeted Audience*
- *Related Documents*
- *Introduction of Yealink Meeting Server*
- *Introduction of the Deployment Structure*
- *Basic Concepts*
- *Browser Requirement*
- *Router Port Requirements*
- *Icons Introduction*
- *In This Guide*
- *Summary of Changes*

Targeted Audience

This guide is mainly intended for the following audiences.

- The distributors
- The network administrators

Related Documents

Apart from Yealink Meeting Server Admin Guide, we also provide the following documents:

- Yealink Meeting Server User Guide: it introduces how to use the common features of YMS.
- Yealink Meeting Server Web App User Guide for PC: it introduces how to use the browser on PC to join to conferences.
- Yealink Meeting Server Web App User Guide for Mobile: it introduces how to use the browser on the mobile phone to join to conferences.
- Yealink Meeting Server Network Deployment Guide: it introduces how to deploy and configure YMS.
- Yealink Meeting Server Installation Guide: it introduces how to install YMS software.
- Yealink Meeting Server RTMP Configuration Guide: it introduces how to configure RTMP on YMS, so that you can stream the conference to the live streaming platform.
- You Tube Streaming Guide: it introduces how to stream the conference to You Tube by RTMP, so that the You Tube user can watch the live broadcast of the conference.
- Yealink Meeting Server and Skype for Business Deployment Guide: it introduces how to make the YMS to communicate with Skype for Business server.
- 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, and how YMS synchronize the data and manage data from the federation management platform.

  Read the *Yealink Products Regulatory Notices guide* for all regulatory and safety guidance.

Introduction of Yealink Meeting Server

Yealink Meeting Server (YMS) is a distributed cloud-based videoconferencing infrastructure tailored for HD video conferencing collaboration in the modern workplace. As a powerful all-in-one meeting server, YMS brings MCU, the registrar server, the directory server, the traversal server, the meeting and device management server, SIP Trunk, WebRTC server and GK & H.460 server together, to better provide users with an enjoyable conferencing experience while cutting costs and improving efficiency. Seamlessly working with multiple devices such as room systems, video phones, mobile apps and PC software, YMS brings people together at any time from any location with the touch of a button.

Introduction of the Deployment Structure

YMS deployment structure can be divided into the standard version and the enterprise version, also called the single version and the cluster version.

Table 1: The Differences Between the single Version and the Cluster Version

Type	Difference
Single Version	A single YMS but containing all service.
Cluster Version	Multiple YMSs and contains the following node types: • **Master node**: it contains all YMS service. • **Sub-master node:** it should contain 2 sub-master node to realize the disaster recovery function for all the features. • **Service node**: you can deploy the service in each service node according to the enterprise deployment plan. The service contains SIP service, MCU service and so on.

Basic Concepts

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

Enterprise Directory: it refers to the directory which includes the user accounts, the room system accounts and other accounts.

Yealink VC devices: this concept refers to the endpoints that support YMS, including PVT950/PVT980, VC880/VC800/VC500/VC200/VC400/VC120/VC200 video conferencing system, CP960 conference phone, SIP VP-T49G IP phone, SIP-T58V IP phone, 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: Yealink Meeting Server in stand-alone or the cluster version.

Browser Requirement

YMS supports the following browsers.

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

Router Port Requirements

If the following ports are restricted in your network environment, please open these ports. If the YMS is deployed in an Intranet, you can solve the interconnection problem between the private and public network by mapping the following ports to the public network on the router.

Requirements of the internal service port: make sure that the following ports in every node of the cluster can communicate with each other.

Port	UDP/TCP	Description
8000-9999	UDP+TCP	Internal service port.
27017	UDP+TCP	The port for accessing the database.
22	TCP	Install or upgrade the server via ssh.

Table 2: Requirements of the external service port

Module	Port	UDP/TCP	Description
Web port	443	TCP	HTTPS port.
	444	TCP	After the HTTPS certificate of the Web is replaced by YMS, YMS still can be trusted by Yealink devices.
	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/TCP	RAS listening port of the GK.
	1720	UDP/TCP	H.225 listening port of the Gateway.
	1722	UDP/TCP	H.225 listening port of the GK.

Module	Port	UDP/TCP	Description
Turnserver port	3478	UDP/TCP	The listening port of the traversal service.
	3479	UDP/TCP	Backup listening port.
	9688	UDP/TCP	As long as the IP address exists, this port should be mapped, because it might influence the traversal service.
SIP port	5060	UDP/TCP	It is used for IP call service.
	5061	UDP/TCP	It is used for registration service.
	5062-5070	UDP/TCP	It is used for third-party registration service, PSTN gateway service, peer trunk service, registration trunk service and Skype for business service.
Media port	10000-65535	UDP/TCP	It is used for MCU service, IVR, BFCP/FECC, conference stack signaling, the conference stack media, the traversal service (UDP is compulsory but TCP is optional).

Icons Introduction

The icons on Yealink Meeting Server is introduced as below.

Table 3:

Icon	Description
	Recurrence conference
	RTMP live conference
	General meeting room (displayed on the Meeting Room Usage page)
	Video meeting room (displayed on the Meeting Room Usage page)

In This Guide

This guide contains the following chapters.

- Chapter 1 *Basic Operations of the Enterprise Administrator*
- Chapter 2 *System Setting*
- Chapter 3 *Service Management*
- Chapter 4 *Call Settings*
- Chapter 5 *Managing the Recording*
- Chapter 6 *Managing Accounts*
- Chapter 7 *Managing Meeting Rooms*
- Chapter 8 *Managing Conferences*
- Chapter 9 *Conference Statistics*
- Chapter 10 *System Maintenance*
- Chapter 11 *Troubleshooting*

Summary of Changes

- *Changes for Release 21, Guide Version 21.0.0.10*

Changes for Release 21, Guide Version 21.0.0.10

The following sections are new for this version:

- *Loading the Orgainzation Structure Slowly*
- *Displaying the Audio-Only Participant*
- *Enabling Receiving Ringtone Receipt*
- *Enabling Join with APP Awakened by Browser*
- *Monitoring the Conference*
- *Adding the Recording Service*
- *Managing the Recording*
- *Viewing the Recording Log*
- *Resetting to Factory*

Major updates have occurred to the following sections:

- *Adding a Sub Admin Account*
- *Editing the Information of a Sub Admin Account*
- *Adding a VMR*
- *Adding Accounts*
- *Setting the Display on the Web Page*
- *Introduction of the Home Page*
- *Configuring the IP Call Service*
- *Configuring the PSTN Gateway Service*
- *Setting the Peer Trunk Service*
- *Configuring the REG Trunk Service*
- *Configuring the GK Service*
- *Configuring the H.323 Gateway*

Basic Operations of the Enterprise Administrator

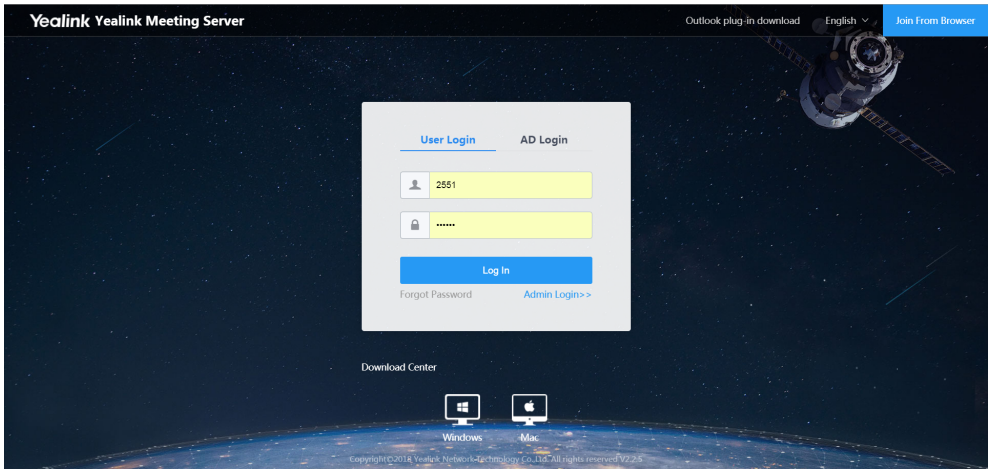
This guide provides instructions for the enterprise administrator to use YMS.

- *Logging into YMS*
- *Setting the Setup Wizard*
- *Introduction of the Home Page*
- *Account Management*
- *Logging out of YMS*

Logging into YMS

Procedure

1. Open a web browser.
2. Enter the IP address or the domain name of YMS in the address bar to go to the Login page of YMS.
3. Click **Admin Login**.
4. Enter the username and the password of the admin account.



Note: By default, the username is “admin” and the password is “123456”.

5. Optional: Select a language from the drop-down menu of **Language**.
6. Click **Log In**.

Note: If you forget the password, click **Forgot Password** and reset the password according to prompts.

Setting the Setup Wizard

To meet the basic call usage, you can go to the Setup Wizard to configure the server.

About this task

When you log into YMS for the first time, the Setup Wizard will pop up.

Procedure

1. Click **Setup Wizard** in the top-right corner.
2. *Setting the Primary Domain Name* .
3. *Editing the Login Password* .
4. *Configuring the Time* .
5. *Configuring the SMTP Mailbox* .
6. *Configuring the Node* .
7. *Configuring the Registration Service* .
8. *Configuring the Traversal Service* .
9. *Configuring the Interactive Media Service* .
10. *Activating a License* .

Introduction of the Home Page

To familiarize yourself with various operation interfaces and system notifications, you can know the layout of home page. YMS supports the management of different permissions. The system administrator has the highest operation permission on YMS. Accounts with different permissions will see different Home pages, and this part takes the Home page viewed by the system administrator account as an example.

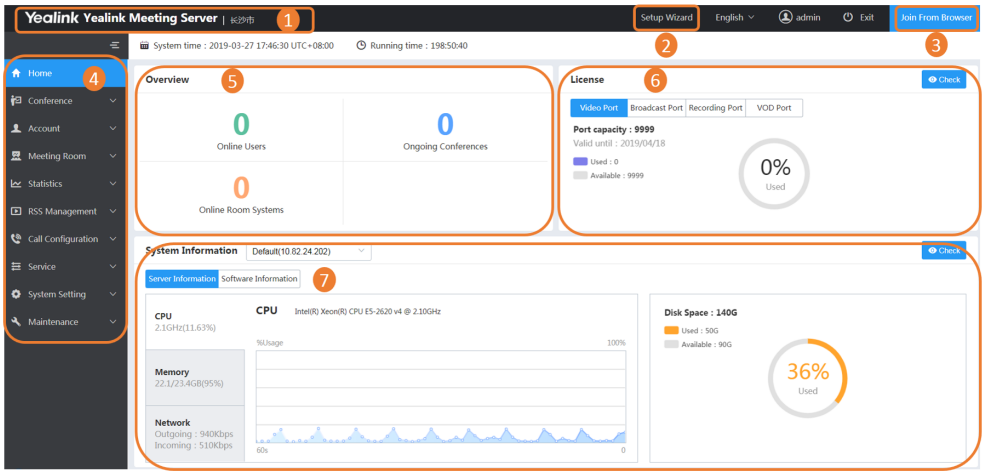


Table 4:

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. • View the server CPU, the memory, the network, and the disk space. • View the information of the software version.

Account Management

- *Editing the Login Password*
- *Editing the Registered Email*

Editing the Login Password

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

Procedure

1. Click the account name in the top-right corner.
2. In **Password** field, click **Change**.
3. Enter the current password, and enter the new password twice.
4. Click **OK**.

Editing the Registered Email

You can edit the registered email. This email is used to receive the information of resetting password and the system alarm when an error occurs to the system.

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**.
3. Enter the new email address.
4. Click **OK**.

Logging out of YMS

If you want to use other accounts to log into YMS, you can log out of the current account first.

Procedure

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

System Setting

- *Setting the Primary Domain Name*

- *Setting the Web Service Address*
- *Setting the Log Service Address*
- *Configuring the Port*
- *Configuring the Time*
- *Setting the Data Space*
- *Configuring the SMTP Mailbox*
- *Allocating the Number Resource*
- *Configuring the Node*
- *Viewing the Node Information*
- *Configuring the Address Port Mapping*
- *Setting the IP Property*
- *Adding a Sub Admin Account*
- *Editing the Information of a Sub Admin Account*
- *Delete the Abnormal IP*
- *Adding a Security Group*
- *Configuring Intelligent Security Strategy*
- *Applying for the Accesskey*
- *Adding the User-Agent Blacklist*
- *Adding the User-Agent Compatible List*
- *Activating a License*
- *Disassociating the License*
- *Importing the Trusted CA Certificate*
- *Importing the HTTPS Certificate*
- *Importing the TLS Certificate*
- *Setting the Display on the Web Page*
- *Configuring the Email Template*
- *Configuring SIP Trunk IVR*
- *Configuring the Audio IVR*

Setting the Primary Domain Name

You can configure the domain name for authentication. When the device is registering, the server address will be directed to this domain name.

Procedure

1. Click **System Settings** > **Common Settings** > **Network Association**.
2. Enter the address in the **Primary Domain** field, and the domain name can be directed to any server node IP.

   Default domain name is <your computer IP>.xip.io. xip.io is an open domain name which is resolved as the IP address before xip.io by default, for example 10.10.10.10.xip.io is resolved as 10.10.10.10 via DNS.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Setting the Web Service Address

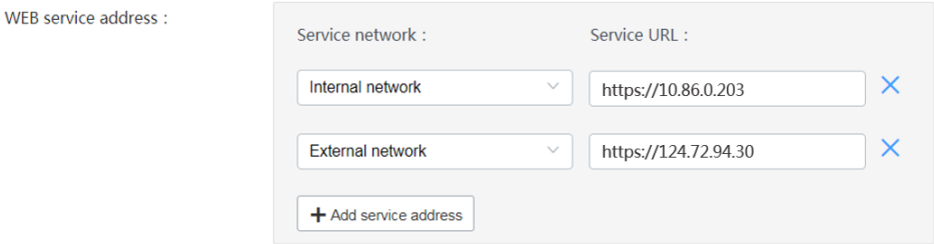
To make the device access the Web service address, for example when the device accessing the contact or downloading the firmware, you can set the service URL for the internal and external network separately, and then the server will send the corresponding address according to the network where the device locates in.

Procedure

1. Click **System Settings** > **Common Settings** > **Network Association**.
2. In the **WEB service address** field, click **Add service address**.
3. In the **Service network** field, select **Internal network**/**External network**.
4. In the **Service URL** field, enter the URL.

   The URL contains the protocol, the address and the port.

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



   Note: If you have changed the port number that was mapped externally by port 80/443, URL should be added to the mapped port.

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

Setting the Log Service Address

When the device uploads the log, the device need access the log service address of the server. You can set the log URL for the internal and external network separately, and the server will send the corresponding address to the device according to the network where the device locates in.

About this task

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

Procedure

1. Click **System Settings** > **Common Settings** > **Network Association**.
2. In the **Log service address** field, click **Add service address**.
3. In the **Service network** field, select **Internal network**/**External network**.
4. In **Transmission type** field, select **UDP**.
5. In the **IP address** field, enter the IP address of the node to which the device uploads the log.

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

6. Click **Save**.
7. Operate according to the prompts, and click **OK**.

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, the maximum IVR port should not be less than 10199.

Procedure

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

Table 5:

Parameter	Description
IVR port	The range of the IVR port. **Default port range**: from 10000 to 19999.
BFCP/FECC port	The range of the BFCP/FECC port. **Default port range**: from 11000 to 12999.
Stack signaling port	If you want to configure two or more MCU services, you need to configure the stack signaling port. **Default port range**: from 13000 to 13199.
Stack media port	If you want to configure two or more MCU services, you need to configure the stack media port. **Default port range**: from 13200 to 13399.

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

Configuring the Time

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

Procedure

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

Table 6: Time parameter

Parameter	Description
Current server time	The current time of YMS.

Parameter	Description
Time access	The method used by YMS to access the time and date. • **SNTP** • **Date & time configuration** **Default**: SNTP.
Server domain	If you select **SNTP**, configure the primary server and the backup server of NTP. **Note**: the first server address is the primary server by default, and its default value is pool.ntp.org.
Date & time	The date and the time.
Timezone	The time zone used by YMS and the default time zone for scheduling the conference.
Auto adjust conference DST	The type of DST. The supported types in YMS are as follows: • **Auto**-YMS will automatically use the corresponding DST according to the selected time zone. When users schedule conferences in countries using the DST, the DST is enabled by default. • **Disable**-DST is not used. **Default**: disabled.

3. Click **Save**.
4. Click **OK**, and the system will reboot.

Setting the Data Space

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

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

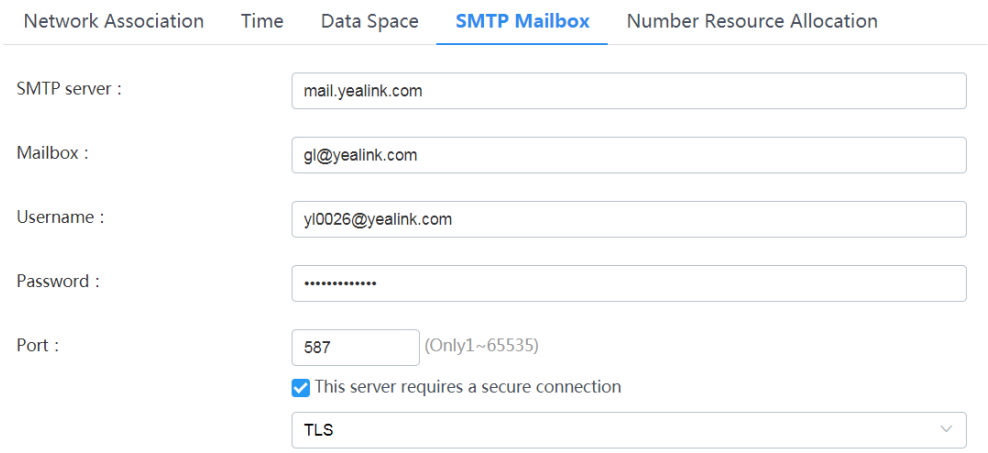
1. Click **System Settings** > **Common Settings** > **Data Space**.
2. Enter the desired quota in the corresponding field.
3. Click **Save**.

Configuring the SMTP Mailbox

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

Procedure

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



3. Click **Test Mailbox Setting**.
4. Enter the email address of the recipient in the **Test mailbox** field.
5. Click **OK**.

   If the mailbox connection succeeds, the prompt “Operation success” is popped up.

   Note: If the mailbox connection fails, make sure the connection between YMS and SMTP server can work and the account information is correct.

   If the test fails, it may be caused by the failure of YMS testing the SMTP server, and *Importing the Trusted CA Certificate* is need to be done.
6. Click **Save**.

Allocating the Number Resource

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

About this task

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

Procedure

1. Click **System Settings** > **Common Settings** > **Number Resource Allocation** > **Add**.
2. Configure the parameters.

Table 7: Parameters of the number

Parameter	Description
Number type	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 number 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**.
Origin section	The origin section.
Rear section	The rear section.
Description	The additional notes.

3. Click **OK**.

Configuring the Node

You can configure the basic network information of the server node to get a smooth network.

Procedure

1. Click **System Settings** > **Node Management**.
2. Click icon on the right side of desired node, and edit the parameters.

Note:

- Make sure that the DNS server is available. Otherwise, the service will be abnormal.
- You can configure only one default routing; when the adapter has multiple IP addresses, the routing of all the IP addresses should be specified, the default one cannot be used; the smaller the number is, the higher the priority is; the routing rule came with the system cannot be deleted. If they are deleted, other added routing rules will be abnormal.
- For a single network adapter deployment in the external network, you need to configure two intranet IP addresses, one mapping to the public network with the public button on and the other mapping to the intranet (only mapping one IP address is not allowed). Only mapping one intranet IP address to the public network will make the service abnormal. For more information, refer to *Yealink Meeting Server Network Installation Guide*.
- If your YMS is the cluster version, you cannot edit the IP address of the master node on the management platform. You can edit it in the installation file and re-install it. For more information, refer to *Yealink Meeting Server Software Installation Guide*.

Related concepts

Introduction of the Deployment Structure

Viewing the Node Information

You can view the status of the server and the service, the information of the progress, the port and the disk.

Procedure

1. Click **System Settings** > **Node Management**.
2. Click on the right side of desired node.

Configuring the Address Port Mapping

You can map the IP address and port of the internal network to the external network, so that the user in the external network can access the service provided by the IP address and port of the internal network.

Procedure

1. Click **System Setting** > **Address Port Mapping** > **Add**.
2. Configure the parameters of the address port mapping.
   The parameters of the address port mapping should be the same as the mapping on the router.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Setting the IP Property

When the egress has multi-line access, you can set the IP attribute for the edge business node, so that the address information of the Turnserver and MCU obtained by the device comes from the same operator as yours, which ensures the conference quality.

Procedure

1. Click **System Setting** > **Address Port Mapping** > **IP Property** > **Add**.
2. Configure the parameters.

Table 8:

Parameter	Description
IP address	The IP address of this business node.
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.

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

Adding a Sub Admin Account

For the system security, you can add different sub admin accounts, and allocate different authorities to them.

About this task

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

Procedure

1. Click **System Setting** > **Sub Admin Account** > **Add**.
2. In the **Username** field, enter the name.
3. In the **Role** field, select the desired type.
4. In the **Level** field, select the read or write permission.
5. If you select **Customization** as the **Role**, select the desired modules in the **Manageable modules** field for the sub admin account.
6. Click **Save**.

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

Editing the Information of a Sub Admin Account

You can edit the password or the authority of a sub admin account.

Procedure

1. Click **System Setting** > **Sub Admin Account**.
2. Click on the right side of the sub admin account.
3. To reset the password of the sub admin account, click **Reset**, and click **OK**.
4. Edit the account authority in the corresponding field.
5. Click **Save**.

Delete the Abnormal IP

If you want to cancel the restriction of the device, you can delete its abnormal IP.

About this task

The device IP is abnormal in the following situations:

- Within one minute, the device fails to register a YMS account via the same IP address for several times (the times depends on the **Max frequency of IP call or auth failure** in *Configuring Intelligent Security Strategy*).
- Within one minute, the device fails to join a conference via the same IP address for several times (the times depends on the **Max frequency of IP call or auth failure** in *Configuring Intelligent Security Strategy*).
- The times of the device calling the same IP address exceeds the max frequency during the device detection period (refer to *Configuring Intelligent Security Strategy*).

Procedure

1. Click **System Setting** > **Security** > **Abnormal IP**.
2. Select the desired account, and click **Delete**.

3. Click **OK**.

Adding a Security Group

You can add security groups applied to the whitelist and the blacklist for various services to secure the server.

Procedure

1. Click **System Setting** > **Security** > **Security Group** > **Add**.
2. Configure the parameters.

Table 9: Parameters of the security group

Parameter	Description
Name	The name of this security group.
Type	The type of this security group. The supported types are as follows: • Single IP • Section IP
IP Address	Enter the IP address or the IP address range.

3. Click **Save**.

Related tasks

Configuring the Registration Service
Configuring the Third Party REG Service
Configuring the IP Call Service
Configuring the PSTN Gateway Service
Setting the Peer Trunk Service
Configuring the SFB Service

Configuring Intelligent Security Strategy

You can customize the security strategy for IP calls or the registration.

Procedure

1. Click **System Setting** > **Security** > **Intelligent Security Strategy**.
2. Configure the parameters of the SIP signaling.

Table 10: Parameters of the SIP Signaling

Parameter	Description
Attack detection cycle	The detection cycle. **Default**: 25 seconds.

Parameter	Description
Max frequency of IP call or auth failure	During the Attack detection cycle, if the number of IP call failure or authentication failure exceeds the max frequency, the action will be taken as an attack and the IP address will be forbidden for a period. **Default**: 10 times.
Suspected attack banned duration	The banned duration. **Default**: 10 minutes.
Max suspected attacks frequency within 24 hours	Within 24 hours, if the number of IP calls from the same IP address exceeds the max frequency, this IP is forbidden for a long time, and you can free this IP by deleting the abnormal IP (refer to *Delete the Abnormal IP*). **Default**: 3 times.
Long term banned duration	The banned duration. You can free up the banned duration by deleting the abnormal IP (refer to *Delete the Abnormal IP*). **Default**: 7 days.
Max concurrent IP call per node	The max number of the concurrent IP calls from the same IP address. If the number of IP calls exceeds the max number, the IP address will be forbidden. **Default**: 30.

3. In the **Whitelist** field, select the security group, and the devices in this group are not affected by the security strategy.
4. Click **Save**.

Applying for the Accesskey

To call the YMS API to integrate with you own system, you need apply for the accesskey.

Procedure

1. Click **System Setting** > **Security** > **Accesskey**.
2. Click **Apply**.

Adding the User-Agent Blacklist

If you know the User-Agent type of devices 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** > **Add**.

2. Configure the parameters.

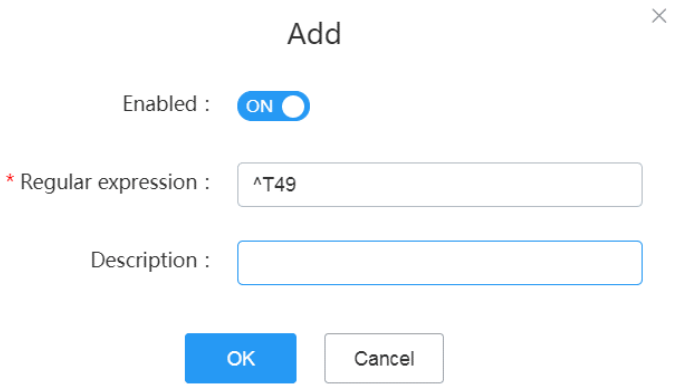


Table 11:

Parameter	Description
Enable	Enable or disable this blacklist. **Default**: enabled.
Regular expression	The Perl Compatible Regular Expressions (PCRE). **Note**: for example, if you set the PCRE as ^T49, all User-Agent devices whose model type starts with T49 cannot call into YMS.
Description	The additional notes for this blacklist.

3. Click **OK**.

Adding the User-Agent Compatible List

If you know the User-Agent type of devices and you want to allow devices of this type to call into YMS or to register YMS accounts, you can add them into the compatible list.

Procedure

1. Click **System Setting** > **Security** > **User-Agent Compatible List** > **Add**.
2. Configure the parameters.

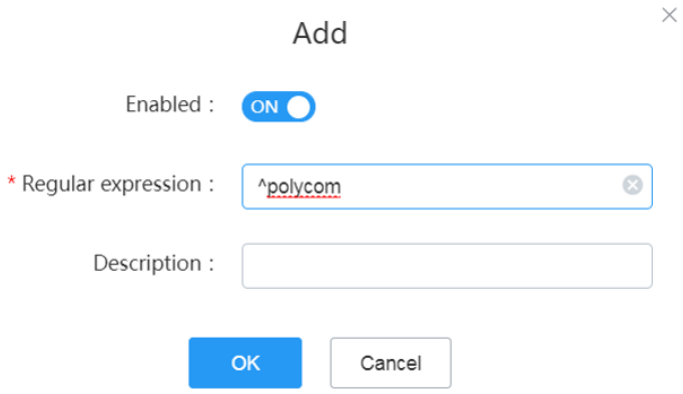


Table 12:

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

3. Click **OK**.

Activating a License

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

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

- *Importing the Server Device License*
- *Activating a License Online*
- *Activating a License Offline*

Related tasks

Enabling the Broadcasting Interactive

Importing the Server Device License

You need import the server device license for unique association with this server.

Before you begin

You submit the enterprise name, the distributor name, the applicant, and the country to Yealink, to get the device license.

Procedure

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

2. Select the device license.
3. Click **OK**.

Results

If the license series number succeeds in linking, the page will display as follows:

Activating a License Online

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

Before you begin

- *Importing the Server Device License* is done.
- You obtain the license by providing the applicant, the license type, the concurrent number and the validity to Yealink.

Procedure

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

Results

The license is displayed on the page.

Related information

Failing to Activating a License Online

Activating a License Offline

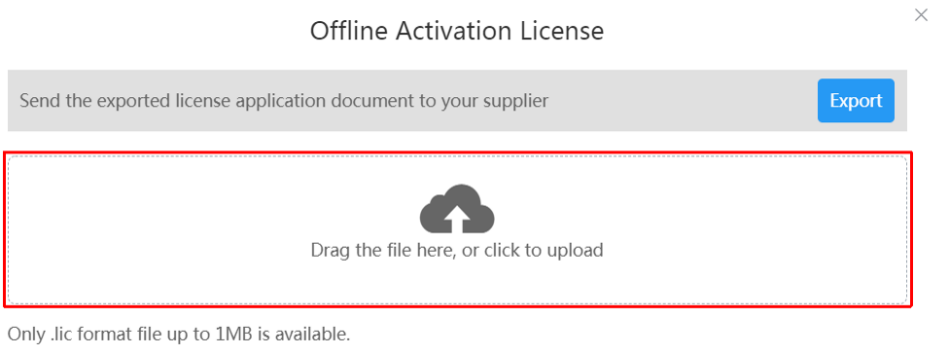
If the server cannot access the public network, you can activate the license offline.

About this task

- *Importing the Server Device License* is done.
- You obtain the license by providing the applicant, the license type, the concurrent number and the validity to Yealink.

Procedure

1. Click **System Setting** > **License** > **Offline Activation License**.
2. Click **Export**, and send the exported file to Yealink.
3. Click the field of the dotted box to upload the license obtained from Yealink.



Results

The license is displayed on the page.

Related information

Failing to Activating a License Offline

Disassociating the License

If you import the wrong license, you can disassociate it.

Procedure

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

Importing the Trusted CA Certificate

When the server sends the request about TLS connection to the device, the server need verify whether or not the device is reliable. The device will send the default certificate to the server to verify.

Procedure

1. Click **System Setting** > **Certificate** > **Trusted CA Certificate** > **Import**.
2. Click **Upload**, select the desired file, and click **OK**.
3. Operate according to prompts, click **OK**, and the system will reboot to make it take effect.

Importing the HTTPS Certificate

When you access YMS by HTTPS protocol, the browser will 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.

Procedure

1. Click **System Setting** > **Certificate** > **HTTPS Certificate** > **Import**.
2. Click **Upload**, and select the desired file.
3. Click **OK**.

Importing the TLS Certificate

When the device sends request about TLS connection to the server, the device will verify whether or not the server is reliable. The server will send the certificate to the device, and the device will verify this certificate according to the list of the reliable certificate.

Procedure

1. Click **System Setting** > **Certificate** > **TLS Certificate** > **Import**.
2. Click **Upload**, and select the desired file.
3. Click **OK**.

Setting the Display on the Web Page

According to the enterprise need, you can customize the enterprise logo, the background image of the web and WebRTC, and the display image of the video conference.

About this task

The parameters are described as below:

Table 13: Parameters of the Logo

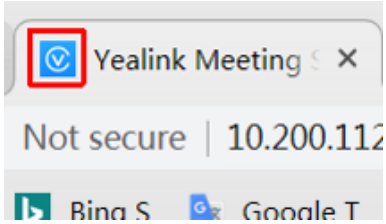
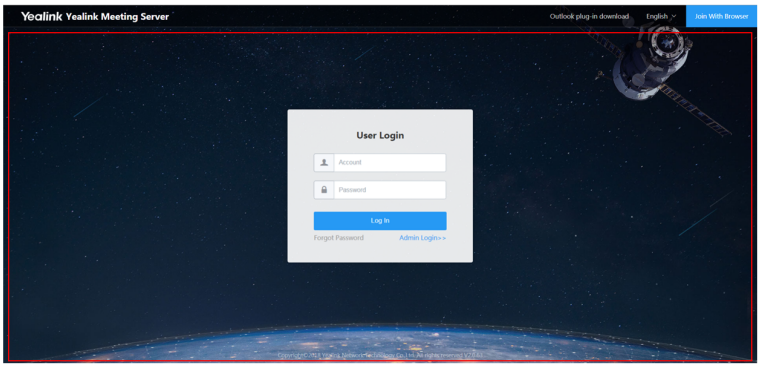
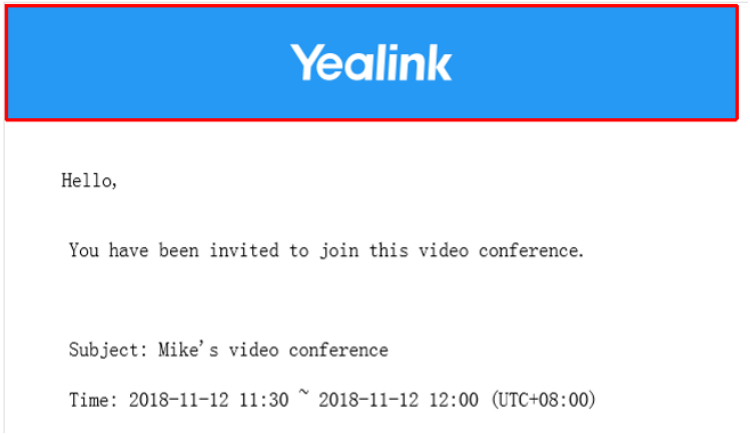
Parameter	Effect
Portal logo	
Tab logo	

Table 14: Parameters of the Web Portal

Parameter	Effect
Background image	
Email header logo	

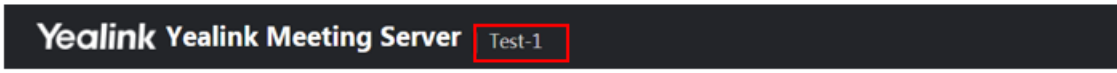
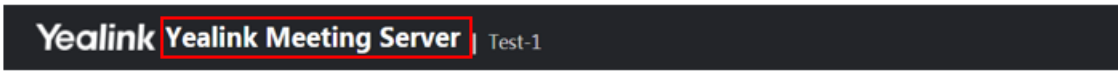
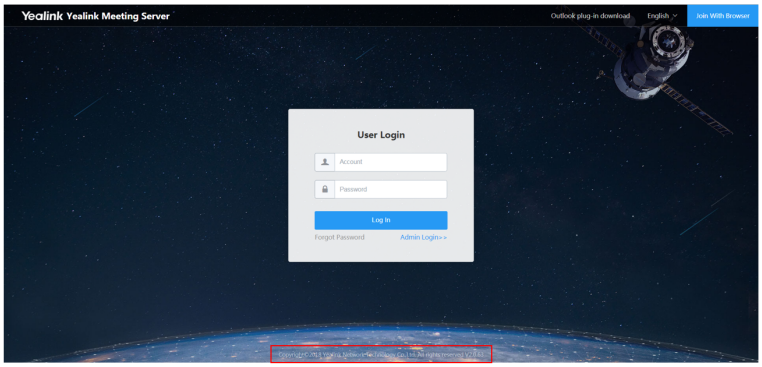
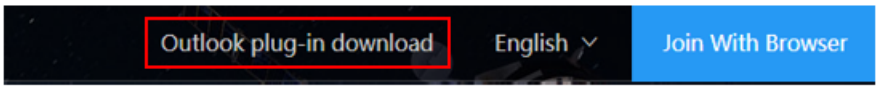
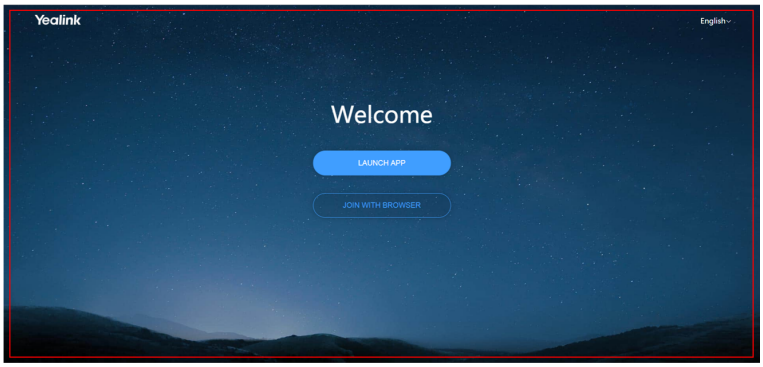
Parameter	Effect
Enterprise name	
Platform name	
Display copyright	
Display Outlook plug-in download	
Session timeout	It refers to that when the user or administrator logs into YMS but do not use YMS for a while, and after a specific time (the timeout), the system will log out the account automatically and return to the login page. **Default**: 30 minutes.

Table 15: Parameters of the WebRTC Portal

Parameter	Effect
Enable WebRTC	Allow or refuse the user to join the conference via browser. **Default**: 30 minutes.
Background image for WebRTC home screen	

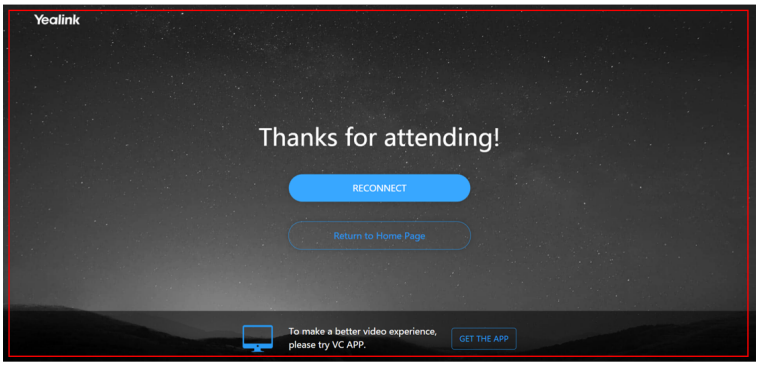
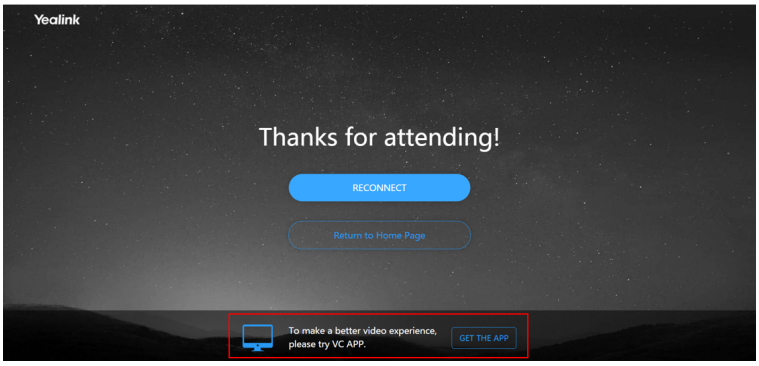
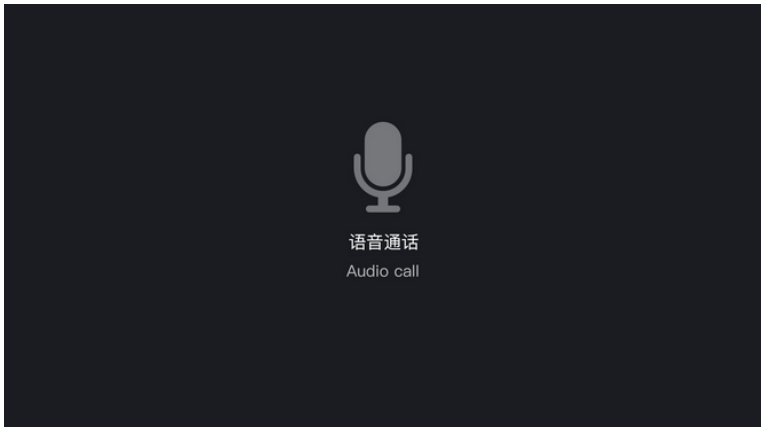
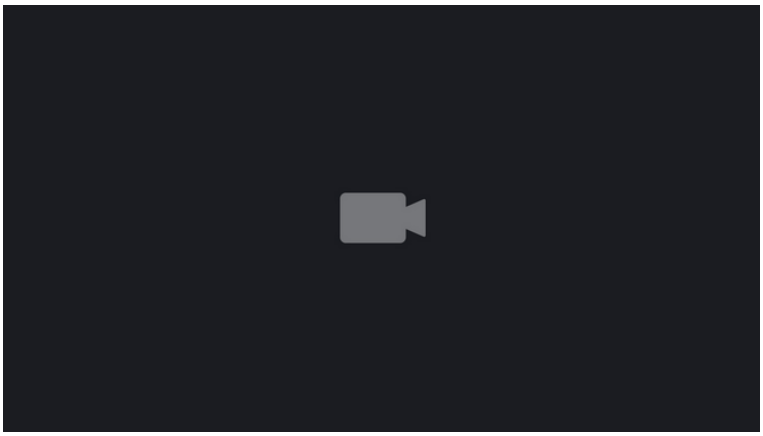
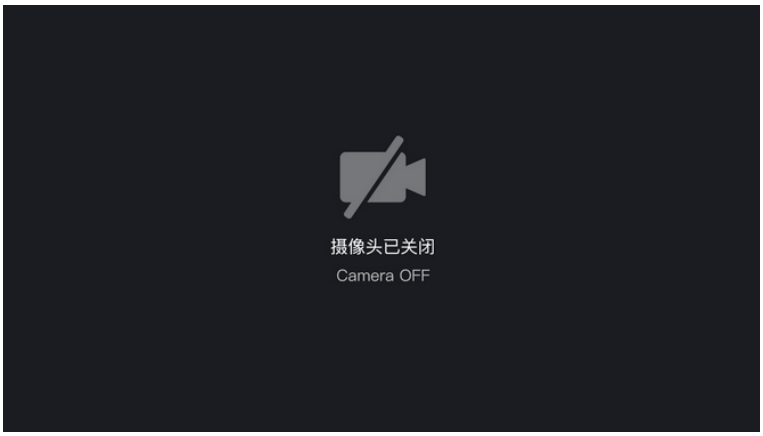
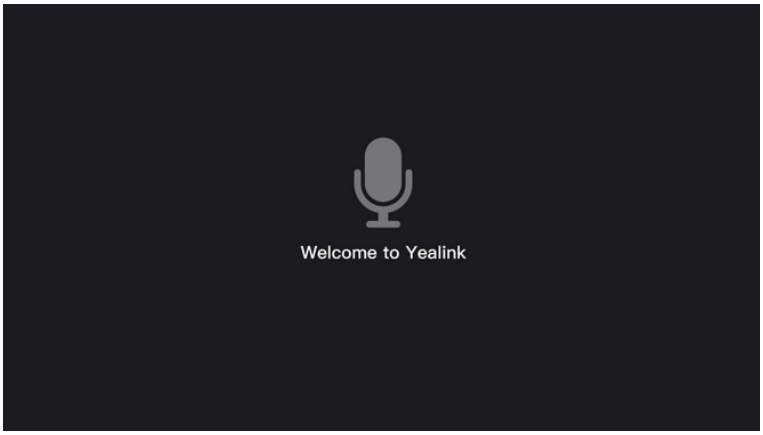
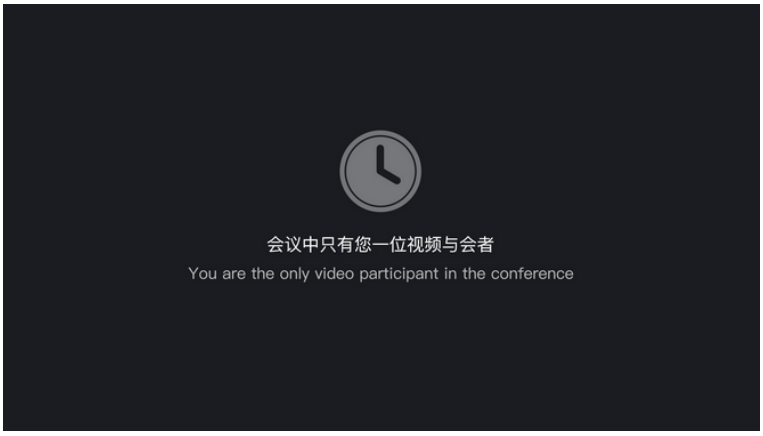
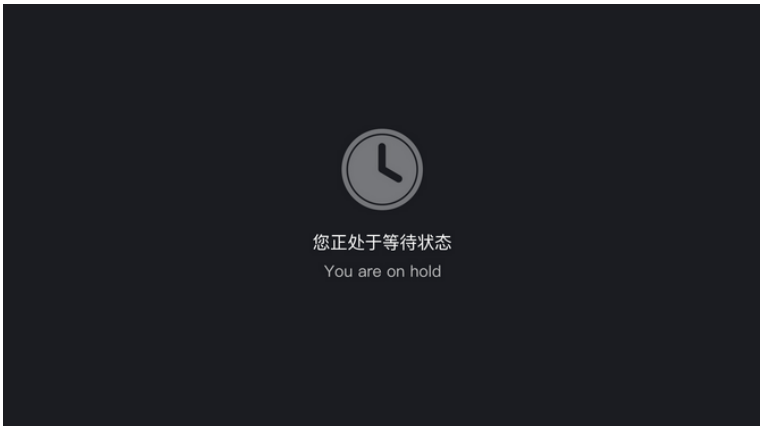
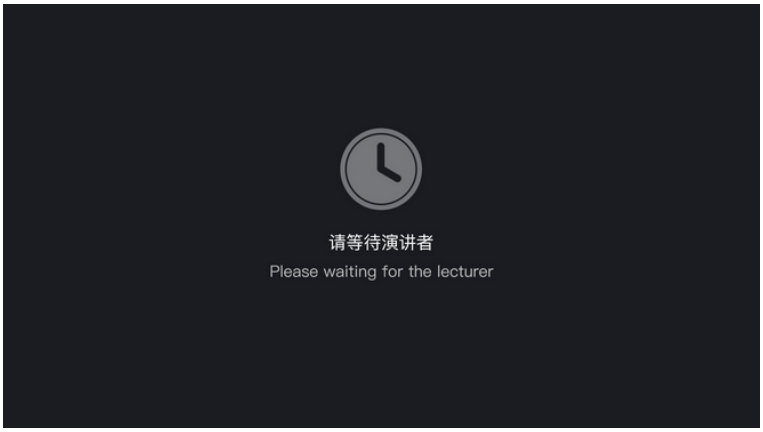
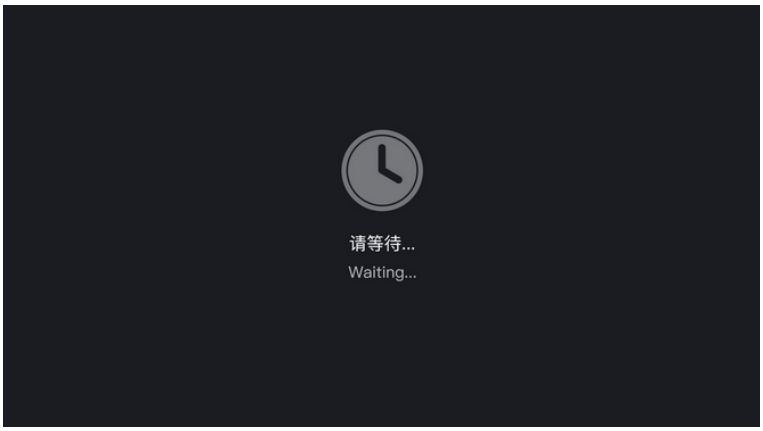
Parameter	Effect
Background image of WebRTC end page	
Extension download address	When you use Google Chrome to visit Yealink Web App, and share contents with the remote, you need to download the content sharing plugin.
Display PC soft-client download	
Windows	The address for downloading Yealink VC Desktop for Windows.
Mac	The address for downloading Yealink VC Desktop for Mac.

Table 16: Parameters of the Video Conference

Parameter	Effect
Audio call image	

Parameter	Effect
License limited image	
No video data image	
Camera OFF image	

Parameter	Effect
Welcome screen image	
The sole video call party image	
Conference lobby image	

Parameter	Effect
Waiting for the lecturer image	
Waiting image	

Procedure

1. Click **System Setting** > **Customization** > **Email Template**.
2. Configure the logo.
3. Configure the parameter of web portal.
4. Configure the parameter of WebRTC portal.
5. Configure the parameter of the video conference.

   If the device negotiates with the server to use the resolution of 360P, 720P, and 1080P, the video conference is displayed in 16:9; if they negotiate to use the resolution of CIF and 4CIF, the video conference is displayed in 4:3.

Configuring the Email Template

According to the enterprise needs, you can customize the email template for the enterprise administrators and the users.

About this task

The code in the **Subject** and **Content** cannot be deleted, otherwise, you might fail to send the email.

Procedure

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

3. Click **Save**.

Configuring SIP Trunk IVR

You can customize the SIP trunk IVR so that the user can join conferences or place calls according to the voice prompts.

About this task

If the regular expression replacement string is main_ivr@server domain name, you will go to the SIP trunk IVR.

Procedure

1. Click **System Setting** > **Customization** > **SIP Trunk IVR**.
2. Configure the receptionist greeting prompt, and do one of the following:
   - Select **Default Greeting**. The language depends on the IVR language. For more information, refer to *Setting IVR language* .
   - Select **Personal Greeting**.

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

     (Optional:) if you want to dial extension directly without pressing the key, select the **Enable first-level extension dialing** checkbox.

     Select the desired key, enter the description and the operation which contains transferring to extension/conference, extension IVR dialing, conference IVR dialing, and repeating menu.
3. Click **Save**.

Configuring the Audio IVR

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

About this task

If the regular expression replacement string is conference_ivr@server domain name, you can set 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.
   - Select **Personal Greeting**.

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

Service Management

- *Configuring the Registration Service*
- *Communicating with Other Devices via IP Call*
- *Setting the Redirect Service*

- *Configuring the Third Party REG Service*
- *Communicating with PSTN*
- *Setting the Peer Trunk Service*
- *Configuring the REG Trunk Service*
- *Communicating with Skype for Business Server*
- *Configuring the GK Service*
- *Configuring the H.323 Gateway*
- *Configuring the Interactive Media Service*
- *Configuring the Broadcast Media Service*
- *Configuring the RTMP Media Service*
- *Configuring the Media Bypass Service*
- *Adding the Recording Service*
- *Configuring the Traversal Service*

Configuring the Registration Service

You need configure the registration service, so that the user in the intranet and the extranet can register YMS accounts. When the device registering, the proxy server directs to this node.

Procedure

1. Click **Service** > **SIP Service** > **Registration Service** > **Add**.
2. Configure the basic parameters.

Table 17: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.

3. Configure the parameters of the service address.

Table 18: Parameters of the Service Address

Parameter	Description
Network	The IP address used by this node.
TLS Port	The TLS port used by this node. **Note**: only TLS registration is available.

4. Configure the security policy.

Table 19: Parameters of the Security Policy

Parameter	Description
Enable security policy	Enable or disable the security policy. **Default:** disabled.

Parameter	Description
Mode	Select a mode. The supported modes are as follows: • **Whitelist**: allow the device in the security group to call into. • **Blacklist**: forbid the device in the security group to call into.
Security Group	Select a security group.

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

Related tasks

Adding a Security Group

Communicating with Other Devices via IP Call

For convenience, you can set the rules for the incoming and outgoing IP calls, and you need set the IP call service (refer to *Configuring the IP Call Service*) and the call routing rules (refer to *Adding a Call Routing Rule*)(if you set the outgoing call rules).

- *Configuring the IP Call Service*

Configuring the IP Call Service

For friendly calls, you can configure the outgoing and the incoming call rules in the IP call service.

Procedure

1. Click **Service** > **SIP Service** > **IP Call Service** > **Add**.
2. Configure the basic parameters of the IP call service.

Table 20: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.
Outgoing protocol	Select a protocol for transmitting the SIP signaling. The supported protocols are as follows: • UDP— the optimal protocol for transmitting SIP signaling. • TCP—the reliable protocol for transmitting SIP signaling. **Default**: UDP.

3. Configure the parameters of the service address.

Table 21: Parameters of the Service Address

Parameter	Description
Network	The IP address used by this node.
UDP/TCP Port	The UDP/TCP port used by this node. **Note**: 5060 port is compulsory.
TLS Port	The TLS port used by this node. **Default**: port 5062.

4. Enable **Support video**, so that you can place a video call to the remote that supports video call.

   It is enabled by default.
5. Enable **Support content sharing**, so that you can share the content with the remote that supports receiving or sending contents.

   It is enabled by default.
6. Enable **Replace the calling domain with the local IP**, so that when you invite the device to join the conference by IP call, the device will display the server IP address as the caller ID.

   It is enabled by default.
7. Enable **Media Bypass** to improve the server performance and to support a larger number of participant in the conference. Note that third-party devices have a lower compatibility.

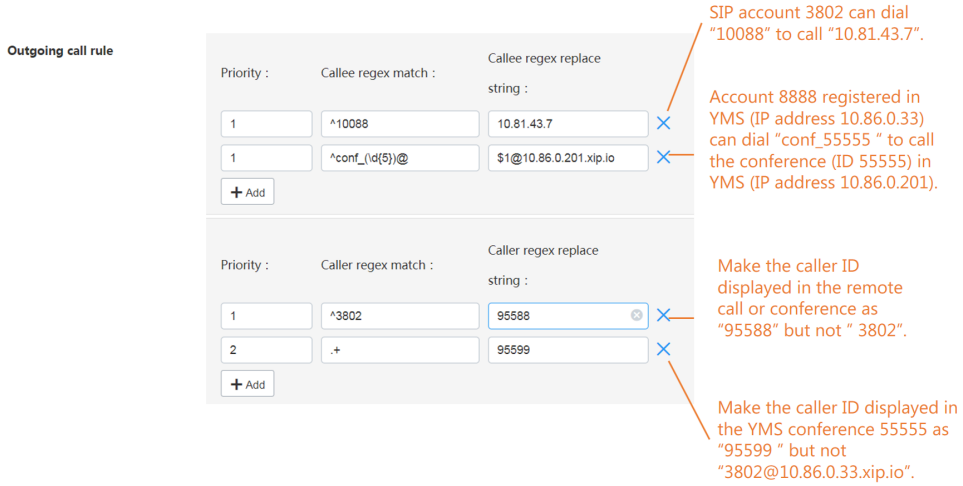
   If **Support video** is enabled, **Media Bypass** is recommended to be enabled.

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

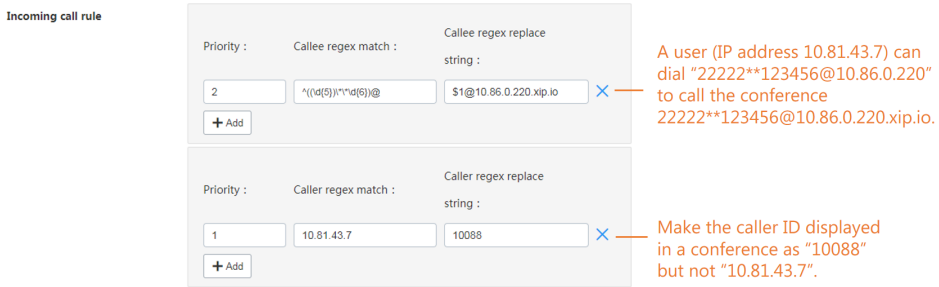
Table 22: Security policy parameter

Parameter	Description
Enable security policy	Enable or disable the security policy. **Default**: disabled.
Mode	Select a mode. The supported modes are as follows: • **Whitelist**: allow the device in the security group to call into. • **Blacklist**: forbid the device in the security group to call into.
Security Group	Select a security group.

9. Configure the outgoing call rule.



10. Configure the incoming call rule.



11. Click **Save**.

12. Operate according to the prompts, and click **OK**.

Related concepts

Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings

Related tasks

Adding a Security Group

Setting the Redirect Service

If you use the cluster version, when there are multiple registration services, you only need to enter the address and port of the redirection service.

Before you begin

Configuring the Registration Service is done.

Procedure

1. Click **Service** > **SIP Service** > **Redirect Service** > **Add**.
2. Configure the corresponding parameters.

Table 23: Basic Parameters

Parameter	Description
Enabled	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.

3. Configure the parameters of the service address.

Table 24: Service address

Parameter	Description
Network	The IP address of this node.
TLS port	The TLS port used by this node. **Note**: only TLS registration is available.

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

Configuring the Third Party REG 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 on this server, you only need edit the third-party REG service to improve the editing efficiency.

About this task

Using TLS to register third-party devices on the server is not supported.

Procedure

1. Click **Service** > **SIP Service** > **Third Party REG Service** > **Add**.
2. Configure the basic parameters.

Table 25: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.

3. Configure the parameters of the service address.

Table 26: Parameters of the Service Address

Parameter	Description
Network	The IP address used by this node.
UDP/TCP Port	The UDP/TCP port used by this node.

4. Enable **Support video**, so that you can place video calls to the remote that supports video call.

   It is enabled by default.
5. Enable **Support content sharing**, so that you can share contents with the remote that supports receiving or sending contents.

   It is enabled by default.
6. 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 a 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* .
7. Configure the security policy.

Table 27: Parameters of the Security Policy

Parameter	Description
Enable security policy	Enable or disable the security policy. **Default**: disabled.
Mode	Select a mode. The supported modes are as follows: • **Whitelist**: allow do the device in the security group to call into. • **Blacklist**: forbid the device in the security group to call into.
Security Group	Select a security group.

8. Click **Save**.
9. Operate according to the prompts, and click **OK**.

Related tasks

Adding a Security Group

Communicating with PSTN

To communicate with Microsoft PSTN, you need do the following: *Configuring the PSTN Gateway Service* and *Adding a Call Routing Rule* .

- *Configuring the PSTN Gateway Service*

Configuring the PSTN Gateway Service

To communicate with the device in PSTN (such as the fixed line), you need configure the PSTN gateway.

Procedure

1. Click **Service** > **SIP Service** > **PSTN Gateway Service** > **Add**.
2. Configure the basic parameters.

Table 28: Basic Parameters

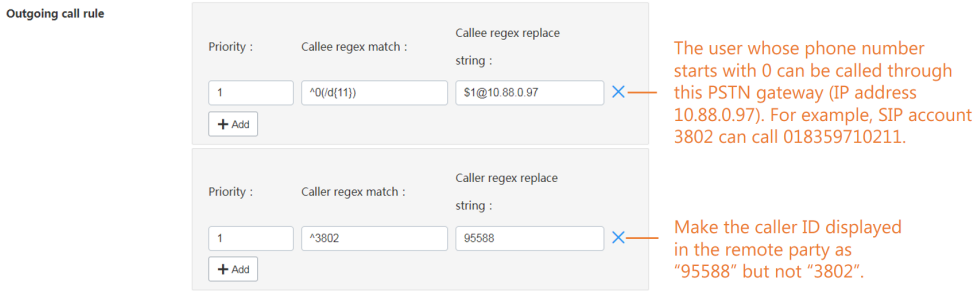
Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.
Network	The IP address of this node.
Port	The source port on YMS for communicating with the PSTN gateway. **Note**: the value can be any integer from 0 to 65535.
Gateway address	The IP address or the domain name of the gateway.
Gateway Port	The port of the PSTN gateway. **Default port**: 5060. The value can be any integer from 0 to 65535.
Transport protocol	Select a protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP**— the optimal protocol for transmitting the SIP signaling. • **TCP**—the reliable protocol for transmitting the SIP signaling. **Default**: UDP.
Support video	Enable it if the PSTN gateway supports video. **Default**: disabled.
Support content sharing	Enable it if the PSTN gateway supports receiving or sending contents. **Default**: disabled.

3. Configure the security policy.

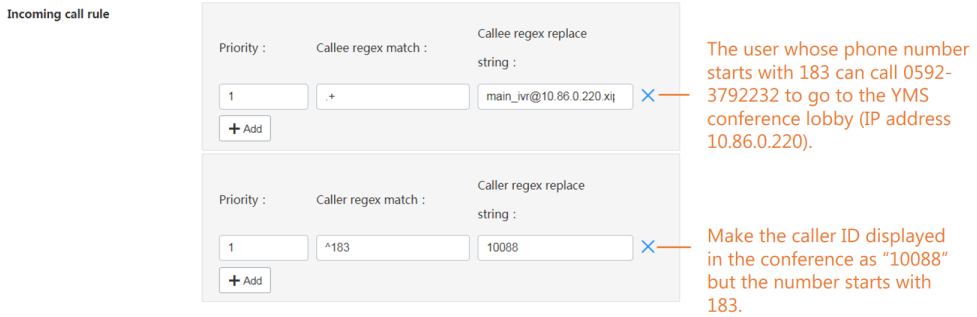
Table 29: Security policy parameter

Parameter	Description
Enable security policy	Enable or disable the security policy. **Default**: disabled.
Mode	Select a mode. The supported modes are as follows: • **Whitelist**: allow the account in the security group to call into via PSTN gateway. • **Blacklist**: forbid the account in the security group to call into via PSTN gateway.
Security Group	Select a security group.

4. Configure the outgoing call rule.



5. Configure the incoming call rule.



6. Click **Save**.
7. Operate according to the prompts, and click **OK**.

Related concepts

Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings

Related tasks

Adding a Security Group

Setting the Peer Trunk Service

You need set the peer trunk service and add call routing rules (refer to *Adding a Call Routing Rule*) to make users in two systems communicate by calling any number, for example, the communication between two YMSs.

Procedure

1. Click **Service** > **SIP Service** > **Peer Trunk Service** > **Add**.
2. Configure the basic parameters.

Table 30: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.
Network	The IP address of this node.
Port	The source port on YMS for connecting to other systems. **Note**: the value can be any integer from 0 to 65535.
Transport protocol	Select a protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP**— the optimal protocol for transmitting SIP signaling. • **TCP**—the reliable protocol for transmitting SIP signaling. **Default**: UDP.
Outbound proxy	Enable or disable the outbound proxy server. **Default**: disabled.
Proxy address	The IP address or domain name of the other system.
Proxy port	The port of the other system. **Note**: the value can be any integer from 0 to 65535.
Support video	If the other system supports the video, you can enable this. **Default**: enabled.

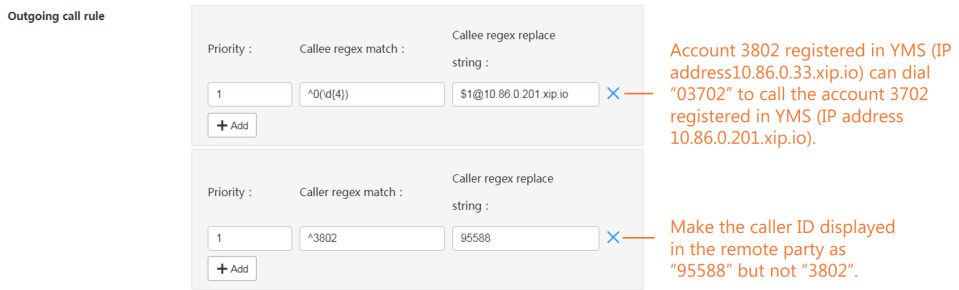
Parameter	Description
Support content sharing	If the other system supports receiving or sending the content, you can enable this. **Default**: enabled.
Media Bypass	Enable it to improve the server performance and to support a larger number of participant in the conference. Note that third-party devices have a lower compatibility. **Note**: it is disabled by default. 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* .

3. Configure the security policy.

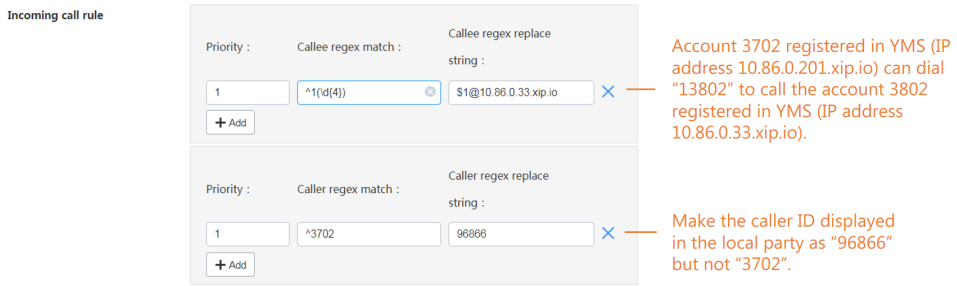
Table 31: Security policy parameter

Parameter	Description
Enable security policy	Enable or disable the security policy. **Default:** disabled.
Mode	Select a mode. The supported modes are as follows: • **Whitelist**: allow the security group of another system to call into. • **Blacklist**: forbid the security group of another system to call into.
Security Group	Select a security group.

4. Configure the outgoing call rule.



5. Configure the incoming call rule.



6. Click **Save**.
7. Operate according to the prompts, and click **OK**.

Related concepts

Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings

Related tasks

Adding a Security Group

Configuring the REG Trunk Service

To communicate with the third-party PBX, you need configure the REG trunk service and add call routing rules (refer to *Adding a Call Routing Rule*). For example, when communicating with 3CX or BSFT server, YMS need register a 3CX or BSFT account.

About this task

The third-party accounts can only join YMS conferences, but cannot place P2P calls to YMS accounts.

Procedure

1. Click **Service** > **SIP Service** > **REG Trunk Service** > **Add**.
2. Configure the basic parameters.

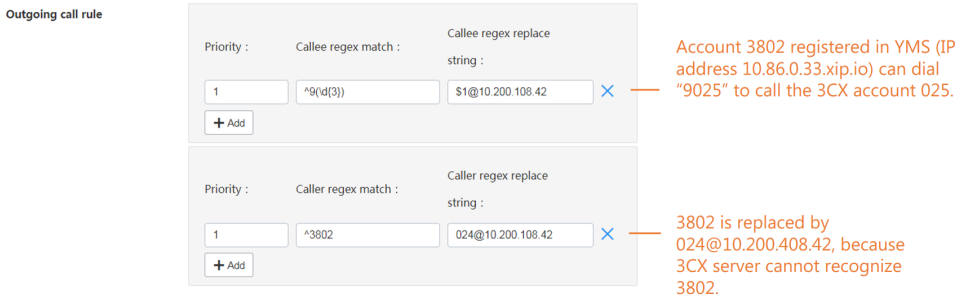
Table 32: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.
Network	The IP address of this node.
Port	The source port on YMS for communicating with the third-party server. **Note**: the value can be any integer from 0 to 65535.

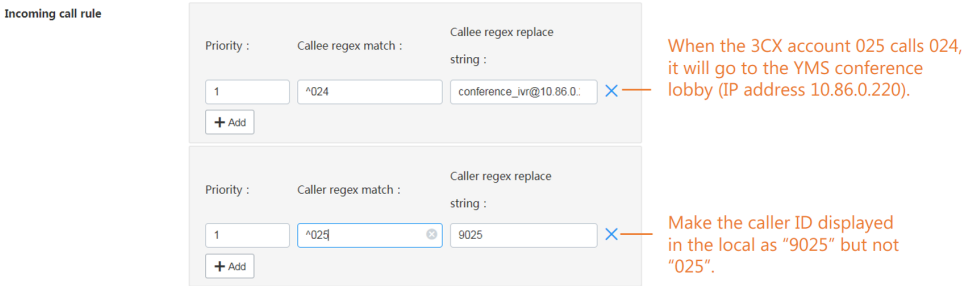
Parameter	Description
Transport protocol	Select a protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP**— the optimal protocol for transmitting the SIP signaling. • **TCP**—the reliable protocol for transmitting the SIP signaling. • **TLS**—the safe protocol for transmitting the SIP signaling. TLS is available only when the YMS is registered at a SIP gateway that supports TLS. **Default**: UDP.
Outbound proxy	Enable or disable the outbound proxy server. **Default:** disabled.
Proxy address	The IP address or the domain name of the third-party server.
Proxy port	The port of the third-party server. **Note**: the value can be any integer from 0 to 65535.
Display name	The name of the third-party server account.
URL	The IP address or the domain name of the third-party server.
Auth name	The authentication name of the third-party server account.
Auth domain	The authentication domain name of the third-party server account.
Password	The password of the third-party server account.
Expires	The registration timeout (in seconds) on YMS. If the time is out, YMS will send the registration request to the third-party server again. **Default**: 3600 seconds.
Support video	Enable it if the remote supports video. **Default**: disabled.
Support content sharing	Enable it if the remote supports receiving or sending contents. **Default**: disabled.

Parameter	Description
Media Bypass	Enable it to improve the server performance and to support a larger number of participants in the conference. Note that third-party devices have a lower compatibility. **Note**: it is disabled by default. 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* .

3. Configure the outgoing call rule.



4. Configure the incoming call rule.



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

Related concepts

Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings

Communicating with Skype for Business Server

YMS can communicate with the local Skype for Business (SfB) server, Microsoft Office 365 and other enterprise SfB servers.

Note: The communication with SfB 2016 and 2015 are supported by YMS.

For more information about the deployment of YMS with SfB, refer to *Skype for Business and Yealink Meeting Server Deployment Guide*.

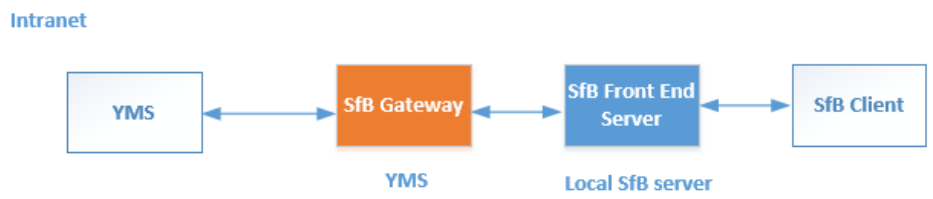
- *Communicating with the Local SfB Server*

- *Communicating with Microsoft Office 365*
- *Communicating with Other Enterprise SfB Servers*
- *Configuring the SFB Service*
- *Configuring 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 them, you can deploy YMS to communicate with the SfB.

To communicate with the local SfB server, you need do the following steps: *Configuring the Local SfB Server* , *Importing the TLS Certificate* , *Configuring the SFB Service* 、 *Configuring the SfB Gateway Media Service* , and *Adding a Call Routing Rule* .



- *Configuring the Local SfB Server*

Configuring the Local SfB Server

If YMS need 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 run the example command below to complete the configuration:

- If you use the cluster YMS 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 account in the Front-End Pool can communicate with YMS after the integration.

For more information the command, refer to *https://docs.microsoft.com/en-us/powershell/module/skype/?view=skype-ps*.

Table 33:

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 with 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. You can customize the name and it is unique. **-TrustedApplicationPoolFqdn**: defines the trusted application to pool to which this YMS belongs. **-Port**: defines the port on YMS that communicates with SfB server. It can be any unoccupied port from 0 to 65535. In YMS, the default port is 5067, which is recommended.
4. View the trusted application to ensure that YMS is added into 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 not an 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:** $newroute = New-CsStaticRoute -TLSRoute **-Destination** "sfb1.5060.space" **-Port** 5067 **-MatchUri** "sfb1.5060.space"	**Syntax explanation:** **-Destination**: defines the YMS DNS FQDN where SfB should send SIP requests matching the domain specified in **-MatchUri**. **-Port**: defines the port on YMS that communicates with SfB server. It can be any unoccupied port from 0 to 65535. In YMS, the default port is 5067, which is recommended. **-MatchUri**: defines the matched YMS DNS FQDN.
8. Apply your required static route to your registrars' static routing configuration.	Set-CsStaticRoutingConfiguration **-Identity** "Service:Registar: <Front End Pool DNS FQDN>" -Route @{Add=$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 with 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 do the following: *Configuring Microsoft Office 365* , *Importing the TLS Certificate* , *Configuring the SFB Service* , *Configuring the SfB Gateway Media Service* , and *Adding a Call Routing Rule* .

Note that you need enable the federation on Microsoft Office 365.

- *Configuring Microsoft Office 365*

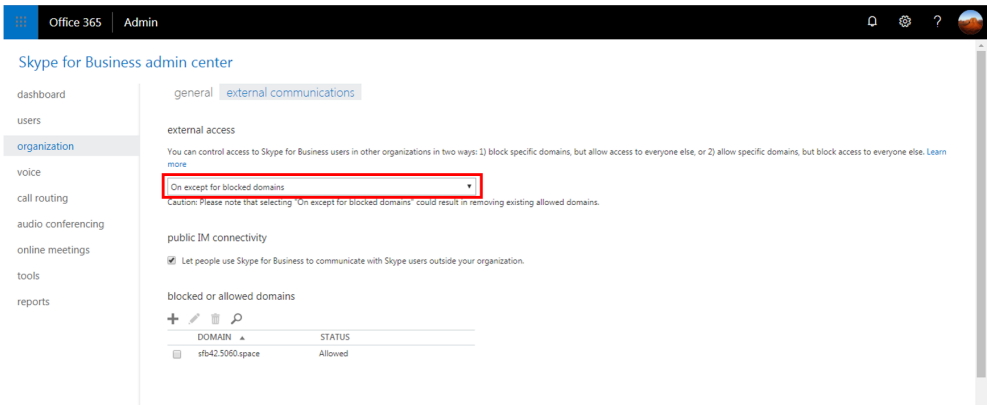
Configuring Microsoft Office 365

Procedure

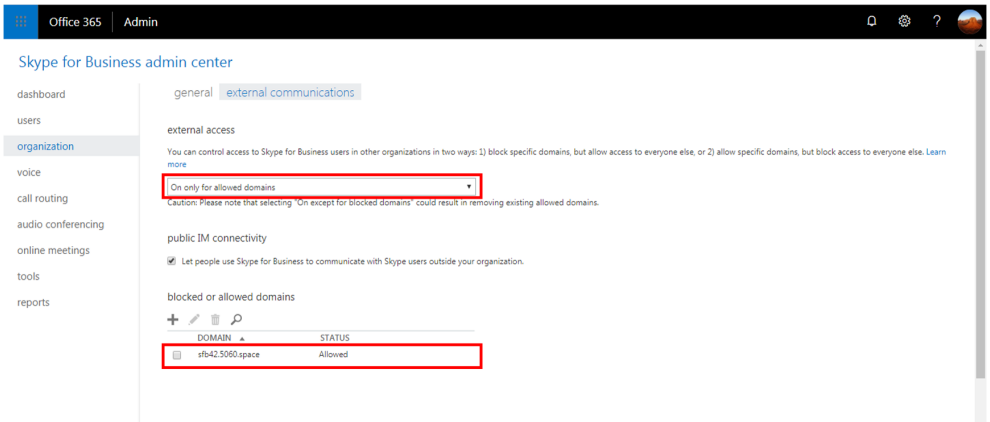
1. Make sure that the SRV record and the A record of YMS and SfB are configured on the public DNS server.
2. If you add a domain name in Office 365, and use the suffix of the added domain name to build a federation with YMS, you need add CNAME record and SRV record to the DNS server which the added domain belongs to.

3. If you use the suffix onmicrosoft.com or 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:

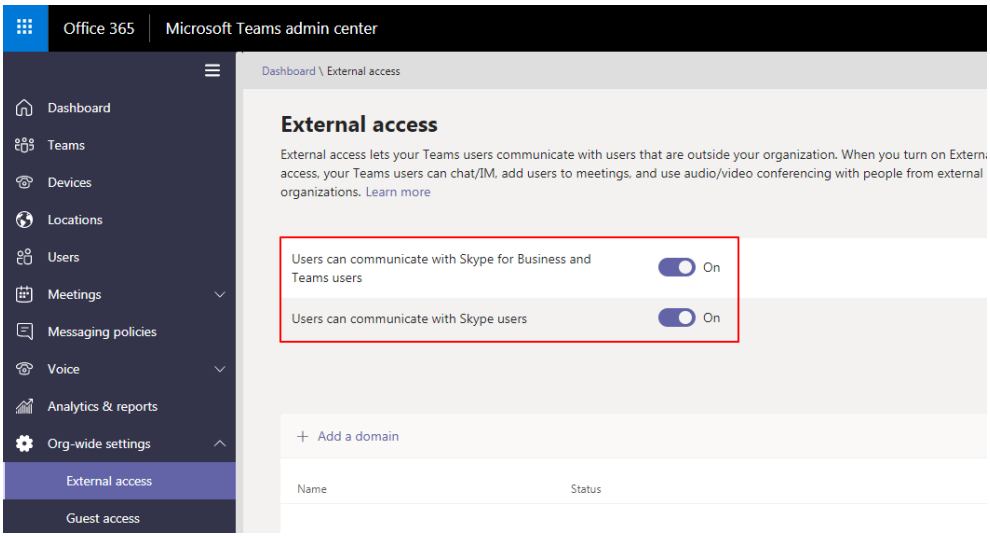
   - If users (using the legacy portal of Office 365) want to create the federation between Office365 and all the external YMSs, they need select **On except for blocked domains** in the **External access** field on Office 365.

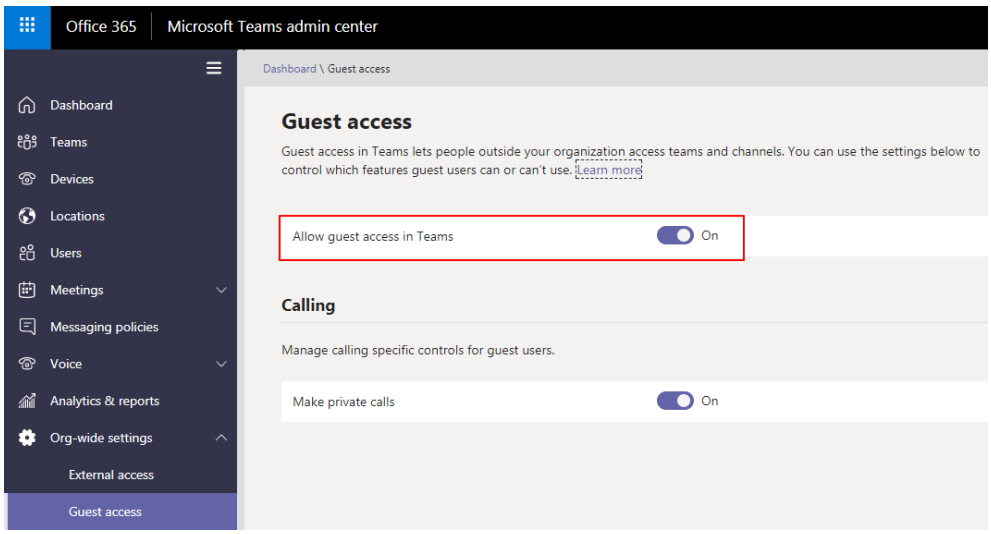


   - If users (using the legacy portal of Office 365) want to create the federation between Office 365 and one YMS, they need select **On only for allowed domains** in the **External access** field on Office 365 and DNS FQDN of YMS is added to the allowed domain.

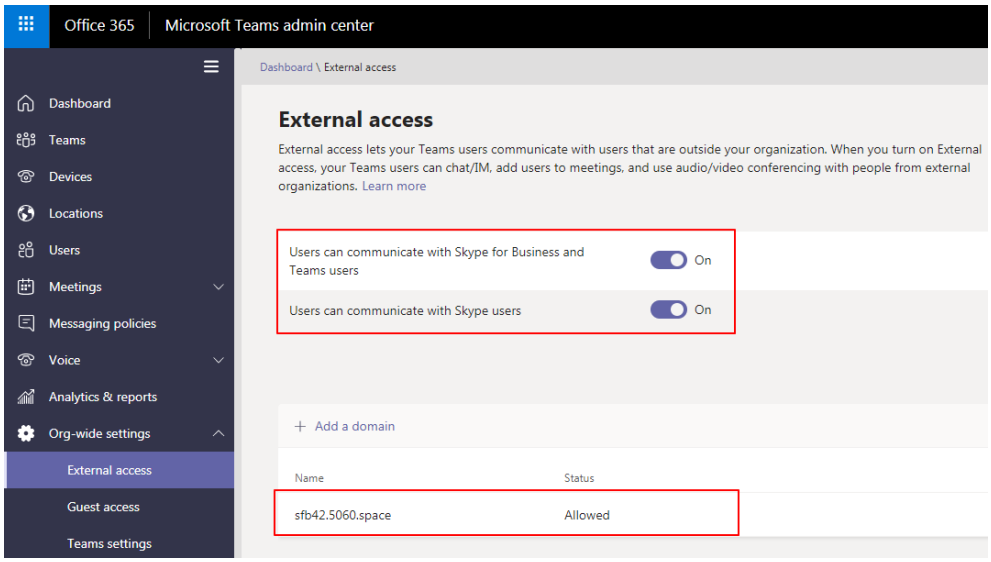


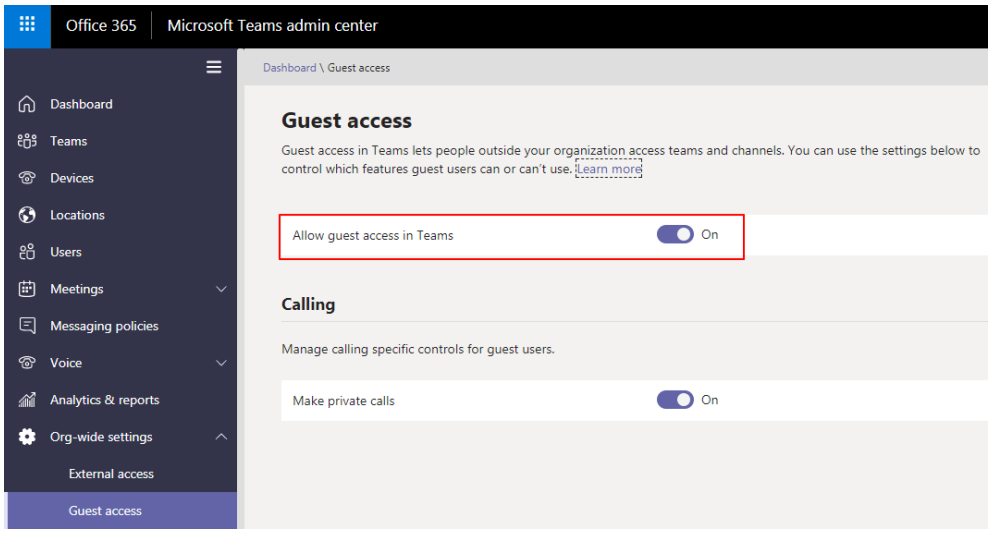
   - If users (using the new portal of Office 365) want to create the federation between Office365 and all the external YMSs, they should enable the switches displayed as below:





- If users (using the new portal of Office 365) want to create the federation between Office 365 and one YMS, they should enable the switches displayed as below and make sure that the DNS FQDN of YMS is added to the allowed domain.



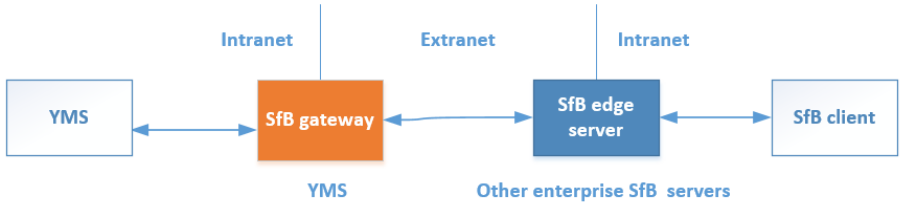


Communicating with Other Enterprise SfB Servers

The YMS device and the SfB device communicate through 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 do the following: *Configuring Other Enterprise SfB Servers* , *Importing the TLS Certificate* , *Configuring the SFB Service* , *Configuring the SfB Gateway Media Service* , and *Adding a Call Routing Rule* .

YMS communicates with the edge servers of other enterprise SfB via the SfB gateway. Note that edge servers of other enterprise SfB should enable the federation.



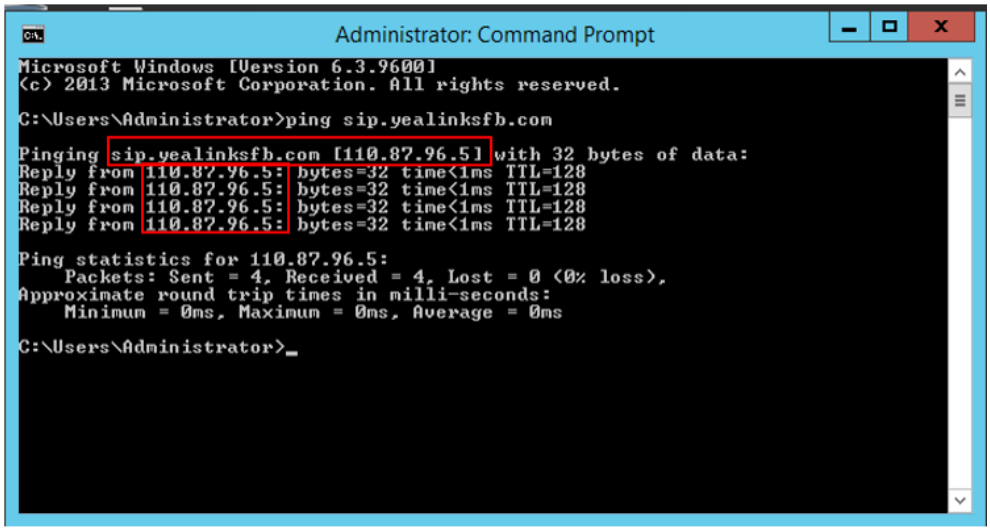
- *Configuring Other Enterprise SfB Servers*

Configuring Other Enterprise SfB Servers

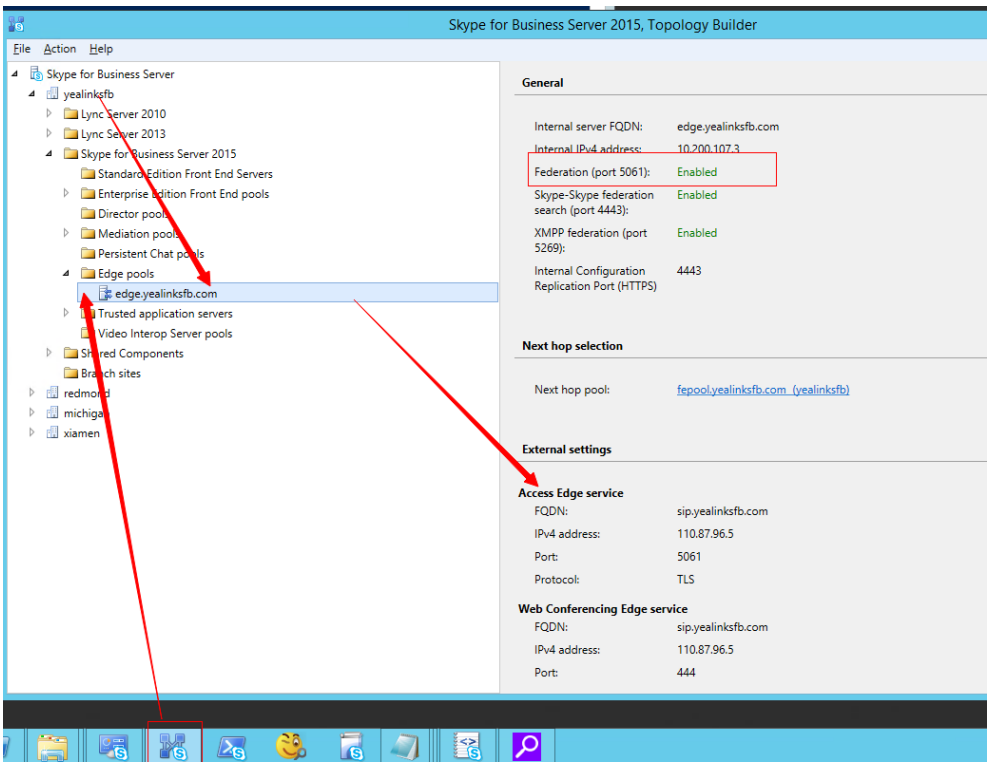
Procedure

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 check the DNS A record of the SfB edge server.



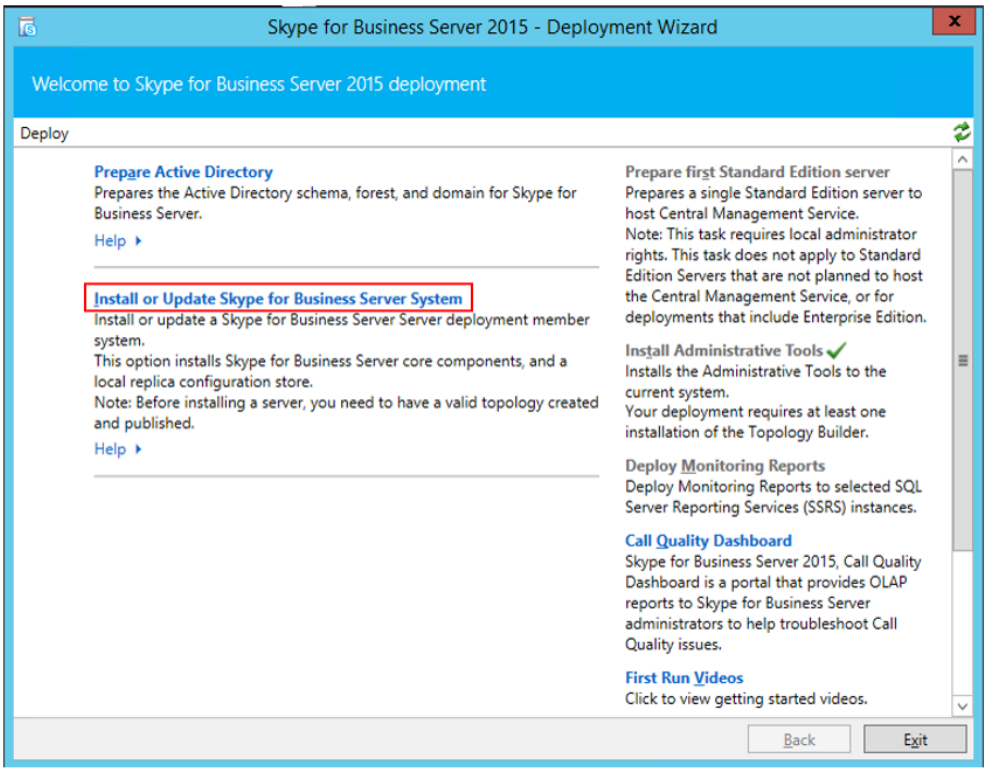
   - View the information of the SfB edge server in the Front End topology. The information includes whether or not the federation is enabled on the SfB edge server.



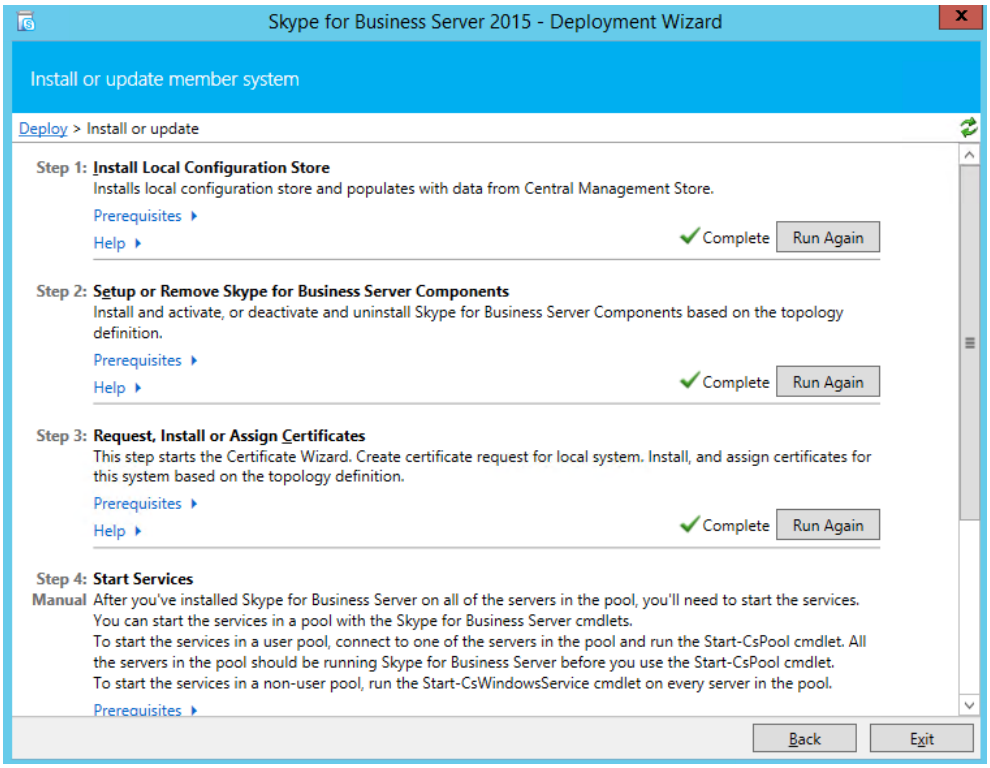
2. Make sure that the SRV record and the A record of both YMS and SfB are configured on the public DNS server.
   - Log into the public DNS server where the SfB edge server is located to view the SRV record and the A record. The host machine record must be_sipfederationtls_tcp in the SRV record.

A	sip	默认	110.87.96.5
A	sipexternal	默认	110.87.96.5
SRV	_sip._tls	默认	0 100 5061 sip.yealinksfb.com
SRV	_sipfederationtls._tcp	默认	0 100 5061 sip.yealinksfb.com
SRV	_sip._tcp	默认	0 0 5060 sip.yealinksfb.com

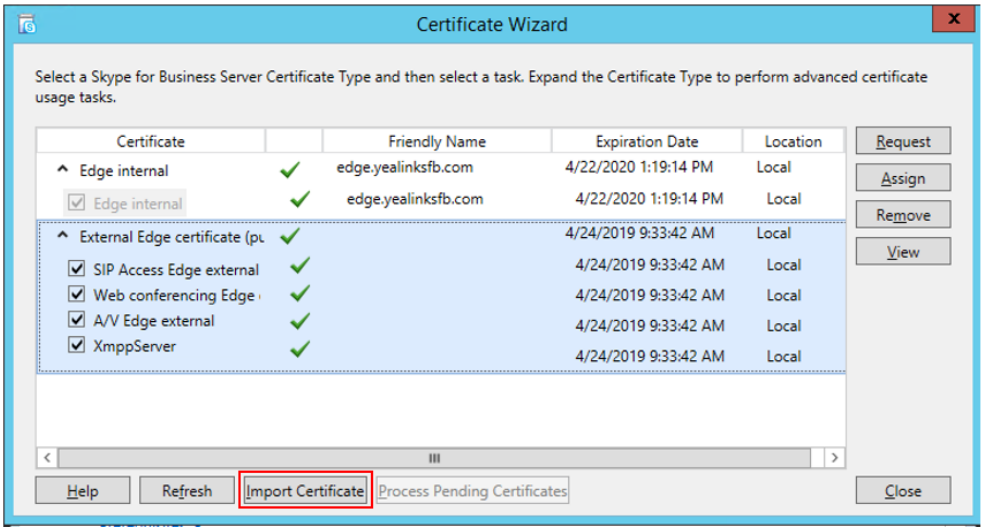
   - Log into the public DNS server where the YMS is located to view the SRV record and the A record. The host machine record must be_sipfederationtls_tcp in the SRV record.
3. Make sure that you purchase the certificate of the SfB edge server from a trusted third-party organization. The procedure of importing 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**.



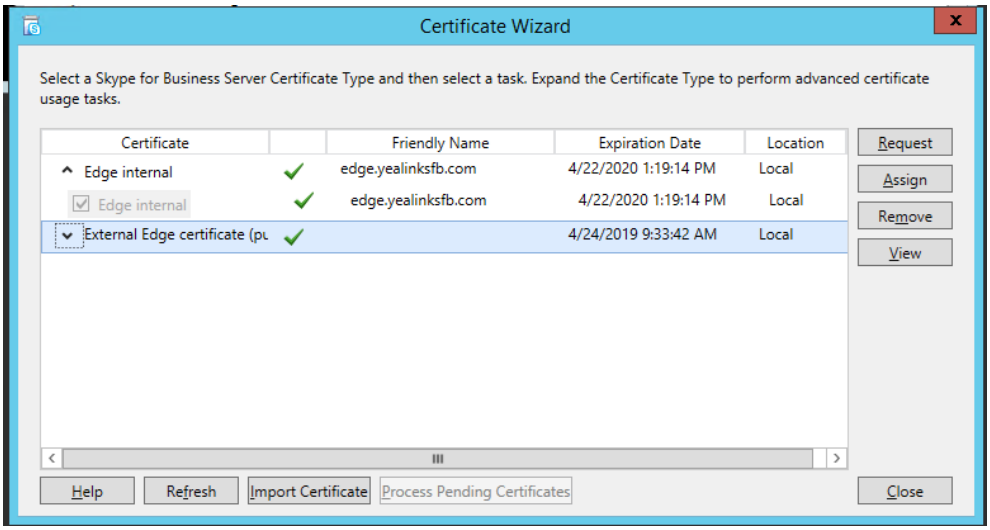
b) Click **Run Again**.



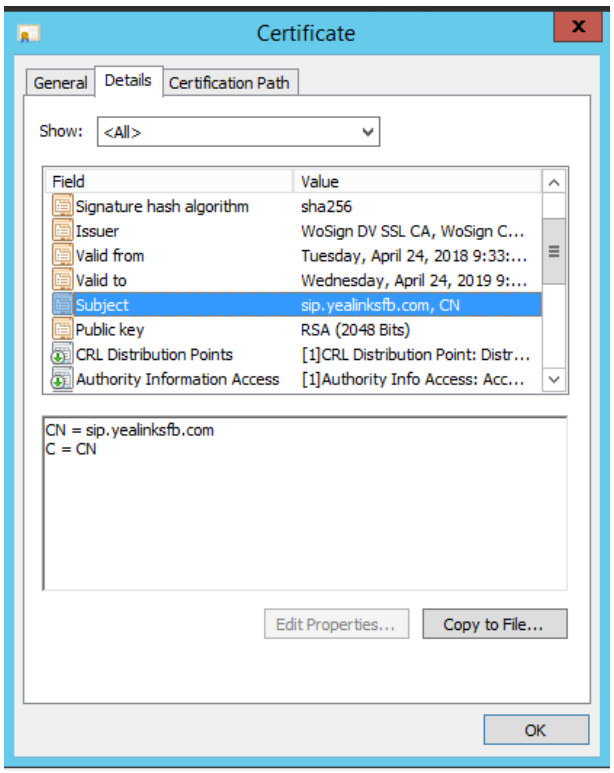
c) Click **Import Certificate** and import the external edge certificate.



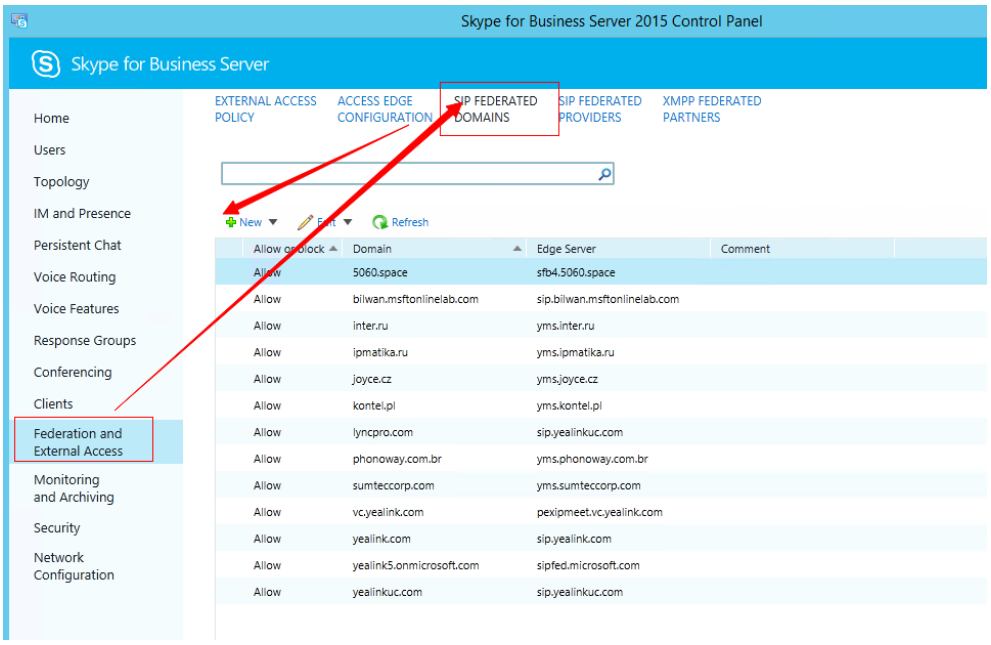
After importing, the page is shown as below:

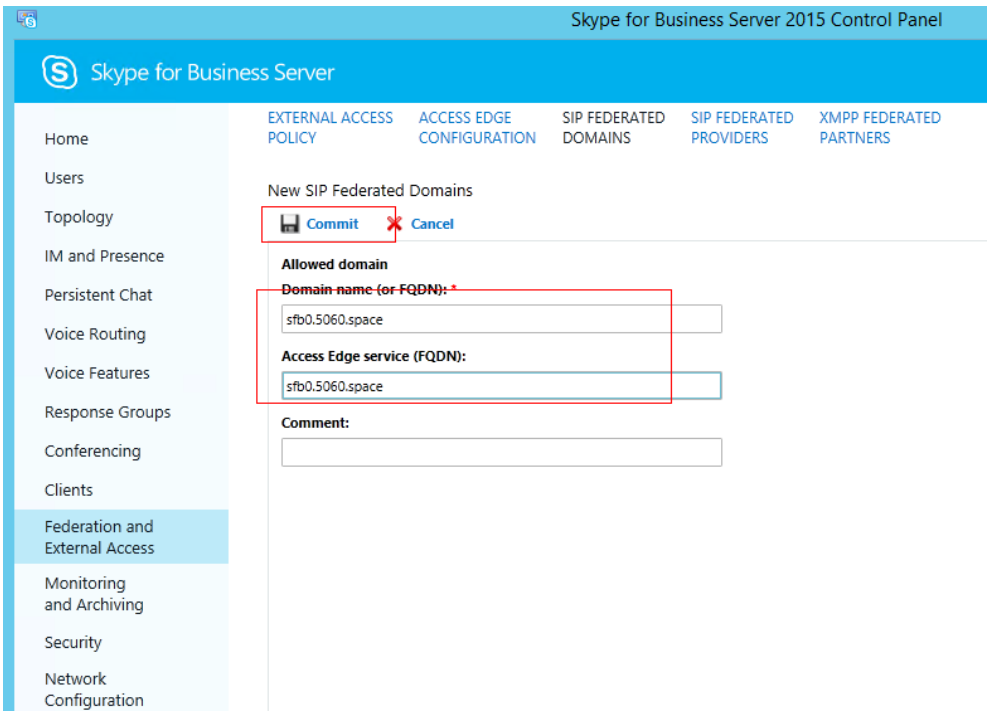


d) Select the imported edge server certificate, click **View**, and make sure that the user name (commonName attribute) or the user optional name (altNames attribute) must contain the FDQN name of the edge server.



4. Configure the federation information on the SfB and YMS.
   a) Open the Control Panel in the SfB Front End, click **Federation and External Access**, and add the YMS FQDN that connects to the SfB business node to the **SIP FEDERATION DOMAINS** field.





Configuring the SFB Service

To ensure calls can be routed to the specified SfB server, you need add a SfB gateway on YMS, to provide the destination gateway for the call routing.

Before you begin

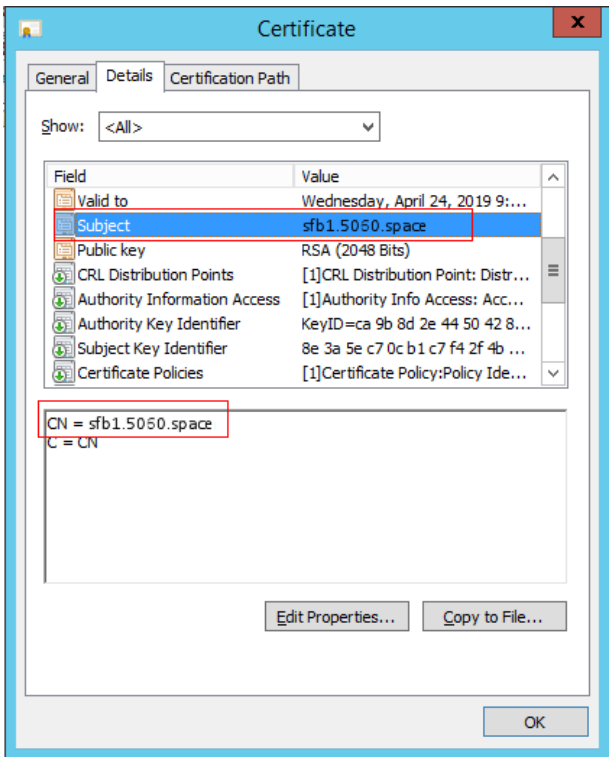
Make the SfB server trust this YMS by *Importing the TLS Certificate* on this YMS.

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 the 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
U0ZCMS41MDYwLnNwYWN1gg9TRkIyLjUwNjAuc3BhY2WCD1NGQjMuNTA2MC5zcGFj
ZYIPU0ZCNC41MDYwLnNwYWN1gg9TRkI1LjUwNjAuc3BhY2WCD1NGQjYuNTA2MC5z
cGFjZYIPU0ZCNy41MDYwLnNwYWN1gg9TRkI4LjUwNjAuc3BhY2WCD1NGQjkuNTA2
MC5zcGFjZTAdBgNVHQ4EFgQUxXmjM3vh1JEgQX2WpmFTpNEJZoowCwYDVR0PBAQD
AgXgMA0GCSqGSIb3DQEBBQUAA4IBAQBtp42PO5TXqPNvEqn1O4QcEBXbukKmErOq
CqxksUVyudOQ/5qqyd6x9KlM/6BmAS2Fi/1463PaoiQEZDAbDHw0UyAvisOyUDDw
WYEAYa2vIe2tvE/NW7TFysWgHPWcvjLN91wtLNDVjJkb7r4Et7//TnRc5oHL5ok9
En43cfZ3inev1HgFhne3C6iHVip5X4T7rZO5j9G51QYp9Jw4GwiCT2syP2DO10u/
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** > **Add**.
2. Configure the basic parameters.

Table 34: Basic Parameters

Parameter	Description
Enable	Enable or disable the SfB gateway server. **Default**: enabled.
Name	The name of SfB gateway.
Node	The node used by this SfB gateway.
Network	The IP address of this node.
Transport protocol	Only TLS is available if communicating with SfB.
FQDN	The name of YMS. Example: sfb1.5060.space **Method**: add this domain name on DNS server to which the A record of YMS is added.
Port	The source port on YMS that communicates with the 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 federation, this port should be 5061. First of all, change the registration port to other port, and make the port as 5061, otherwise the port will be closed by the firewall.
Domain	The domain name of SfB server. For example: xiamen.yealinksfb.com.
Port	The source port on the SfB server that communicates 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 federation.
Outbound proxy	Enable or disable it to allow the SfB server to send requests to the outbound proxy server. **Default**: disabled.

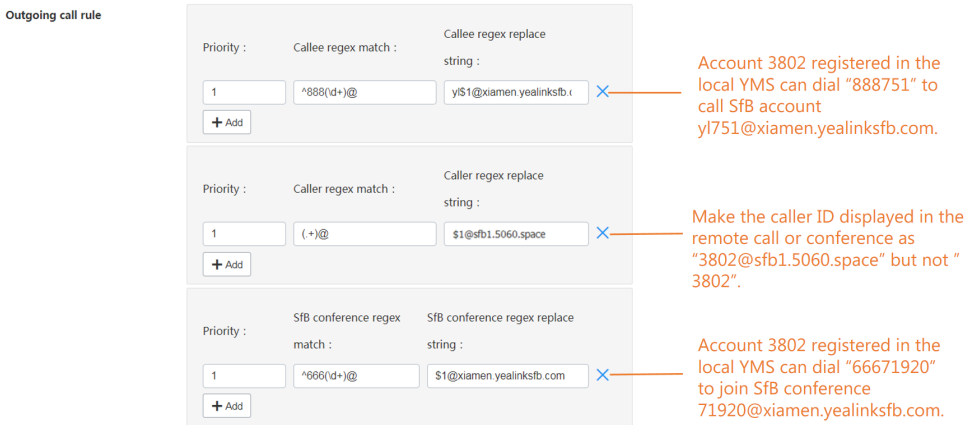
Parameter	Description
Proxy address	The IP address or the domain name of this outbound proxy server.
Proxy port	The port of this outbound proxy server. **Note**: the value can be any integer from 0 to 65535.
Support video	If you enable this, you can place video calls to the remote that supports video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

3. Configure the security policy.

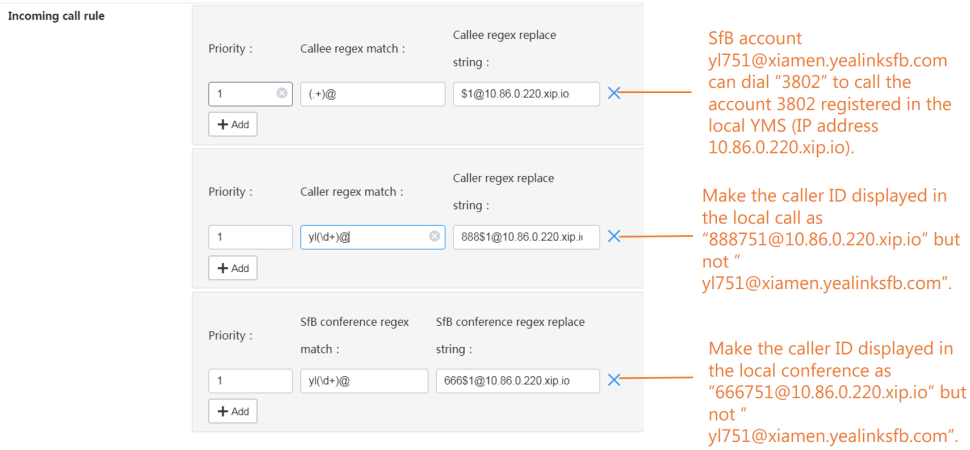
Table 35: Parameters of the Security Policy

Parameter	Description
Enable security policy	Enable or disable the security policy. **Default**: disabled.
Mode	Select a mode. The supported modes are as follows: • **Whitelist**: allow the security group of this SfB Server to call into. • **Blacklist**: forbid the security group of this SfB Server to call into.
Security Group	Select a security group.

4. Configure the outgoing call rule.



5. Configure the incoming call rule.



6. In the **SfB certificate** field, select the desired certificate to make the SfB server trust this YMS.
7. Click **Save**.
8. Operate according to the prompts, and click **OK**.

Related concepts

Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings

Related tasks

Adding a Security Group

Configuring 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** > **Add**.
2. Configure the basic parameters.

Table 36: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.
External media port	Configure the port range for the SFB gateway media service. **Default port range**: 61000-63999. To avoid the port conflict, the gap between the maximum port and the minimum port should be more than 200. For example, you set 61000 as the minimum port, and the maximum port should be more than 61199.
All local networks	The IP address used by this service.

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

Configuring the GK Service

You can configure the GK service for registering YMS accounts in the H.323 device, so that the H.323 devices can call each other, join conferences, and communicate with the SIP devices.

Procedure

1. Click **Service** > **H.323 Service** > **Embedded GK Server** > **Add**.
2. Configure the basic parameters.

Table 37: Basic Parameters

Parameter	Description
Enable	Allow the server to send registration request to the GK server or not. **Default:** enabled.
Name	The server name.
Node	The server
GK ID	The network ID of the GK server on which YMS is registered.
TTL timeout duration	After YMS is registered on the GK server, it will periodically send handshake messages (Registration Request) to the GK server to maintain the registration status. If the GK server does not receive the handshake messages when the time is out, it means this GK server does not exist, and the YMS will log out of this server automatically. **Default**: 600 seconds.
TTL timeout duration	The GK can decide whether or not the server can be called according to IRR (Information Request Response) sent by the server. **Default**: 120 seconds.
RAS broadcast port (UDP)	It defaults to 1718 and is not configurable.
RAS port (UDP)	It defaults to 1719 and is not configurable.
H.225 listening port (TCP)	It defaults to 1722 and is not configurable.
Q.931/H.245(TCP)	The range of the Q931/H.245 port. **Default port range**: from 20000 to 23999. 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 20000 as the minimum port, the maximum port should not be less than 20199.

Parameter	Description
Media forwarding port (UDP)	The port range of the media forwarding service. **Default port range**: from 20000 to 29999. 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 20000 as the minimum port, the maximum port should not be less than 20199.
H.225 listener	It defaults to 1721 and is not configurable.
Q.931/H.245(TCP)	Configure the range of the Q.931/H.245 port used by the conference gateway. **Default port range**: from 24000 to 26999. 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 24000 as the minimum port, the maximum port should not be less than 24199.
H.235 encryption	The supported types are as follows: • **Optional**—negotiate with the remote 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 cannot be used in H.323 calls. **Default**: Optional.
H.239	Enable or disable the H.239. **Default:** enabled. When the H.323 devices use H.323 protocol to request YMS to initiate a video conference, H.239 protocol is used to receive and send contents.
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 a lower compatibility. **Default**: disabled. If **Conference media ByPass** is enabled, Media bypass service should be enabled too. For more information, refer to *Configuring the Media Bypass Service* .

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

Configuring the H.323 Gateway

You can configure the H.323 gateway and add call routing rules (refer to *Adding a Call Routing Rule*), which can be used for the H.323 devices to join the conference via IP call (the listener port is 1720). You can also take the gateway as a device and register the gateway on the third-party GK server for communication.

Procedure

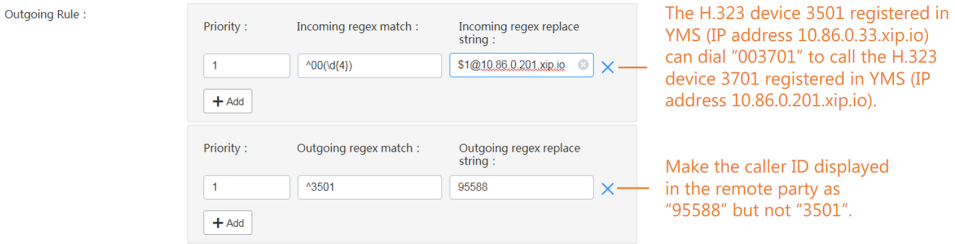
1. Click **Service** > **H.323 Service** > **H.323 Gateway** > **Add**.
2. Configure the basic parameters of the H.323 gateway.

Table 38: Basic Parameters

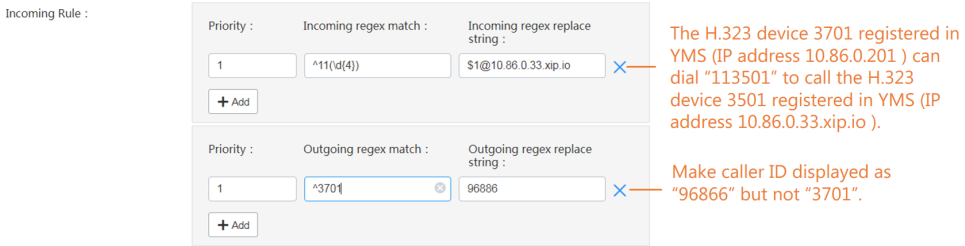
Parameter	Description
Enable	Enable or disable the H.323 gateway server. **Default**: enabled.
Name	The server name.
Node	The server.
Username	The authentication ID used by this gateway.
GK address	Configure the IP address and domain name of the GK server.
GK authentication	Enable or disable the GK authentication. **Default**: disabled.
GK auth name	Specify the account for the GK server authentication.
GK auth password	Specify the password for the GK server authentication.
H.225 listening port (TCP)	Configure the H.225 listening port. **Default**: 1720.
Q.931/H.245(TCP)	The range of the Q931/H.245 port. **Note**: the default port range is from 27000 to 29999. 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 27000 as the minimum port, the maximum port should not be less than 27199.

Parameter	Description
H.235 encryption	The supported types are as follows: • **Optional**—negotiate with the remote 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 cannot be used in H.323 calls. **Default**: Optional.
H.239	Enable or disable the H.239. **Default**: enabled. When the H.323 devices use H.323 protocol to request YMS to initiate a video conference, H.239 protocol is used to receive and send contents.
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 a lower compatibility. **Default**: disabled. If **Conference media ByPass** is enabled, Media bypass service should be enabled too. For more information, refer to *Configuring the Media Bypass Service* .

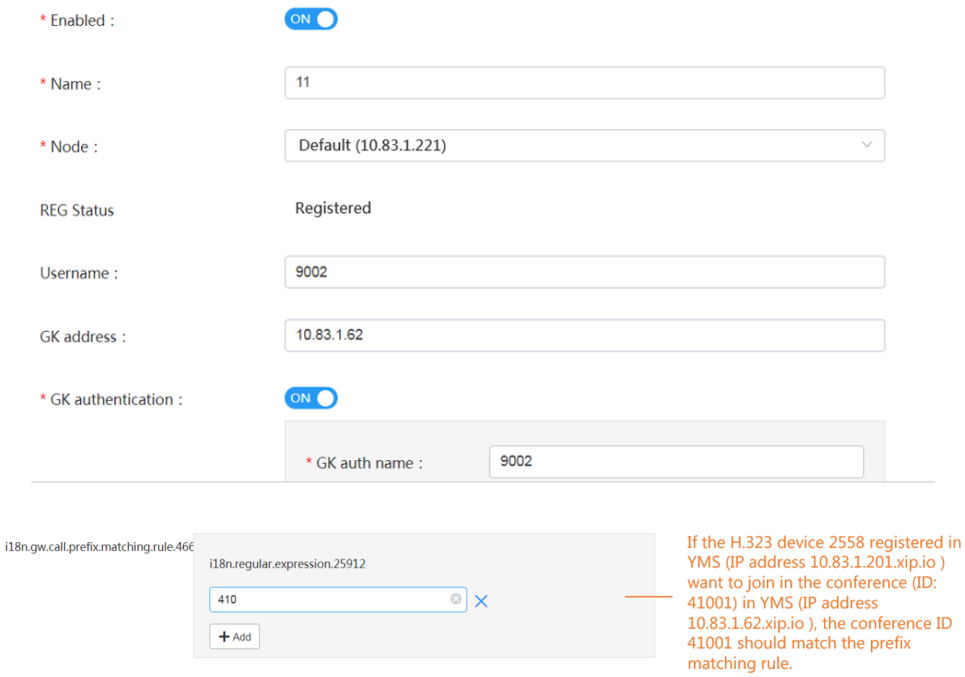
3. Click **Advance Option**, and configure the outgoing call rule.



4. Configure the incoming call rule.



5. If the gateway is as the device and registered on the third-party GK server, configure the GW prefix matching rules. The H.323 account on the server can directly call the conference ID to join the conference, but the conference ID should meet the prefix matching rule.



6. Click **Save**.
7. Operate according to the prompts, and click **OK**.

Note: If the H.323 devices fail to join conference by IP call, make sure that *Configuring the Interactive Media Service* is correct.

Related concepts

Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings

Configuring the Interactive Media Service

You need configure the interactive media service to ensure the user can join the conference.

Procedure

1. Click **Service** > **MCU Service** > **RTMP Media Service** > **Add**.
2. Configure the basic parameters of the interactive media service.

Table 39: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.

Parameter	Description
External media port	The port range of the interactive media service. **Default port range**: from 50000 to 54999. 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 50000 as the minimum port, the maximum port should not be less than 50199.
All local networks	The IP address used by this service.

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

Configuring the Broadcast Media Service

If you want to use the broadcasting interactive, you need configure the broadcast media service.

Procedure

1. Click **Service** > **MCU Service** > **Broadcast Media Service** > **Add**.
2. Configuring the basic parameters.

Table 40: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.
External media port	The port range of the broadcast media service. **Default port range**: from 55000 to 59999. 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 55000 as the minimum port, the maximum port should not be less than 55199.
All local networks	The IP address used by this service.

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

Related tasks

Enabling the Broadcasting Interactive

Configuring the RTMP Media Service

If you want to use the RTMP live broadcast, you need configure the RTMP media service.

Procedure

1. Click **Service** > **MCU Service** > **RTMP Media Service** > **Add**.
2. Configure the basic parameters.

Table 41: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.
External media port	The port range of the RTMP media service. **Default port range**: from 60000 to 60999. 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 60000 as the minimum port, the maximum port should not be less than 60199.
All local networks	The IP address used by this service. If the user logs into YMS via intranet IP to schedule conference and enable the live broadcast, you can select the intranet IP. If not, you can select the extranet IP.

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

Related tasks

Configuring the RTMP Live

Configuring the Media Bypass Service

When the number of servers exceeds the concurrent ports allowed in the certificate, and you want to make the server support a larger number participant, you can configure the media bypass service.

Before you begin

The media Bypass service in the SIP service and H.323 service is enabled.

Procedure

1. Click **Service** > **MCU Service** > **Media Bypass Service** > **Add**.
2. Configure the basic parameters.

Table 42: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.
External media port	The port range of the media bypass service. **Default port range**: from 64000 to 64999. 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 64000 as the minimum port, the maximum port should not be less than 64199.
All local networks	The IP address used by this service.

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

Adding the Recording Service

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

Before you begin

- *Activating a License* is done.
- The disk space of the node home directory used by this service should not be less than 50G.

Procedure

1. Click **Service** > **Recording Service** > **Add**.
2. Configure the corresponding parameters of the recording server.

Table 43: Basic Parameters

Parameter	Description
Enabled	Enable or disable this service. **Default**: enabled.
Name	The name of the server.
Node	The node used by this service.

Parameter	Description
External media port	The port range of the recording service. **Default port range**: from 65000 to 65499. 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 65000 as the minimum port, the maximum port should not be less than 65199.
All local networks	The IP address used by this service.

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

Configuring the Traversal Service

You need configure the traversal service for the network traversal of the call media. If the server is deployed in the intranet, you also need configure the traversal service to ensure that the device can place point-to-point call.

About this task

- If you use cluster YMS and all nodes are deployed in the intranet, you must add the traversal service on the master node.
- If you use cluster YMS and it need be available for the registration and joining conference both in the intranet and the extranet, you must add the traversal service on the business node (in both the intranet and the extranet). Adding the traversal service in only the intranet node is not allowed. If not, there will be an abnormal situation in the traversal service.

Procedure

1. Click **Service** > **Traversal Service** > **Add**.
2. Configure the basic parameters.

Table 44: Basic Parameters

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.
Listener (UDP & TCP)	Select the desired listener. **Default**: 3478.
Spare listener (UDP & TCP)	Select the desired spare listener. **Default**: 3479.

Parameter	Description
Relay port range	Configure the range of the range port. **Default port range**: from 40000 to 49999. 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 40000 as the minimum port, the maximum port should not be less than 40199.

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

Related concepts

Introduction of the Deployment Structure

Call Settings

- *Call Control Policy*
- *Video Display Policy*
- *Restricting the Dialed Number*
- *Call Routing Rule*

Call Control Policy

- *Setting the Video and the Content Resolution*
- *Configuring the Call Bandwidth*
- *Configuring the Max Video Parties per Conference*
- *Configuring the Max Audio-Only Parties per Conference*
- *Setting IVR language*
- *Configuring the Time for Joining Conference Beforehand*
- *Enabling Auto Dialing*
- *Enabling the Auto Redialing*
- *Enabling Play Sound When Participants Join*
- *Displaying the Native Video*
- *Setting the Last Participant Backstop Timeout*
- *Setting the Auto End Conference Without Moderator*
- *Enabling the Content Only*
- *Enabling Join with APP Awakened by Browser*
- *Enabling Receiving Ringtone Receipt*
- *Enabling External/Internal Network Access WebRTC Authentication*
- *Disabling the Roll Call Setting*
- *Configuring the iOS Push Address*
- *Enabling the Broadcasting Interactive*
- *Configuring the RTMP Live*
- *Enabling the Conference Recording*
- *Setting the QoS*

Setting the Video and the Content Resolution

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

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Configure the parameters of the video and the content resolution.

Table 45: Parameters of video resolution

Parameter	Description
Max video resolution	You can set the maximum video resolution. **Default**: 720P/30FPS.
Max content sharing resolution	Configure the maximum content sharing resolution. **Default**: 1080P/5FPS

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

Configuring the Call Bandwidth

According to the limit of enterprise bandwidth, you can limit the media bandwidth sent by YMS to conference participants. For example, if you set the call bandwidth as 2M and the bandwidth of a participant is 4M, when he joins the conference and his devices negotiate with the server, he can only receive the bandwidth of 2M.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. In **Max call bandwidth** field, select the desired bandwidth.
   Defaults to 2Mbps.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Configuring the Max Video Parties per Conference

You can limit the max audio-only parties per conference, to meet the concurrent needs of other important conferences. If the number of the video parties exceeds the max number, users cannot place video calls to join the conference (except the VMR).

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enter the desired number in the **Max video parties per conference** field.
   The default value is 1500 party.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Configuring the Max Audio-Only Parties per Conference

You can limit the max audio-only parties per conference, to meet the concurrent needs of other important conferences. If the number of audio-only parties exceeds the max number, users cannot place audio calls to join the conference (except the VMR).

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enter the desired number in the **Max audio-only parties per conference** field.
   The default value is 1500 party.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Setting IVR language

You can set the voice prompt language for IVR service.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Select a language from the drop-down menu of **Audio IVR language**.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Configuring 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.
   60 minutes in advance is by default.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Enabling Auto Dialing

You can enable **Auto dialing** feature. When the scheduled conference begins, the system will automatically place calls to the invited participants to join the conference. The invited participants are the YMS accounts registered on Yealink device or on third-party devices in the enterprise directory.

About this task

The supported devices are: PVT950/PVT980,VC880/VC800/VC500/VC400/VC200/VC120/VC200 video conferencing system, SIP VP-T49G IP phone, SIP-T58V IP phone and third-party devices.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Auto dialing**.
   It is enabled by default.
3. In the **Device** field, select the device type.
4. Click **Save**.

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

Enabling the Auto Redialing

During a scheduled conference, if the device you invite disconnects with YMS, you can enable the **Auto redialing**, so that the system can invite it to join the conference again after the account is registered in the device again.

Before you begin

Enabling Auto Dialing is done.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Auto redialing**.
   It is enabled by default.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Enabling Play Sound When Participants Join

If you want the system prompt a sound when a participant joins the conference, you can enable **Play sound when participants join**.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Play Sound When Participants Join**.
   It is enabled by default.
3. Click **Confirm**.
4. Operate according to the prompts, and click **OK**.

Displaying the Native Video

If you want to make all the participants in the conference can view the native video, you can enable **Display native video.**

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Display native video**.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Setting the Last Participant Backstop Timeout

If there is only the last participant in the conference, you can set the timeout, if the time is out, the conference will end automatically, so that you can manage the useless conference and free up the server resource.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Last participant backstop timeout**.
   It is enabled by default.
3. Configure the timeout.

The default value is 30 minutes.

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

Setting the Auto End Conference Without Moderator

When there is no moderator in the conference, you can set the system to end conference automatically to manage the useless conference and to free up the server resource.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Auto End Conference Without Moderator**.
3. Configure the timeout.
4. Click **Save**.
5. Operate according to the prompts, and click **OK**.

Enabling the Content Only

If you want the device that does not support dual-stream protocol receive the content, you can enable **Content only**. When the devices share content in a call, the device that do not support dual-stream protocol can only receive the content and the audio.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Content Only**.

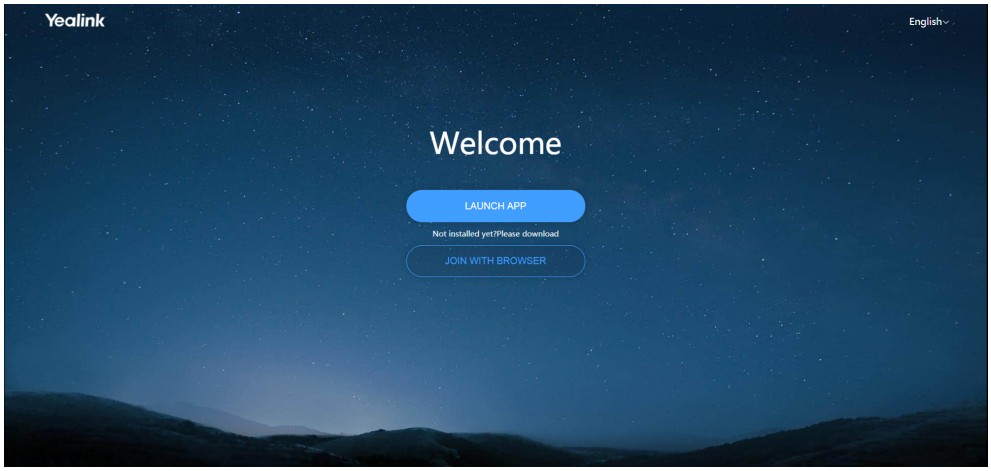
   It is enabled by default.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Enabling Join with APP Awakened by Browser

If you want to get the entrance to awake 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**.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Enabling Receiving Ringtone Receipt

If you want to hear the Ringback Tone of the callee in the PSTN (for example the fixed line) when the callee joins the conference, you can enable **Receiving ringtone receipt**.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Receiving ringtone receipt**.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Enabling External/Internal Network Access WebRTC Authentication

If you do not want the person who does not belong to your organization to join the conference, you can enable **External/Internal network access WebRTC authentication**, after you enable it, the user need YMS account and the password to join the conference via browser.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **External network access WebRTC authentication/Intranet access WebRTC authentication**.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Disabling the Roll Call Setting

By default, the participant whose name is called out is unmuted automatically. If other participants do not want to hear the called party, you can disable this setting.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Disable the **Roll call** .

   It is enabled by default.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Configuring the iOS Push Address

You can configure the iOS push address, so that 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

You use YMS account to log into Yealink VC Mobile for iOS.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. In the **iOS push address** field, enter the push address.
   Default: https://ios.push.yealinkvc.com:8443.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Enabling the Broadcasting Interactive

If you want to create a conference with a larger number of participants, you can enable the broadcasting interactive.

Before you begin

- You have enabled the broadcast license, refer to *Activating a License* .
- *Configuring the Broadcast Media Service* and *Configuring the Broadcast Media Service* are done.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Broadcasting interactive**.
3. Click **Save**.
4. Operate according to the prompts, and click **OK**.

Related tasks

Configuring the Broadcast Media Service

Related information

Activating a License

Configuring the RTMP Live

You can enable the **RTMP live** feature, so that users can stream the conference to live platform service and watch the live broadcast of the conference.

Before you begin

- You can obtain the information about Alibaba Cloud.
- *Configuring the RTMP Media Service* is done.

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 **RTMP live**.
3. Configure the parameters.

Table 46: RTMP live parameters

Parameter	Description
Organizer Logo	The logo displayed on the Live Broadcast page.
Domain	The domain name of the server.

Parameter	Description
Application name	The application name in the authentication URL.
Live domain	The live video domain name.
Enable GK authentication	Enable or disable the authentication. **Default:** disabled.
Authentication key	The authentication password.

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

Related tasks

Configuring the RTMP Media Service

Enabling the Conference Recording

If the **Recording** feature is enabled, you can configure the third-party recording server to record conferences.

About this task

Before you configure the third-party recording server, make sure Yealink technical support engineer have deployed the third-party recording server. If the recording server is deployed, you need obtain the corresponding information of the recording server from the Yealink technical support engineer.

Procedure

1. Click **Call Configuration** > **Call Control Policy**.
2. Enable **Recording**.
3. Enter the corresponding information of the recording server.
4. Click **Save**.
5. Operate according to the prompts, and click **OK**.

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 in the process of 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.
   The default value is 63.
4. Operate according to the prompts, and click **OK**.

Video Display Policy

- *Setting the Default Layout*

- *Setting Video Layout of 1+N*
- *Setting the Video Layout of Equal N×N*
- *Display participant name*
- *Display Participant Status*
- *Displaying the Participant Quantity*
- *Displaying the Audio-Only Participant*

Setting the Default Layout

You can set default video layout, which takes effect for participants in VMRs, participants in schedule conference of discussion mode and moderators in scheduled conference of training mode.

Procedure

1. Click **Call Configuration** > **Video Display Policy**.
2. Select a default layout.

Table 47: Parameters of the Default Layout

Parameter	Description
Default layout	The supported layouts are as follows: • **Equal N×N**: the video images of participants are displayed in equal parts. • **1+N**: the video image of the first participant who joins the conference is displayed in a large screen, and the video images of other participants are displayed in small screens around the first participant. **Default:** 1+N.

3. Click **Save**.

Setting Video Layout of 1+N

In the video layout of 1+N, if current participants exceeds 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. You can set the rules per carousel and the interval of auto-switching video images. You can use the voice-activated feature so that the system will automatically identify the speaking participant. When the participant continues speaking during the preconfigured voice-activated time, his video image will be displayed in the large screen, and the video images of other participants will be displayed in small screens.

Procedure

1. Click **Call Configuration** > **Video Display Policy**.
2. Configure parameters of 1+N Video Layout.

Table 48: Parameters of 1+N Video Layout

Parameter	Description
1+N	Configure the maximum video images of videos on screen. **Default:** 1+7.
	Set the carousel interval.

Parameter	Description
	Configure the number of video images per carousel. The maximum video image depends on the N in 1+N video layout.
	Configure the voice-activated time.

3. Click **Save**.

Setting the Video Layout of Equal N×N

In the video layout of Equal N×N, if current participants exceeds 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. You can set the rules for each carousel and the interval of auto-switching video images.

Procedure

1. Click **Call Configuration** > **Video Display Policy**.
2. Configure the Equal N×N video layout.

Table 49: Parameters of Equal N×N video layout

Parameter	Description
Equal N×N	Configure the maximum number of video images per screen in Equal N×N mode. **Default:** 4*4.
	Set the carousel interval.

3. Click **Save**.

Display participant name

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

Procedure

1. Click **Call Configuration** > **Video Display Policy**.
2. Enable **Display participant name**.
   It is enabled by default.
3. Click **Save**

Display Participant Status

If you want to view the status on the video image, for example the participant is muted or blocked, you can enable **Display participant status**.

Procedure

1. Click **Call Configuration** > **Video Display Policy**.
2. Enable **Display participant status**.
   It is enabled by default.
3. Click **Confirm**.

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**.
   It is enabled by default.
3. In the **Type** field, select the audio or video.
4. Click **Save**.

Displaying the Audio-Only Participant

If you want to display the audio-only participant 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**.
   It is enabled by default.
3. Click **Save**.

Restricting the Dialed Number

You can restrict the dialed number.

Restrict the dialed number: 1. *Add a Number Filter* is used to configure the dialed number; 2. *Adding a Call Routing Rule* specifies the service type used by the number filter rules.

- *Add a Number Filter*

Add a Number Filter

Procedure

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

Table 50: Basic Parameters

Parameter	Description
Enable	Enable or disable this rule. **Default**: enabled.
Name	The rule name.
Note	The additional description of this rule.

3. Click **Add**, configure the number filter, and click **OK**。

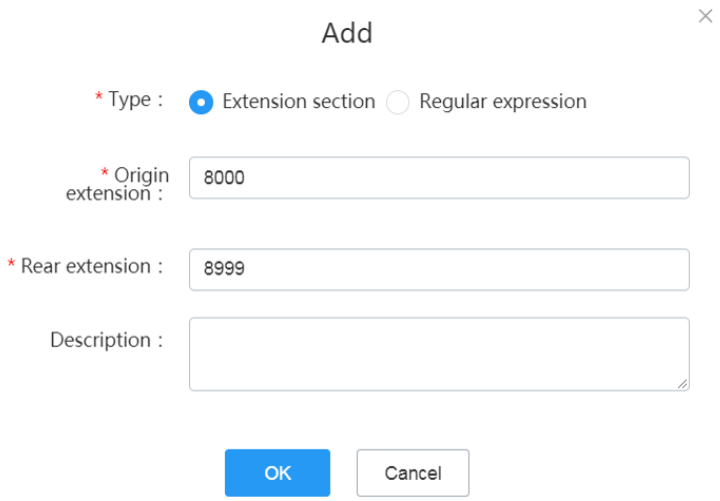


Table 51:

Parameter	Description
Type	The match type of this number. • **Extension section** • **Regular expression**
Origin extension, Rear extension	These two extensions should have the same length.
Regular expression	The Perl Compatible Regular Expressions (PCRE).
Description	The additional description of this rule.

4. Click **Save**.

Related concepts

Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings

Related tasks

Adding a Call Routing Rule

Call Routing Rule

When you place a call, the server will select the desired gateway according to your call routing rules, and send the request message. You can edit or delete call routing rules.

- *Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings*
- *Adding a Call Routing Rule*
- *Configuring the Call Routing Rule*

Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings

Table 52: Common Perl Compatible Regular Expressions (PCRE) are described as below:

PCRE	Description
^(1\d{10})$	Match the 11-digit number which starts with 1. For example: 12345678912
^0(\d+)$	Match the number (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}$	Match 11-digit mobile phone number, the first 3 digits includes the following types, the rest 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
^(\d{3,4}-)?\d{7,8}$	The format for matching the number is described as follows: • **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}	The format for matching the number is described as follows: • **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

PCRE	Description
(\d{11})|((\d{3,4})-)?(\d{7,8})(-(\d{1,4}))?	The format for matching the number is described as follows: • **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 53: Regex replace string

PCRE	Description
$1@$2	Take the parts of the first and the second parentheses in the PCRE. For example: the compatible 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** > **Add**.
2. Configure the parameters of the call routing rules.

Table 54: Parameters of the Call Routing Rule

Parameter	Description
Enable	Enable or disable the call routing rule. **Default**: enabled. All the disabled rules are ignored, though they are displayed in the rule list.
Name	The name of the call routing rule.
Priority	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 the priority in ascending order.

Parameter	Description
Destination regex match	The Perl Compatible Regular Expressions (PCRE) is used to match the target call number. If the match succeeds, the server will use this call routing rule.

3. If you want to restrict the number you call, enable **Caller filtering policy**, and configure the parameters.

Table 55:

Parameter	Description
Mode	Select a mode. The supported modes are as follows: • **Whitelist**: if a call number in this whitelist matches the target regular expression, it will be called by this call routing rule. • **Blacklist**: even if a call number in this blacklist matches the target regular expression, it will not be called by this call routing rule.
Caller filtering policy	Select the filtering policy.

4. Configure the parameter of the outgoing location.

Table 56:

Parameter	Description
Call target	The call target. The supported type are as follows: • **Reject** • **IP Call** • **Federation service** • **Peer Trunk** • **PSTN** • **SfB** • **Register Trunk** • **H.323 GW**
Outgoing location	The gateway used to place the call. If the call number matches this call routing rule, it is called via this gateway.

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

Related tasks

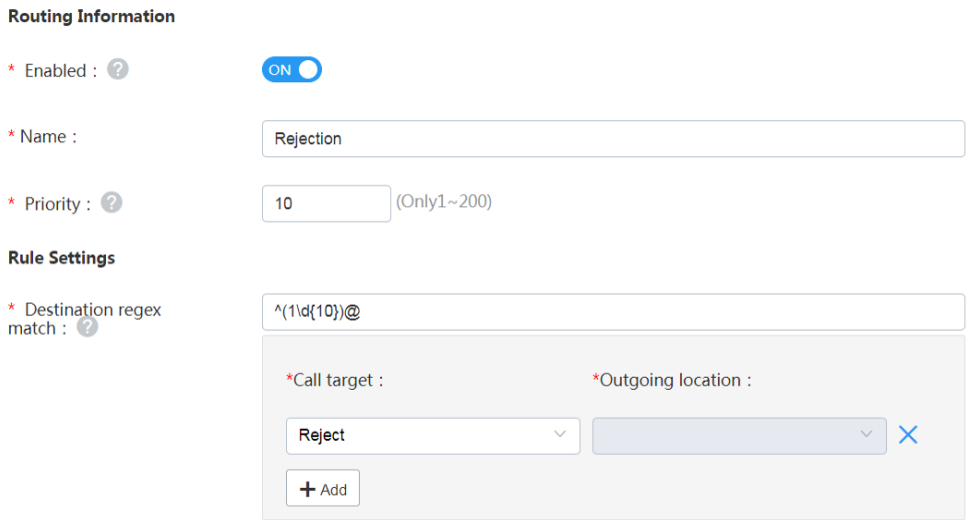
Add a Number Filter

Configuring the Call Routing Rule

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

Procedure

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



3. If you want to restrict the number you call, enable **Caller filtering policy**, and configure the parameters.

   For example, if you want to make the call to the YMS account (whose number is not within 5555 to 9999) be rejected, you can put the number within 5555 to 9999 into the blacklist. Otherwise, you can put the number into the whitelist.
4. In the **Call target** field, select **Reject**.
5. Click **Save**.
6. Operate according to the prompts, and click **OK**.

Managing the Recording

- *Showing the Recording Icon During Recording*
- *Parameters of the Recording Template*
- *Editing the Default Recording Template*
- *Adding the Recording Template*
- *Viewing the Application Object of the Recording Template*
- *Deleting the Recording Template*
- *Viewing the Usage*
- *Editing the Recording Parameters of User Account*
- *Managing the Recording Files*
- *Deleting Recording Files*
- *Copying the Sharing Link*
- *Disabling the Sharing Link*

Showing 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 **RSS Management** > **Recording Setting**.
2. Enable **Show the recording icon**.

Parameters of the Recording Template

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

Table 57:

Parameter	Description
Template name	The name of this template.
Video resolution	Set the maximum video resolution for the recording file. **Default**: 720P30fps.
Audio and video code rate	Set the maximum bandwidth for the recording file. **Default**: 768 Kbps.
Layout	Set the layout when recording. **Default**: 1+7.

Related concepts

Parameters of User Account

Parameters of Room System Account

Editing the Default Recording Template

After you successfully configure the recording server and enable the recording feature, the system will generate a default recording template and the template is enabled by default. You can edit the default recording template.

Procedure

1. Click **RSS Management** > **Recording Setting**.
2. Click ··· on the right of the default template.
3. Click **Modify Configurations**.
4. Edit the template parameters.
5. Click **OK**.

Adding the Recording Template

You can add the recording template and select the users whom this template is applied to.

Procedure

1. Click **RSS Management** > **Recording Setting**.
2. Click **Add Template**.
3. Configure the parameters of the recording template.
4. Click **Save**.
5. According to the prompts, click **OK**.
6. Select the desired users.
7. Click **Save**.

Viewing the Application Object of the Recording Template

You can view the application object of the custom recording template.

Procedure

1. Click **RSS Management** > **Recording Setting**.
2. Click ··· on the right side of the template.
3. Click **View application object**.

Deleting the Recording Template

Procedure

1. Click **RSS Management** > **Recording Setting**.
2. Click ··· on the right side of the template.
3. Click **Delete**.
4. Operate according to the prompts, and click **OK**.

Viewing the Usage

You can view the usage of the recording space of the user accounts and room system accounts, the number of the recording file and the number of the shared link.

Procedure

Click **RSS Management** > **Usage**.

Editing the Recording Parameters of User Account

You can edit the recording authority, the recording space and the template for the user accounts and the room system accounts.

Procedure

1. Click **RSS Management** > **Usage**.
2. On the right side of desired account, click .
3. Edit the recording parameters.
4. Click **Save**.

Related concepts

Parameters of User Account

Managing the Recording Files

You can view, edit and share the recording files created by all user accounts and room system accounts.

Procedure

1. Click **RSS Management** > **File Management** > **All files**.
2. Click the corresponding recording file.
3. Do the following:
   - Play the recording file.
   - Click on the right side of **Remarks,** and add the remark.
   - Click **Share URL** in the top-right corner, and share the link with others or set the link authority.
   - Click **Delete** in the top-right corner, and delete the recording according to the prompts.
   - Click **Conference file**, and click on the right side of the desired file to download it.
   - Click **Conference info**, and view the conference subject, ID, the start time, the location and the participants.

Related tasks

Copying the Sharing Link

Disabling the Sharing Link

Deleting Recording Files

You can delete the recording file of any account.

About this task

The account contains the user accounts and the room system accounts.

Procedure

1. Click **RSS Management** > **File Management**.
2. Select the desired recording files.
3. Click **Delete**.
4. Operate according to the prompts, and click **OK**.

Copying the Sharing Link

You can copy the link that are sharing and send it to the people who want to view the recording file.

Procedure

1. Click **RSS Management** > **File Management** > **Share URL**.
2. On the right side of desired link, click .

Related tasks

Managing the Recording Files

Disabling the Sharing Link

Before you begin

You share the link with others. Refer to *Managing the Recording Files* .

Procedure

1. Click **RSS Management** > **File Management** > **Share URL**.
2. On the right side of desired link, click .
3. Operate according to the prompts, and click **OK**.

Related tasks

Managing the Recording Files

Managing Accounts

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

- *User Accounts, Room System Accounts and Other Accounts*
- *Managing Groups*
- *Adding Accounts*
- *Sending an Email to a YMS Account*
- *Adjusting the Account Group*
- *Editing the Authority*
- *Editing the GK Registration Parameter*
- *Editing a Batch of Accounts*
- *Configuring the LDAP*

User Accounts, Room System Accounts 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. The same user account can log into 5 devices at most at the same time.	They are called as YMS accounts.
Room system account	The account is used to be associated with the device in the video meeting room. The same room system account can log into 5 devices at most at the same time.	
Other account	Enter the IP address or URL to add devices. It can be used to invite other devices during a conference. Those devices do not have 4-digit YMS accounts.	No limit.

Managing Groups

In order to manage users and other accounts by group, you can customize the group according to the enterprise organization.

The organization root is the enterprise name by default. You can manage users and other accounts of your group and the subordinate groups.

- *Adding a Group*
- *Editing/Deleting the Group*

Adding a Group

You can add groups according to enterprise department to make account management convenient.

Procedure

1. Click **Account** > **User Account/Other Account** > **Add Group**.
2. In **Group name** field, enter the group name.
3. In **Upper group** field, select a upper group.
4. Click **Save**.

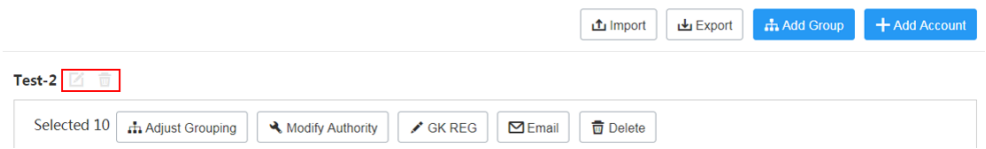
Editing/Deleting the Group

About this task

If the group has subordinated groups, you cannot delete this group.

Procedure

1. Click **Account** > **User Account/Other Account**.
2. In the Organization list, select the desired group, and click to edit this group or click to delete this group.



Adding Accounts

You can add user accounts, room system accounts and other accounts.

- *Parameters of User Account*
- *Parameters of Room System Account*
- *Parameters of Other Devices*
- *Adding an Account Manually*
- *Adding a Batch of Accounts*

Parameters of User Account

Before adding user account, you need to know parameters of the user account first.

Method	Parameter	Description
Adding Manually or adding in batch	**Name**	The user name.
	Account	The account to log into YMS.
	AD account	If **Obtain from AD server** is selected, specify the AD account which is used to obtain the AD account name and account number. The account on AD server can be obtained from the AD server administrator.
	Group	Name of the department to which the user belongs to.

Method	Parameter	Description
	Authority	The user authority. The available rights are as follows: • **A**: this account can see all user accounts, room system accounts, and VMRs synced to the directory. • **B**: this account can see only the user accounts, the room system accounts, and the VMRs (synced to the directory) in his group and in the same level group. If the user is in root node, this account can also see the third-party devices. • **C**: this account can see only the user accounts, the room system accounts, and the VMRs (synced to the directory) in his group. • **D:** this account can only see himself, and cannot see any meeting room when scheduling conferences. • **Custom**: you can customize the authority for this account.
	Email	The user email. It is used to receive the initial password and the conference notification.
Adding Manually	**Account Information**	If the LDAP feature is enabled, select the way to add account. The supported ways are as follows: • **Manual**: you need add account information manually. • **Obtain from AD server**: you can obtain the account information from the specified AD server.
	Obtain	Obtain the AD account name and account number from the specified account on AD server.
	Enable schedule	Enable or disable this account to schedule meeting room or video conference. **Default**: enabled.

Method	Parameter	Description
	Enable Meet Now	Enable or disable this account to create a Meet Now conference. **Default**: enabled.
	Enable call authority	If this feature is enabled, this account can only call the contacts which are visible to him. **Default:** disabled.
	Enable Recording	If this feature is enabled, this account can record the conference.
	Support H.323 registration	If *Configuring the GK Service* is done, you can enable or disable this account to use H.323 to register at a device. **Default:** disabled.
	GK REG	If this feature is enabled, the account need password to register in GK servers. **Note:** it is recommended to enable.
	Recording space	Set the maximum recording space for this account. If you select **Customization**, the maximum recording space cannot be larger than the storage space of the server. **Note**: no limit.
	Recording template	When this account is the organizer of the conference or the VMR, the recording template of the organizer is applied when recording. For more information, refer to *Parameters of the Recording Template* .
Adding in Batch	**Password**	You can customize the password.

Related tasks

Adding an Account Manually
Adding a Batch of Accounts
Configuring the LDAP
Editing the Authority

Parameters of Room System Account

You need to know the parameters before adding the room system accounts.

Method	Parameter	Description
Add manually or batch add	**Name**	The user name.

Method	Parameter	Description
	Name	The account required to log into the YMS.
	AD account	If **Obtain from AD server** is selected, specify the AD account which is used to obtain the AD account name and account number. The AD account can be obtained 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 account can only see the user accounts, the room system accounts, and the VMRs (synced to the directory) in his group and in the same level groups. If the user belongs to the root node, this account can also see the third-party devices. • **C**: this account can only see the user accounts, the room system accounts, and the VMRs (synced to the directory) in his group. • **D**: this account can only see himself, and cannot see any meeting room when scheduling conferences. • **Custom**: you can customize the authority for this account.
	Email	The email address of the user. This email address is used to receive the initial password and the conference notifications.

Method	Parameter	Description
Add manually	**Account Information**	If the LDAP feature is enabled, specify the way of adding accounts. The available ways are as below: • **Manual**: add names and accounts manually. • **Obtain from AD server**: according to the AD account you specified, you can obtain names and accounts from AD server.
	Obtaining account information	Obtain the name and number of AD account from the specified account.
	Enable schedule	Allow or refuse this account to schedule conferences. **Default**: enabled.
	Enable Meet Now	Allow or refuse this account to create Meet Now conferences. **Default**: enabled.
	Enable call authority	If this feature is enabled, this account can only call the contacts which are visible to him. **Default:** disabled.
	Enable Recording	If this feature is enabled, this account can record the conference.
	Recording space	Set the maximum recording space for this account. If you select **Customization**, the maximum recording space cannot be more than the storage space of the server. **Note**: no limit.
	Recording template	When this account is the organizer of the conference or the VMR, the recording template of the organizer is applied when recording. For more information, refer to *Parameters of the Recording Template* .
Batch add	**Password**	Customize the password for YMS accounts.

Parameters of Other Devices

Before adding other devices, you need know parameters of other devices.

Table 58: Parameters of Other Devices

Parameter	Description
Name	The name of this device.
Protocol	The call protocol used by the device.
Number	The URL of this device.
Group	The name of the group to which the device belongs.
Email	The email address of the device owner. This email is used to receive conference notifications.

Related tasks

Adding Other Account Manually
Adding a Batch of Other Accounts

Adding an Account Manually

If you can add an account manually.

Procedure

1. Do one of the following:
   - If you want to add user accounts, click **Account** > **User Account** > **Add Account**.
   - If you want to add room system accounts, click **Account Management** > **Room System Account** > **Add**.
   - If you want to add other accounts, click **Account** > **Other Account** > **Add Account**.
2. Configure the account parameters, and save them.
3. If you enter the email address, click **Send email**, the account information will be sent to the user by email.
4. Click **OK**.

Note: If you do not add email addresses when adding the user or room system accounts, you need send the initial passwords to the corresponding users, and remind them to change the passwords promptly.

Related concepts

Parameters of User Account

Adding a Batch of Accounts

If you want to add a batch of accounts at the same time, you can import the accounts by the template (excel file). Note that you cannot customize the template, you need to download a blank template.

Procedure

1. Click **Account** > **User Account/Room System Account/Other Account** > **Import**.
2. Click **Download Template** to download the template.
3. Enter the account parameters in the template and save it to your computer.
4. Click the field in the dotted box, and select the desired excel file to upload.
5. Click **OK**.

Related concepts

Parameters of User Account

Sending an Email to a YMS Account

You can send the YMS account information to the specified user by email.

Procedure

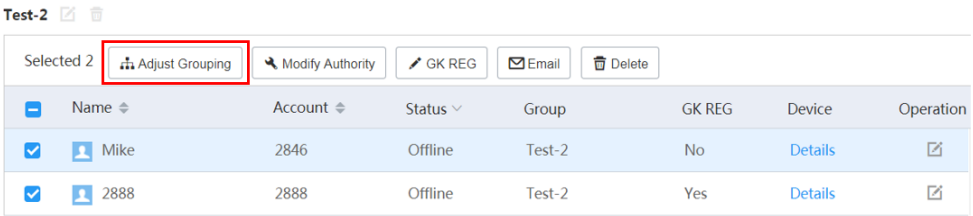
1. Click **Account** > **User Account/Room System Account** .
2. Select the desired account, and click **Email**.

Adjusting the Account Group

If the group of the user accounts and other accounts changes, you can adjust the group.

Procedure

1. Click **Account** > **User Account/Other Account**.
2. Select the desired meeting room, and click **Adjust Grouping**.



3. Select the group, and click **Save**.

Editing the Authority

You can configure the visible account range for the user accounts and the room system accounts, the scheduling conferences authority, the creating Meet Now conferences authority, and the call authority.

Procedure

1. Click **Account** > **User Account/Room System Account** .
2. Select the desired account, and click **Modify Authority**.
3. Edit the authority parameters.
4. Click **Save**.

Related concepts

Parameters of User Account

Related tasks

Adding a Room System Account

Editing the GK Registration Parameter

You can edit the GK registration parameter of the user accounts and the room system account. GK registration parameter includes whether or not the account can be registered in the device by H.323 protocol, and whether or not the account need the password to register in the GK server.

Procedure

1. Click **Account** > **User Account/Room System Account** .
2. Select the desired account, and click **GK REG**.
3. Configure the GK registration parameter.
4. Click **Save**.

Editing a Batch of Accounts

If you want to edit a batch of user accounts or other accounts, you can export excel file of all user account or other accounts, and download it on your computer, edit details in the excel file and import the edited file.

About this task

If you add a batch of user accounts and other accounts by importing template, you can edit account details in the template, and import this template to YMS to complete editing.

Procedure

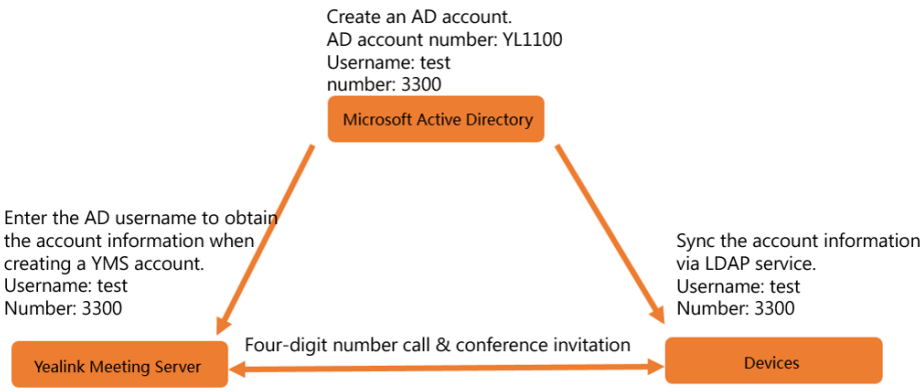
1. Click **Account** > **User Account/Other Account** > **Export**.
2. Edit the parameters in the exported file.
3. Click **Import**.
4. Click the field in the dotted box, and select the desired excel file to upload.
5. Click **OK**.

Configuring the LDAP

You can connect YMS to LDAP server that supports LDAPv3, so that the devices which register in YMS by standard SIP/H.323 can obtain YMS contacts. Microsoft Active Directory is supported by YMS.

About this task

Because the AD server can only be read, the accounts should be created on both YMS and AD server and be associated with each other. Take the image below as an example: the accounts created on AD server and the accounts created on YMS, they should follow the same rule to create their account names and account numbers. The account name should be less than 64 characters, and the account number should be within the number range of the system account (refer to *Allocating the Number Resource*). When creating an account on YMS, you can enter the corresponding AD account, and the system can get the account information automatically from AD server. The device registered in YMS can sync the YMS contacts from AD server to realize the 4-digit number call among YMS contacts, the conference invitation and so on.



Note: When the AD server administrator edits the AD account number and account name, the corresponding account on YMS will sync the account name but not the account number.

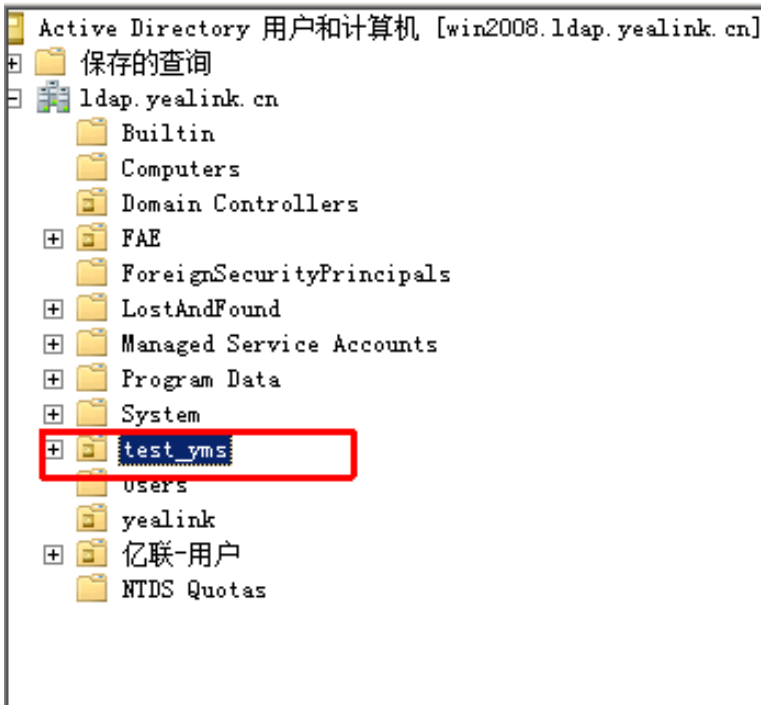
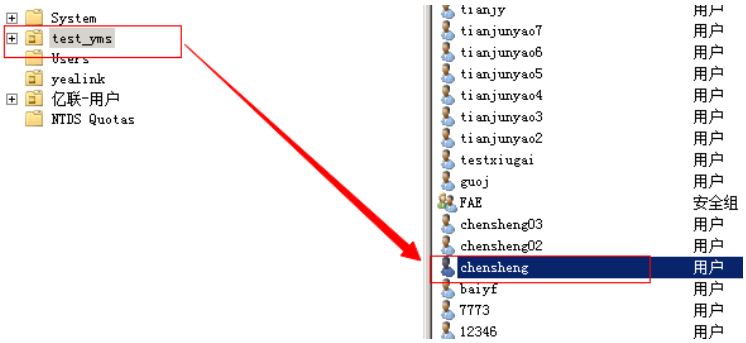
The organizational structure of YMS and LADP server are independent. If you want to edit the organizational structure, the organizational structure viewed by the third-party devices should be edited via AD server, and the organizational structure viewed by YMS devices should be edited via YMS.

Procedure

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

Table 59: LDAP parameters

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

Parameter	Description
Base DN	The root path of YMS obtaining the AD account. **For example**: OU=test_yms,DC=ldap,DC=yealink,DC=cn **Obtaining method**: the image below is the contents of AD server, if YMS wants to obtain the user information under this contents, right click test_yms->Attribute->Attribute Editor->View distinguishedname, and the value is OU=test_yms,DC=ldap,DC=yealink,DC=cn. Enter the value in the **Base** field on YMS. 
Username	The username used to log into the AD server. **Note**: The user name is provided by the AD server administrator. For example, the “chensheng” account in the test_yms contents. The user in in the test_yms contents is all acceptable. Username is “chensheng@ldap.yealink.cn”. 

Parameter	Description
Password	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 attribute	The returned name attribute of AD account. **Example**: name or cn. For example, when the name attribute is name and when you create a YMS account by obtaining from the AD server, the YMS account name equals to the corresponding value of AD user name attribute.
Number attribute	The number attribute of each record to be returned by the LDAP server. **Example**: telephoneNumber, mobile, or ipPhone and so on, when the number attribute is telephoneNumber and when you create a YMS account by obtaining from the AD server, the YMS account number is the corresponding value of AD account telephoneNumber attribute. In additionally, the corresponding value of telephoneNumber 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 the condition, there will be an error when creating a YMS account by obtaining from the AD server.
AD account attribute	The account attribute in AD server. **Example**: sAMAccountName

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

Related concepts

Parameters of User Account

Managing Meeting Rooms

You can view, edit and delete entity meeting rooms and VMRs.

- *The Entity Meeting Room and the Virtual Meeting Room*
- *Managing Groups of Meeting Room*
- *Adding a General Meeting Room*
- *Adding a Video Meeting Room*
- *Discussion Mode and Training Mode*
- *Adding a VMR*
- *Adjusting the Meeting Room Group*
- *Sending Emails About Joining the Conference*

The Entity Meeting Room and the Virtual Meeting Room

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

Difference	Type	Description	
Definition	**Entity meeting room**	The entity meeting rooms can be used to schedule OA conferences. For more information, refer to *Yealink Meeting Server User Guide*.	
	VMR	Users can join the VMR at any time. But the VMR cannot be used to schedule conferences.	
Classification	**Entity meeting room**	**General meeting room**	The general meeting room is not deployed with devices.
		Video meeting room	The video meeting room is deployed with devices.
	VMR	No	

Managing Groups of Meeting Room

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 Groups of Meeting Room*
- *Editing/Deleting the Meeting Room Group*

Adding Groups of Meeting Room

You can add groups according to the location of meeting room.

Procedure

1. Click **Meeting Room** > **Entity Meeting Room/Virtual Meeting Room** > **Add Group**.
2. In the **Name** field, enter the group name.
3. In the **Group** field, select the upper group.
4. Click **Save**.

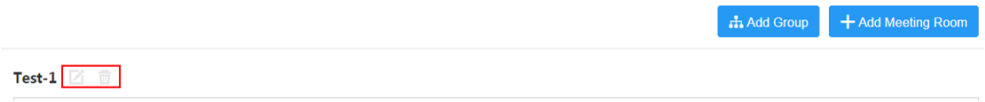
Editing/Deleting the Meeting Room Group

About this task

If the group has subordinated groups, you cannot delete this group.

Procedure

1. Click **Meeting Room** > **Entity Meeting Room/Virtual Meeting Room**.
2. In the Organization list, select the desired group, and click to edit this group or click to delete this group.



Adding a General Meeting Room

If the user wants to initiate conferences in an entity meeting room without devices, you can add a general meeting room.

Before you begin

You add the meeting room group.

Procedure

1. Click **Meeting Room** > **Entity Meeting Room** > **Adding Meeting Room**.
2. In the **Type** field, select **Common**.
3. In the **Name** field, enter the meeting room name.
4. In **Group** field, select the desired group.
5. Click **Save**.

Adding a Video Meeting Room

If the user wants to initiate conference in an entity meeting room with devices, you can add a video meeting room.

Before you begin

You add the meeting room group.

Procedure

1. Click **Meeting Room** > **Entity Meeting Room** > **Add Meeting Room**.
2. In **Type** field, select **Video**.
3. In the **Name** field, enter the meeting room name.
4. In **Group** field, select the desired group.
5. Select the desired account from the drop-down menu of **Account bound**.
6. Click **Save**.

Discussion Mode and Training Mode

The differences between these two modes are listed as below:

Table 60:

Difference	Discussion Mode		Training Mode	
Participant Role	**Moderator**	You can set any participants in the enterprise directory as moderators.	**Moderator**	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.
	Guest	It refers to the participants who join the VMR but are not set as moderators.	**Lecturer**	Moderators can set any moderators or guests as lecturers during the conference.
			Guest	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.
Feature Privilege	Moderators can configure the layout during the discussion mode conferences or meet now conferences.		Moderators can configure the layout in the training mode conference, they can also allow/reject the participant application for speaking, make the roll call, export the roll call result, and switch the roles between lecturers and moderators/guests.	
	Moderators can edit conferences and delete conferences, and during the conference, they can also send messages, invite participants, invite participants by email, invite the third parties, share the conference information, call participants, call participants from the call history, hang up participants, move the participants into the waiting center, allow/reject the participant to join the conference, mute/unmute participants, turn on/off the camera, block/unblock the voice, switch the roles between the moderators and guests, control the far-end camera, lock or unlock conferences, view the conference recording, turn on/off RTMP Live,			
	Other participants can only view the conference details.			

Difference	Discussion Mode	Training Mode
Layout	Moderators and guests can view all participants. For setting the default layout, refer to *Setting the Default Layout* .	• The moderators can view all participants by default. For setting 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 guest, all lecturers are given equal prominence in the layout by default. If there is no lecturer, all guests can view the reminder of waiting for the lecturer. If broadcasting interactive feature is enabled, the broadcasting parties will see that all lecturers are displayed in equal video images 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. After cancelling the mute status, the moderators can speak. Guests can speak only when the moderators allow their application for speaking.
Contents	All moderators and guests can share contents by default.	Only moderators and lecturers can share contents. Guests cannot share contents.

Related tasks

Adding a VMR

Adding a VMR

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

Before you begin

The meeting room group is added.

Procedure

1. Click **Meeting Room** > **Virtual Meeting Room** > **Adding Meeting Room**.
2. Configure the parameters of VMR.

Table 61: Parameters of VMR

Parameter	Description
Mode	The mode of the VMR. For more information, refer to *Discussion Mode and Training Mode* .
Conference ID	The conference ID used to call into this meeting room. **Default range**: from 20000 to 89999.

Parameter	Description
Password	Enable or disable the password required to join the conference. If it is enabled, a password is required to join the conference. **Default:** disabled.
Group	The group name of this meeting room.
Moderator	They can control the VMR at any time. For more information, refer to *Yealink Meeting Server User Guide*.
Favorites	During a conference, users can call the desired favorites to invite them to join the VMR.
Sync contacts	Sync this meeting room to the device enterprise directory or not. **Default:** enabled.
Max video parties	The max video parties of this meeting room. Reserving the video party can meet the concurrent needs of other important conferences. If the number of video parties in this meeting room exceeds the max number, the user cannot place a video call to this meeting room.
Max audio-only parties	The max audio-only parties of this meeting room. Reserving the audio party can meet the concurrent needs of other important conferences. If the number of audio-only parties in this meeting room exceeds the max number, the participants cannot place an audio call to this meeting room.
Max video resolution	The max video resolution. **Default**: 720P/30FPS.
Max content resolution	The max content resolution. **Default**: 1080P/5FPS
Max call bandwidth	According to the limit of the enterprise bandwidth, you can limit the media bandwidth sent by YMS to conference participants.
Default layout	The default layout, which takes effect for the participants in VMRs of discussion mode and for the moderators in VMRs of training mode.
Display native video	Enable or disable the native video to be displayed in the conference. **Default:** disabled.
Content Only	If the device does not support dual-stream protocol, you can enable **Content only** feature. When other devices share contents in a call, this kind device can only receive the content and the audio. **Default**: enabled.

Parameter	Description	
Roll call setting	In **Training** mode, enable it to unmute the participant whose name is called out on the list or not. If the participants do not want to hear the voice of the participant whose name is called out on the list, you can disable the **Roll call setting**. **Default**: enabled.	
Broadcasting interactive	In **Training** mode, enable it to create a broadcasting interactive conference or not. If it is enabled, you can create a conference with a large number of participants.	
RTMP Live	Enable or disable the RTMP live broadcast. If it is enabled, the users can watch the live broadcast of the conference. **Default**: disabled.	
	Definition	It refers to the video resolution that the specified MCU sends to live streaming platform. The supported video resolution are as below: • **HD**: 720p. • **SD**: 360p. **Default**: HD.

Parameter	Description	
	Video options	Supported video options are as follows: • **Receive video and content**: when the participants share contents, the Live page will be displayed in 1+4 layout with the contents displayed in a large screen and the video images of all participants displayed in small screens, and the video images of all participants take part in carousel in the small screen. When there are no contents, the Live page is the same as **Receive video only**. • **Receive video only**: when in discussion mode conferences, the video images of all participants are displayed in the Live page by default but the contents are not displayed. This layout depends on the conference layout set by moderators when they control the conference (refer to *Controlling the Conference*). When in training mode conferences, the video images of all lecturers are displayed in equal parts in the Live page by default but the contents are not displayed. This layout depends on the conference layout set by moderators when they control the conference (refer to *Controlling the Conference*). • **Receive content only**: only the content is displayed on the Live page. **Default**: Receiving video and content.
	Event details	It refers to the text displayed on the Live page.

Parameter	Description
IP Call Blacklist	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.

Table 62: Advanced Option

Parameter	Description
Video port resource reservation	To ensure that the important conferences can proceed successfully without being occupied by other conferences, you can enable this configuration to reserve video ports. **Default**: 3. The maximum number of the video port resource reservation cannot exceed the total number of the video port and the broadcasting port that are available in the license.
Recording Privilege	Specify the desired participant that has the privilege to record the conference.
Recording files owner	For the recording generated during the conference in this VMR, the applied recording template is based on the owner's recording template, and the recording file is saved in the owner's personal folder after the recording is finished. **Note**: when the recording file owner is deleted, the recording template of this VMR uses the default template and the generated recording files are managed by the administrator.

3. Click **Save**.

Related concepts

Discussion Mode and Training Mode

Adjusting the Meeting Room Group

If the group of the entity meeting rooms and the VMRs change, you can adjust the group.

Procedure

1. Click **Meeting Room** > **Entity Meeting Room/Virtual Meeting Room**.
2. Select the desired meeting room, and click **Adjust Grouping**.
3. Select the group, and click **Save**.

Sending Emails About Joining the Conference

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

Procedure

1. Click **Meeting Room** > **Virtual Meeting Room**.
2. Click icon on the right side.
3. Configure the email information.
4. Click **Send**.

Managing Conferences

You can view, delete and control video conferences. The video conferences include scheduled conferences, Meet Now conferences and VMRs.

- *Viewing the Conference*
- *Viewing the Meeting Room Usage*
- *Monitoring the Conference*
- *Deleting a Conference*
- *Controlling the Conference*

Viewing the Conference

You can view the ongoing conference, the scheduled conference that can join in advance (refer to *Configuring the Time for Joining Conference Beforehand*) and the free VMRs. Conference information contains the subject, the type, the number, the password, the organizer, the start time and the duration.

Procedure

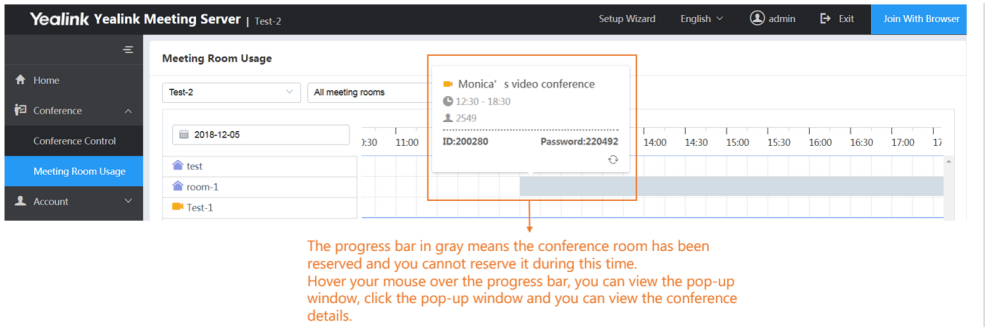
Click **Conference** > **Conference Control**.

Viewing the Meeting Room Usage

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**.



Monitoring the Conference

You can monitor the unoccupied VMRs, the ongoing conference, and the scheduled conference that can join in advance (refer to *Configuring the Time for Joining Conference Beforehand*). You can subscribe to this service from Yealink technical support.

- *Going to the Conference Monitoring Page*
- *Adjusting the Output Volume*
- *Selecting an Audio Output Device*
- *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*
- *Changing Video Layouts*
- *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 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 desired conference, click ⊙ to go to the Conference Monitoring page.

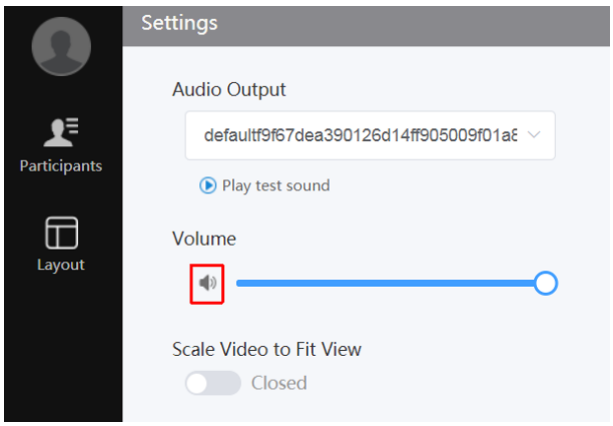
Adjusting the Output Volume

Before you begin

Going 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 conference monitor.
3. Click the icon below to mute the device.



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

Going to the Conference Monitoring page via Chrome.

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.

Changing the Display Language

The supported languages are Simplified Chinese, Traditional Chinese, English, Russian, Polish, Spanish and Portuguese.

Before you begin

Going 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

Going 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

Going 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

Going to the Conference Monitoring page.

Procedure

1. Click **Participants**.
2. Select the desired participant, and click **Zoom In**/**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

Going to the Conference Monitoring page.

Procedure

1. Click **Settings**.
2. Enable **Scale Video to Fit View**.

Changing Video Layouts

- *Hiding/Showing the Conference Video*
- *Switching Between the Video Window and the Content Window*

Hiding/Showing the Conference Video

You can hide or display the conference video.

Before you begin

Going to the Conference Monitoring page.

About this task

By default, when participants are sharing contents, the received content is displayed in a large window, the video is displayed in a small window in the bottom-left corner.

Procedure

Click in the right-corner of the 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 contents, the received content is displayed in a large window, and the video is displayed in a small window in the bottom-left corner.

Before you begin

Going 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 in the small window.

The video will be displayed in a large window, and the received content is displayed in a small window 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 exit the full screen.

Before you begin

Going to the Conference Monitoring page.

About this task

By default, the conference video is displayed in window.

Procedure

Do one of the following:

- Click **Full Screen**/**Exit Full Screen**.
- Double click the large window to display it in full screen or exit the full screen.

Deleting a Conference

You can delete the ongoing conference and the scheduled conference that can join in advance (refer to *Configuring 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 delete the recurrence conference, click **Cancel occurrence**/**Cancel series**.
4. If you want to delete a single conference, click **OK**.

Controlling the Conference

You can control the unoccupied VMRs, the ongoing conference, and the scheduled conference that can join in advance (refer to *Configuring the Time for Joining Conference Beforehand*) as the moderator. The conference control includes configuring the conference layout, configuring messages, managing conference participants and so on.

Procedure

1. Click **Conference** > **Conference Control**.
2. Select **Ongoing**, **Scheduled**, and **VMR**.
3. On the right side of desired conference, click to go to the Conference Control page.
4. Control the conference. For more information, refer to *Yealink Meeting Server User Guide*.

Conference Statistics

You can view the call statistics, the MCU usage, and the records of different call types.

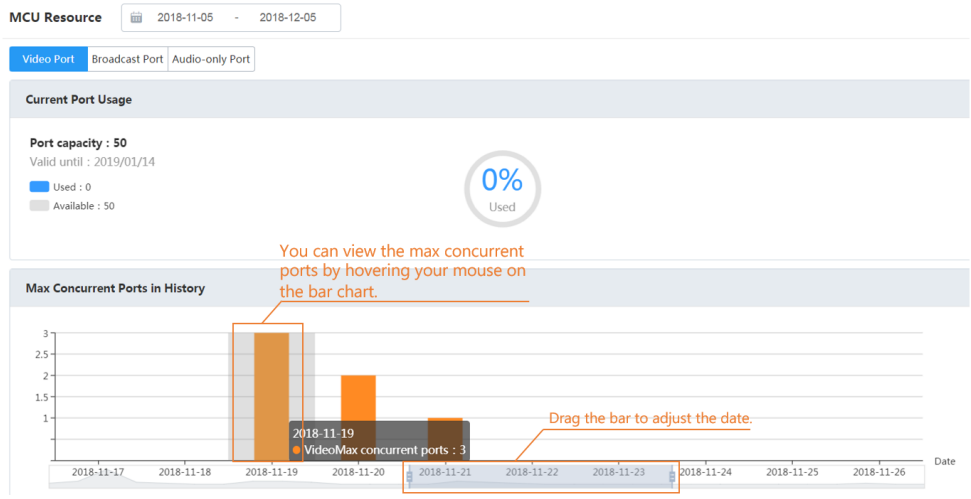
- *Viewing the MCU Resource*
- *Viewing the Conference Statistics*
- *Viewing the Call History*

Viewing the MCU Resource

You can view the max concurrent port, the usage of the video port, the broadcast port and the audio-only port.

Procedure

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

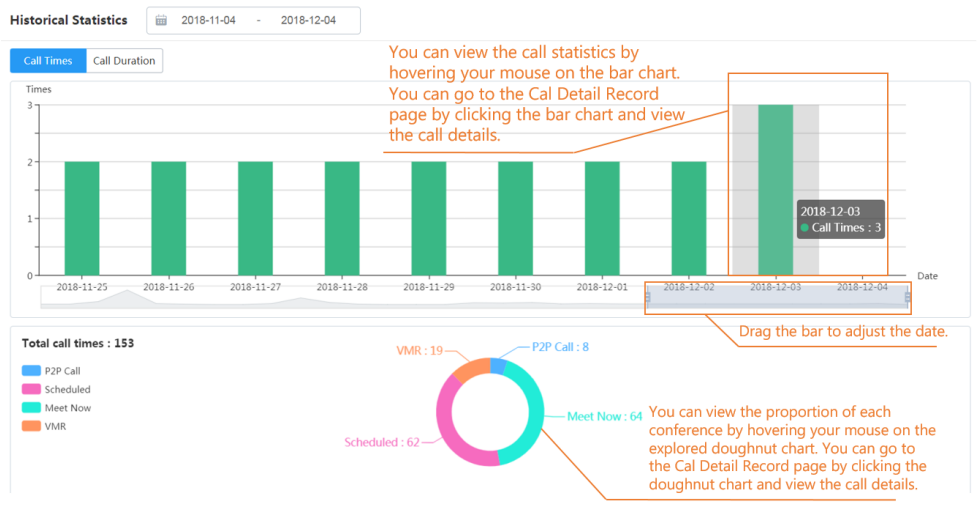


Viewing the Conference Statistics

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 information of conferences and 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 the 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 on your computer.

Related tasks

Viewing the Conference Statistics

System Maintenance

- *Viewing the System Version*
- *Upgrading the System*
- *Enabling the Device Upgrade*
- *Adding the Firmware*
- *Updating the Firmware*
- *Setting the Auto Backup*
- *Creating a Backup Manually*
- *Downloading a Backup*
- *Backup/Restore*
- *Rebooting the System*
- *Resetting to Factory*
- *Viewing the Operation Log*
- *Viewing the System Log*
- *Viewing the Device Log*
- *Viewing the Recording Log*

Viewing the System Version

You can view the current system version to update the system in time.

Procedure

Click **Maintenance** > **Upgrade** > **System Update**.

Upgrading the System

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

Procedure

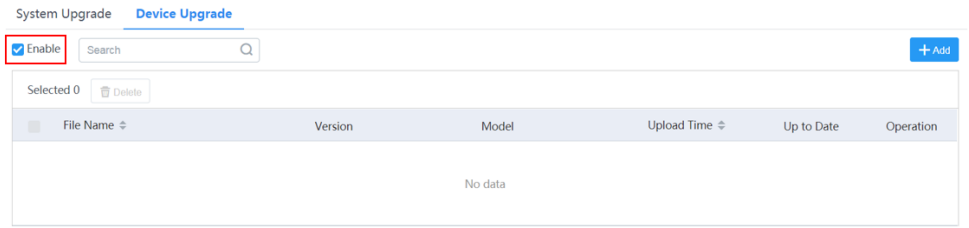
1. Click **Maintenance** > **Upgrade** > **System Update**.
2. Click **Update**, and select the desired software version.

Enabling the Device Upgrade

After you enable **Device Upgrade**, you can remotely upgrade the devices with YMS accounts registered on, including PVT950/PVT980,VC880/VC800/VC500/VC400/VC200/VC120/VC200 video conferencing system, CP960 conference phone, SIP VP-T49G IP phone, SIP-T58V IP phone and VP59 flagship smart video phone.

Procedure

1. Click **Maintenance** > **Upgrade** > **Device Upgrade**.
2. Select the **Enable** checkbox.



Adding the Firmware

Before upgrading the firmware, you need add it.

Procedure

1. Click **Maintenance** > **Upgrade** > **Device Upgrade** > **Add**.
2. Click **Upload** to upload the desired file.
3. If you also want to upgrade the accessory firmware, select the desired one in the **Accessory firmware** field.
4. Click **Save**.

Updating the Firmware

You can update the firmware manually or automatically.

Procedure

1. Click **Maintenance** > **Upgrade** > **Device Upgrade**.
2. Select the desired firmware, enable **Up to Date** and the firmware will be updated automatically if it is not the latest one.
3. If you want to update the firmware manually, click .
4. Click **OK**, to update the same type devices.

Setting the Auto Backup

You can enable the Auto backup, so that the server can create a backup for the important information automatically.

Procedure

1. Click **Maintenance** > **Backup/Restore** > **Setting**.
2. Configure the parameters.
3. Click **OK**.

Creating a Backup Manually

You can create a backup for YMS manually.

Procedure

1. Click **Maintenance** > **Backup/Restore** > **Add**.
2. Enter the file name.
3. Click **OK**.

Downloading a Backup

You can download the desired backup.

Procedure

1. Click **Maintenance** > **Backup/Restore**.
2. Click on the right side of the desired file.

Backup/Restore

- *Restoring a backup by Selecting a Backup Directly*
- *Restoring a backup by Uploading a Backup*

Restoring a backup by Selecting a Backup Directly

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

Procedure

1. Click **Maintenance** > **Backup/Restore**.
2. Click on the right side of the desired file.
3. Click **OK**.

Restoring a backup by Uploading a Backup

When an exception occurs to the server or the data is lost by accidental operation, you can restore the data by the backup file to keep the server working normally.

Procedure

1. Click **Maintenance** > **Backup/Restore** > **Upload**.
2. Click **Upload**, and select the desired file.
3. Click **OK** to restore.

Rebooting the System

When YMS fails to upgrade, for example it remains on a certain page, you can reboot the system.

Procedure

1. Click **Maintenance** > **System Restart**.
2. select the node, and click**Restart**.
3. Click **OK**.

Resetting to Factory

You might need to clear up all the user data, the system settings, the call records, the log and the recording files to solve the problem occurred to the YMS.

Procedure

1. Click **Maintenance** > **Restore to factory setting**.
2. Select the data type.
3. Click **Restore to Factory Settings**.
4. Operate according to the prompts, and click **OK**.

Viewing the Operation Log

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

Procedure

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

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

Viewing the System Log

You can view the system log to find out the reason when a problem occurs to the server.

Procedure

1. Click **Maintenance** > **Support Log** > **System log**.
2. Select the time, the module, and the node to export the log.
3. Click **Export Syslog**.

Viewing the Device Log

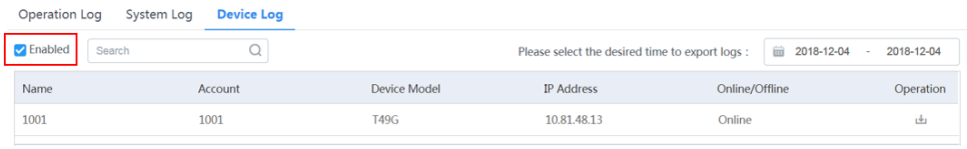
To view the SIP information communicated between the device and the server, for example, the device registration, you can enable the device log.

About this task

- After you enable it, the device logs will occupy some bandwidth and the system performance may vary according to the number of devices.
- For offline devices, you cannot view their log.

Procedure

1. Click **Maintenance** > **Support Log** > **Device log**.
2. Select the **Enable**checkbox.



3. Click on the right side of desired file.

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** > **Support Log** > **Recording log**.

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

Troubleshooting

- *Users Do Not Receive Emails*
- *User Fail to register an Account*
- *Failing to Activating a License Online*
- *Failing to Activating a License Offline*
- *Loading the Orgainzation Structure Slowly*

Users Do Not Receive Emails

Situation:

When you send user account information to users by email, but users do not receive any emails.

Cause:

- The emails may be in the spam folders.
- The emails may be intercepted by the back-end server.

Solution:

Procedure

1. Remind users to check the spam folders.
2. Contact the enterprise IT staff to check the back-end server.

User Fail to register an Account

Situation:

User fail to register an account.

Cause:

- The user may enter the wrong registration information.
- The user IP address is set as abnormal IP address.

Solution:

Procedure

1. Check the registration information.
2. Check whether or not the user IP address is set as abnormal IP address. If it is, *Delete the Abnormal IP* need to be done.

Failing to Activating a License Online

Situation:

Click **Refresh**, and the prompt “Unable to connect to LicenseServer due to network problem” is popped up.

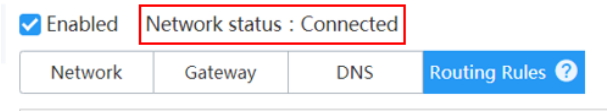
Cause:

- Network configuration error.
- The license was used by other YMS, or the CPU, the network adapter or the motherboard on YMS is changed, that causing the mismatch between the license and the YMS hardware information.

Solution:

Procedure

1. Check whether or not the network cable of the YMS server 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, execute the command "ping license.yealinkops.com".
   - If it fails, there is a problem with the DNS or 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 YMS, 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 Activating a License Offline

Situation:

Import the authority file obtained from Yealink, but the page prompts “Certificate import failed”.

Cause:

- Authority file error.
- The license was used by other YMS, or the CPU, the network adapter or the motherboard on YMS is changed, that causing 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 series number associated with your YMS.
2. Make sure that the server license is not used by other YMS, 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 Orgainzation Structure Slowly

Situation:

If you use the stand-alone version, wherever there is the organization structure, when the number of the staff reaches 25,000, the speed of loading the data may become slower.

Cause:

Large amount of data.

Solution:

Procedure

Contact the technical support to modify the contact push mechanism.