

# **Yealink Meeting Server Administrator Guide V20.0.0.5**

# Contents

<b>About This Guide.....</b>	<b>6</b>
Introduction of Yealink Meeting Server.....	6
Introduction of the Deployment Structure.....	6
Targeted Audience.....	7
Basic Concepts.....	7
Browser Requirement.....	7
Port Mapping Requirements.....	7
Icons Introduction.....	8
Related Documents.....	8
In This Guide.....	9
 <b>Basic Operations of the Enterprise Administrator.....</b>	 <b>9</b>
Logging into YMS.....	9
Setting the Setup Wizard.....	10
Introduction of the Home Page.....	10
Account Management.....	11
Editing the Login Password.....	11
Editing the Registered Email.....	12
Logging out of Yealink Meeting Server.....	12
 <b>System Setting.....</b>	 <b>12</b>
Setting the Primary Domain Name.....	13
Setting the Web Service Address.....	13
Setting the Log Service Address.....	14
Configuring the Port.....	14
Configuring the Time.....	15
Setting the Data Space.....	16
Configuring the SMTP Mailbox.....	16
Allocating the Number Resource.....	17
Configuring the Node.....	18
Viewing the Node Information.....	19
Configuring the Address Port Mapping.....	19
Setting the IP Property.....	19
Adding a Sub Admin Account.....	20
Editing the Information of a Sub Admin Account.....	20
Delete the Abnormal IP.....	20
Adding a Security Group.....	21
Configuring Intelligent Security Strategy.....	21
Applying for the Accesskey.....	22
Adding the User-Agent Blacklist.....	23
Adding the User-Agent Compatible List.....	23
Activating a License.....	24
Importing the Server Device License.....	24
Activating a License Online.....	25
Activating a License Offline.....	25
Disassociating the License.....	26
Importing the Trusted CA Certificate.....	26

Importing the HTTPS Certificate.....	26
Importing the TLS Certificate.....	26
Setting the Display on the Web Page.....	27
Configuring the Email Template.....	32
Configuring SIP Trunk IVR.....	32
Configuring the Audio IVR.....	33

## **Service Management.....33**

Configuring the Registration Service.....	34
Communicating with Other Devices via IP Call.....	35
Configuring the IP Call Service.....	35
Configuring the Third Party REG Service.....	37
Communicating with PSTN.....	38
Configuring the PSTN Gateway Service.....	38
Setting the Peer Trunk Service.....	41
Configuring the REG Trunk Service.....	43
Communicating with Skype for Business Server.....	46
Communicating with the Local SfB Server.....	46
Communicating with Microsoft Office 365.....	50
Communicating with Other Enterprise SfB Servers.....	51
Configuring the SfB Service.....	56
Configuring the SfB Gateway Media Service.....	60
Configuring the GK Service.....	61
Configuring the H.323 Gateway.....	63
Configuring the Interactive Media Service.....	65
Configuring the Broadcast Media Service.....	66
Configuring the RTMP Media Service.....	66
Configuring the Media Bypass Service.....	67
Configuring the Traversal Service.....	68

## **Call Settings.....69**

Call Control Policy.....	69
Setting the Video and the Content Resolution.....	69
Configuring the Call Bandwidth.....	70
Configuring the Max Video Parties per Conference.....	70
Configuring the Max Audio-Only Parties per Conference.....	70
Setting the Audio IVR language.....	70
Configuring the Time for Joining Conference Beforehand.....	71
Enabling Auto Dialing.....	71
Enabling the Auto Redialing.....	71
Displaying the Native Video.....	72
Setting the Last Participant Backstop Timeout.....	72
Setting the Auto End Conference Without Moderator.....	72
Enabling the Content Only.....	72
Disabling the Roll Call Setting.....	73
Configuring the iOS Push Address.....	73
Enabling the Broadcasting Interactive.....	73
Configuring the RTMP Live.....	74
Enabling the Conference Recording.....	74
Setting the QoS.....	75
Video Display Policy.....	75
Setting the Default Layout.....	75
Setting the 1+N Video Layout.....	76
Setting the Equal N×N Video Layout.....	76

Displaying the Participant Name.....	77
Displaying the Participant Status.....	77
Displaying the Participant Quantity.....	77
Restricting the Dialing Number.....	77
Add a Number Filter.....	77
Call Routing Rule.....	79
Common Perl Compatible Regular Expressions (PCRE) and Replacement Strings.....	79
Adding a Call Routing Rule.....	80
Configuring the Call Routing Rule.....	82
<b>Account Management.....</b>	<b>82</b>
User Accounts, Room System Accounts and Other Accounts.....	83
Group Management.....	83
Adding a Group.....	83
Editing/Deleting the Group.....	83
Adding an User Account.....	84
Parameters of User Account.....	84
Adding an User Account Manually.....	86
Importing a Batch of User Accounts.....	87
Adding a Room System Account.....	87
Adding Other Account.....	89
Parameters of Other Devices.....	90
Adding Other Account Manually.....	90
Adding a Batch of Other Accounts.....	90
Sending an Email to a YMS Account.....	90
Adjusting the Account Group.....	91
Editing the Authority.....	91
Editing the GK Registration Parameter.....	91
Editing a Batch of Accounts.....	92
Configuring the LDAP.....	92
<b>Meeting Room Management.....</b>	<b>95</b>
The Entity Meeting Room and the Permanent VMR.....	95
Managing the Meeting Room Group.....	95
Adding the Meeting Room Group.....	95
Editing/Deleting the Meeting Room Group.....	96
Adding a General Meeting Room.....	96
Adding a Video Meeting Room.....	96
Discussion Mode and Training Mode.....	97
Adding a Permanent VMR.....	98
Adjusting the Meeting Room Group.....	100
Sending Emails about Joining the Conference.....	100
<b>Conference Management.....</b>	<b>101</b>
Viewing the Conference.....	101
Viewing the Meeting Room Usage.....	101
Deleting a Conference.....	102
Controlling the Conference.....	102
<b>Conference Statistics.....</b>	<b>102</b>
Viewing the MCU Resource.....	102
Viewing the Conference Statistics.....	103



Viewing the Call History.....	103
-------------------------------	-----

## **System Maintenance..... 104**

Viewing the System Version.....	104
Upgrading the System.....	104
Enabling the Device Upgrade.....	105
Adding the Firmware.....	105
Updating the Firmware.....	105
Setting the Auto Backup.....	105
Creating a Backup Manually.....	106
Downloading a Backup.....	106
Backup/Restore.....	106
Restoring a backup by Selecting a Backup Directly.....	106
Restoring a backup by Uploading a Backup.....	106
Rebooting the System.....	107
Clearing up All Accounts and the Conference Statistics.....	107
Viewing the Operation Log.....	107
Viewing the System Log.....	107
Viewing the Device Log.....	107

## **Troubleshooting..... 108**

Users Do Not Receive Emails.....	108
Users Fail to Register Accounts.....	108
Failing to Activating a License Online.....	109
Failing to Activating a License Offline.....	109

## **Appendix-Time Zones..... 110**

# About This Guide

---

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

This guide is applied to YMS.

- [Introduction of Yealink Meeting Server](#)
- [Introduction of the Deployment Structure](#)
- [Targeted Audience](#)
- [Basic Concepts](#)
- [Browser Requirement](#)
- [Port Mapping Requirements](#)
- [Icons Introduction](#)
- [Related Documents](#)
- [In This Guide](#)

## Introduction of Yealink Meeting Server

---

Yealink Meeting Server (YMS) is a distributed cloud-based videoconferencing infrastructure tailored for HD videoconferencing 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, the SIP Trunk, the WebRTC server, and the 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
<b>Single Version</b>	A single YMS but with all services.
<b>Cluster Version</b>	<p>Multiple YMSs and contains the following node types:</p> <ul style="list-style-type: none"> <li>• <b>Master node:</b> it contains all YMS services.</li> <li>• <b>Sub-master node:</b> it should contain 2 sub-master nodes to realize the disaster recovery function for all the features.</li> <li>• <b>Business node:</b> you can deploy the service in each business node according to the enterprise deployment plan. The services contain SIP service, MCU service and so on.</li> </ul>

## Targeted Audience

This guide is mainly intended for the following audiences.

- The distributors
- The network administrators

## 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:** it refers to the devices that support YMS, including VC880/VC800/VC500/VC200/VC400/VC120/VC200 video conferencing system, SIP VP-T49G IP phone, SIP-T58V IP phone, VC Desktop and 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.

## 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

## Port Mapping Requirements

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

**Requirements of the internal service port:** make sure that the port from 8000--9999 (UDP+TCP), the port 27017 (UDP+TCP), and the port 22 (TCP) in every node of the cluster can communicate with each other.

**Table 2: Requirements of the external service port**





Port	UDP/TCP	Description
443	TCP	Web port
444	TCP	

Port	UDP/TCP	Description
80	TCP	
514	UDP/TCP	Rsyslog log service port
1719	UDP/TCP	H.323 port
1720	UDP/TCP	
1722	UDP/TCP	
3478	UDP/TCP	Turnserver port
3479	UDP/TCP	
5060	UDP/TCP	SIP port
5061	UDP/TCP	
5062-5070	UDP/TCP	
10000-60000	UDP/TCP	Select it according to the configuration of the media, the traversal service and so on (UDP is compulsory but TCP is optional).

## Icons Introduction

The icons on Yealink Meeting Server are 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)

## 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 Web App User Guide: it introduces how to join the conference via browser.
- 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.

Read the [Yealink Products Regulatory Notices guide](#) for all regulatory and safety guidance.

## 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 [Account Management](#)
- Chapter 6 [Meeting Room Management](#)
- Chapter 7 [Conference Management](#)
- Chapter 8 [Conference Statistics](#)
- Chapter 9 [System Maintenance](#)
- Chapter 10 [Troubleshooting](#)
- Chapter 11 [Appendix-Time Zones](#)

## Basic Operations of the Enterprise Administrator

---

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

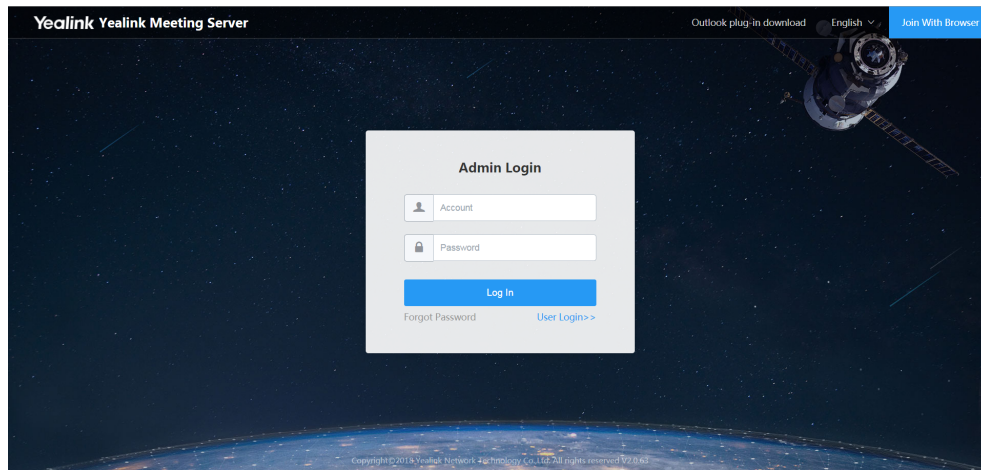
- [Logging into YMS](#)
- [Setting the Setup Wizard](#)
- [Introduction of the Home Page](#)
- [Account Management](#)
- [Logging out of Yealink Meeting Server](#)


## 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 administrator 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 have entered wrong passwords for 10 times, your account will be locked for 3 minutes. Please try again later.

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 is managed by group or by different authorities. The system administrator has the highest operation authority on YMS. Accounts with different permissions can see different Home pages, and this part takes the Home page viewed by the system administrator account as an example.

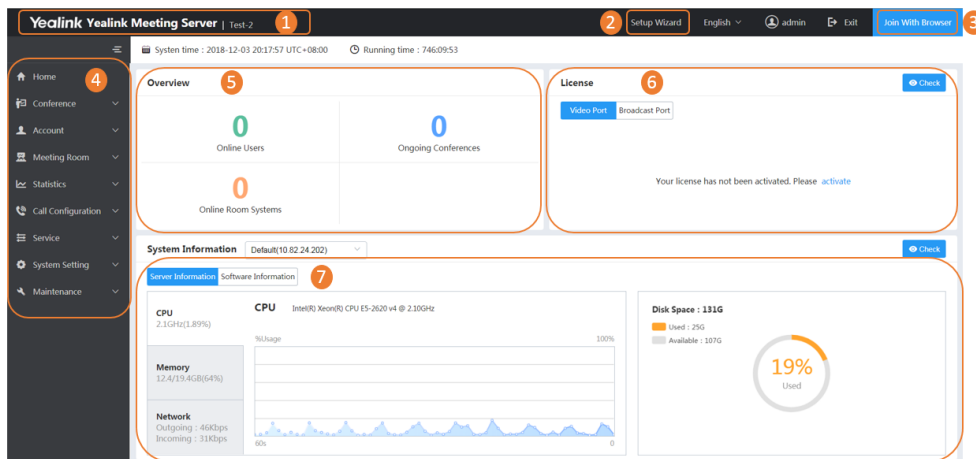


Table 4:

Number	Description
1	Go to the Home page quickly.
2	Go to the Setup Wizard.
3	Join the conference by browser. For more information about Joining With Browser, refer to <a href="#">Yealink Web App User Guide</a> .
4	The navigation bar.
5	<ul style="list-style-type: none"> <li>View the number of the online users, the ongoing conferences and the online room system accounts.</li> <li>Go to the corresponding module quickly.</li> </ul>
6	<ul style="list-style-type: none"> <li>Go to the License page quickly.</li> <li>View the video port.</li> <li>View the broadcast port.</li> </ul>
7	<ul style="list-style-type: none"> <li>View the node information.</li> <li>View the server CPU, the memory, the network, and the disk space.</li> <li>View the information of the software version.</li> </ul>

## 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 warning 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 Yealink Meeting Server

---

If you want to use other account 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.



**Note:** If the system has been idle on either page for more than 30 minutes, the system will log out of your account automatically and 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 primary domain name which can be accessed by the devices to register.

### Procedure

1. Click **System Settings > Common Settings > Network Association**.
2. Enter the address in the **Primary Domain**, and the domain name directs to any server node IP.  
Default domain name is <IP>.xip.io.
3. Click **Save**.
4. Operate according to prompts, and click **OK**.

## Setting the Web Service Address

Considering the security, you can set access addresses for the internal and the external network respectively, to realize the separation of the internal and external network when the device is accessing the server and YMS contacts, downloading or uploading the firmware from the server.

### 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.

Enter the domain name of the master node in the internal **Service URL** field, and enter the address of the mapped public network in the external **Service URL** field.

\* Primary domain :

WEB service address :

Service network :	Service URL :
<input type="text" value="Internal network"/>	<input type="text" value="https://10.82.24.202"/> ✕
<input type="text" value="External network"/>	<input type="text" value="https://ymstest2.yealink.com"/> ✕
<input type="button" value="+ Add service address"/>	



**Note:** You cannot edit the intranet listener port. In general, the internal network uses port 80 for HTTP protocol and port 443 for HTTPS protocol. If the extranet cannot use port 80 and 443, you need map the port, and the external network can visit the URL which the mapped port is added into.

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

## Setting the Log Service Address

You can set the log service address, so that the devices can upload the log to log service address.

### Procedure

1. Click **System Settings > Common Settings > Network Association**.
2. In the **Log service address** field, click **Add service address**.
3. Configure the basic parameters.

**Table 5: Basic Parameter**

Parameter	Description
Service network	The network of the node to which the devices upload the log.
Transmission type	When the devices uploading the log to YMS, the transmission type is UDP.
IP address	<p>The IP address of the node to which the devices upload the log.</p> <p><b>Note:</b> If you use cluster version, you need to specify the master node or the sub-master node for uploading the device log. The master node is recommended.</p>

4. Click **Save**.
5. Operate according to 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 signaling port and the minimum port should be not less than 200. For example, you set 10000 as the minimum port, the maximum port should be not less than 10199.

### Procedure

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

Table 6:

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

3. Click **Save**.
4. Operate according to 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 7: Time parameter

Parameter	Description
<b>Current server time</b>	The current time of YMS.
<b>Time access</b>	The method used by YMS to access the time and date. <ul style="list-style-type: none"> <li>• <b>SNTP</b></li> <li>• <b>Date &amp; time configuration</b></li> </ul> <b>Default:</b> SNTP.
<b>Server domain</b>	If you select <b>SNTP</b> , configure the primary server and the backup server of NTP.  <b>Default:</b> the first one is the primary server, and its default value is pool.ntp.org.
<b>Date &amp; time</b>	The date and the time.

Parameter	Description
<b>Timezone</b>	The time zone used by YMS and the default time zone for scheduling the conference.
<b>Auto adjust conference DST</b>	<p>The type of DST.</p> <p>The supported types in YMS are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Auto</b>-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.</li> <li>• <b>Disable</b>-DST is not used.</li> </ul> <p><b>Default:</b> disable.</p>

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 be not 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.

Network Association	Time	Data Space	SMTP Mailbox	Number Resource Allocation
SMTP server :	<input type="text" value="mail.yealink.com"/>			
Mailbox :	<input type="text" value="gl@yealink.com"/>			
Username :	<input type="text" value="yl0026@yealink.com"/>			
Password :	<input type="password" value="....."/>			
Port :	<input type="text" value="587"/>	(Only1~65535)		
	<input checked="" type="checkbox"/> This server requires a secure connection			
	<input type="text" value="TLS"/>			

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](#) need to be done.

6. Click **Save**.

## Allocating the Number Resource

You can customize the range of 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 8: Parameters of the number


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

3. Click **OK**.

## Configuring the Node

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

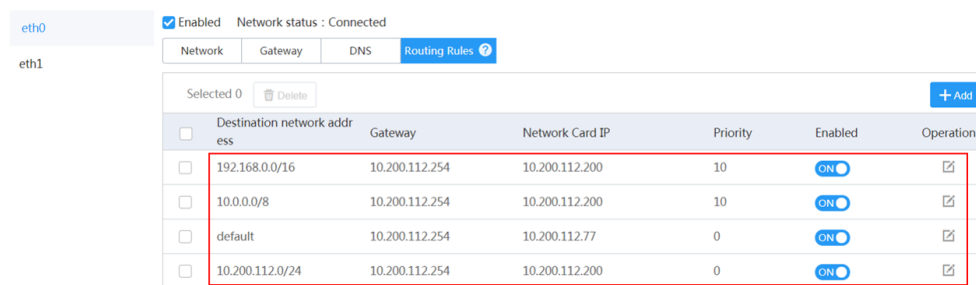
### Procedure

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.
- The routing rules came with your server 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 mapped to the public network with the public button on and the other mapped 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 the port of the intranet to the extranet, so that the extranet can access the IP address and the port for various services.

#### Procedure

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

## Setting the IP Property

---

When there are multiple operators, you can set the IP property for the edge business node, so that the device can register a YMS account quickly by the route, to guarantee the conference quality.

#### Procedure

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

**Table 9:**

Parameter	Description
IP address	The IP address of this node.

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

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

## Adding a Sub Admin Account

To ensure the system security, you can configure different sub admin accounts with different admin authorities.

### About this task

Sub admin account contains the conference manager, the conference operator, and the operation manager. 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 **Level** field, select the level.
4. 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 and authority type for a sub admin account.

### Procedure

1. Click **System Settings > 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. In the **Level** field, select the level.
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 situation:

- 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 ensure the server security.

### Procedure

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

**Table 10: Parameters of the security group**

Parameter	Description
<b>Name</b>	The name of this security group.
<b>Type</b>	<p>The type of this security group.</p> <p>The supported types are as follows:</p> <ul style="list-style-type: none"> <li>• Single IP</li> <li>• Section IP</li> </ul>
<b>IP Address</b>	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 11: Parameters of the SIP Signaling**

Parameter	Description
<b>Attack detection cycle</b>	The detection cycle. <b>Default:</b> 25 seconds.
<b>Max frequency of IP call or auth failure</b>	During a period, if the number of IP calls from the same IP address exceeds the max frequency, this IP is considered as suspicious attack and is forbidden during a specified time. <b>Default:</b> 10 times.
<b>Suspected attack banned duration</b>	The banned duration. <b>Default:</b> 10 minutes.
<b>Max suspected attacks frequency within 24 hours</b>	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 via web (refer to <a href="#">Delete the Abnormal IP</a> ). <b>Default:</b> 3 times.
<b>Long term banned duration</b>	The banned duration. You can free this IP via web (refer to <a href="#">Delete the Abnormal IP</a> ). <b>Default:</b> 7 days.
<b>Max concurrent IP call per node</b>	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. <b>Default:</b> 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 your 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.

Add ×

Enabled : ☒

\* Regular expression :

Description :

**Table 12:**

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

### Procedure

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

Add ×

Enabled : ☒

\* Regular expression :

Description :

**Table 13:**

Parameter	Description
<b>Enable</b>	Enable or disable this compatible list. <b>Default:</b> enable.
<b>Regular expression</b>	The Perl Compatible Regular Expressions (PCRE). <b>Note:</b> for example, if you set the PCRE as ^polycom, all User-Agent devices whose model type starts with polycom can call into YMS.
<b>Description</b>	The additional description for 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 license; 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 association between the license device ID and the server succeeds, the page will display as follows:

License Device ID : E0E767F76A3A0C92

Unbind License Refresh Offline Activation License

## 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 can get the license by submitting the applicant, the license type, the concurrent number, and the period of 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

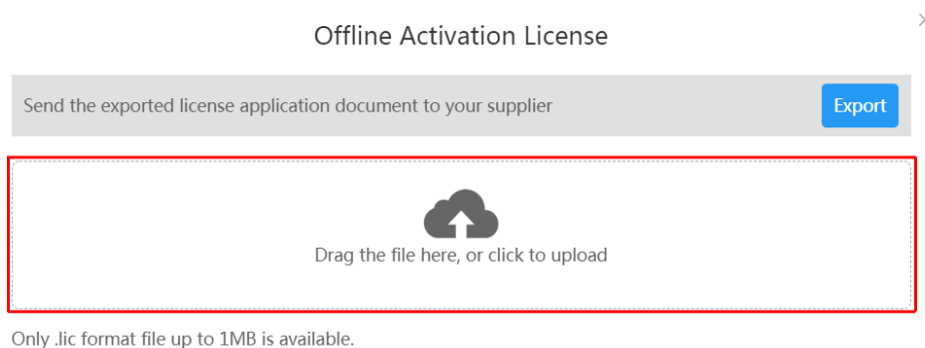
If the server cannot access the public network, you can activate the license offline.

### About this task

[Importing the Server Device License](#) is done.

### Procedure

1. Click **System Setting > License > Offline Activation License**.
2. Click **Export**, and send the exported file to Yealink.
3. Click the dotted box area 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 check 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 check 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**.

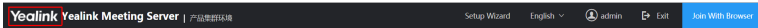
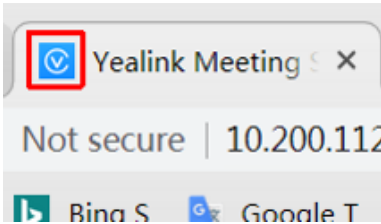
## Setting the Display on the Web Page

According to the enterprise need, you can customize the logo, the web protocol, the WebRTC protocol, and the video conference.

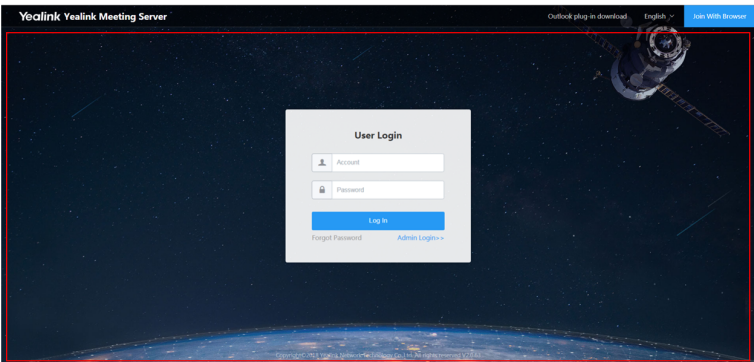

### About this task

The parameters are described as below:

**Table 14: Parameters of the Logo**

Parameter	Effect
Portal logo	
Tab logo	

**Table 15: Parameters of the Web Portal**

Parameter	Effect
Background image	
Email header logo	  Hello,  You have been invited to join this video conference.  Subject: Mike's video conference  Time: 2018-11-12 11:30 ~ 2018-11-12 12:00 (UTC+08:00)

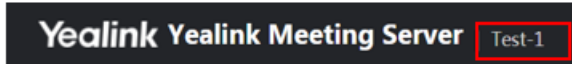
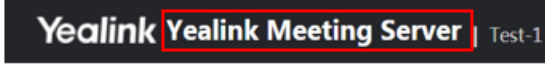
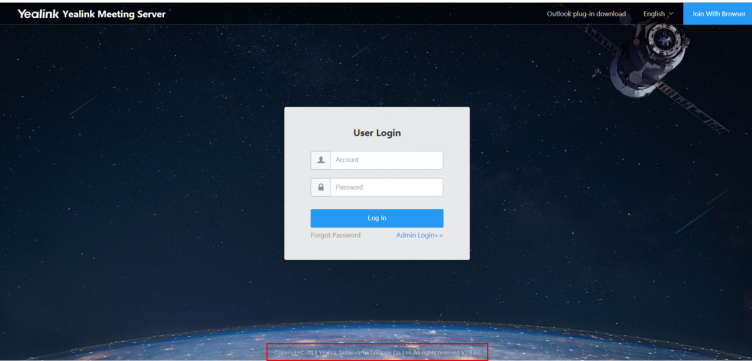
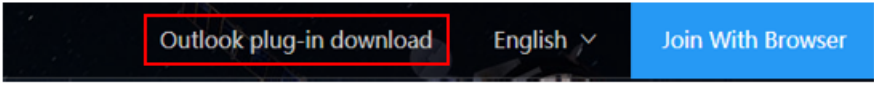
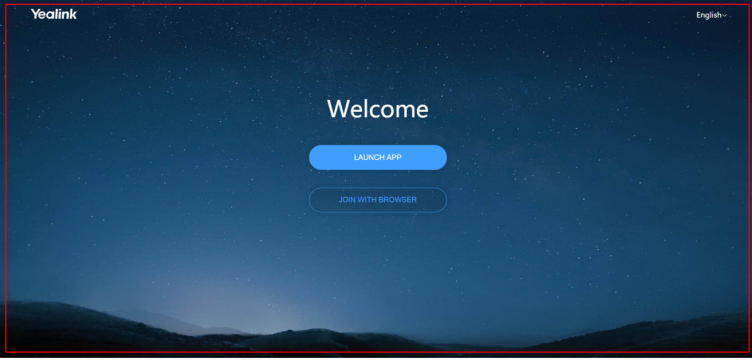
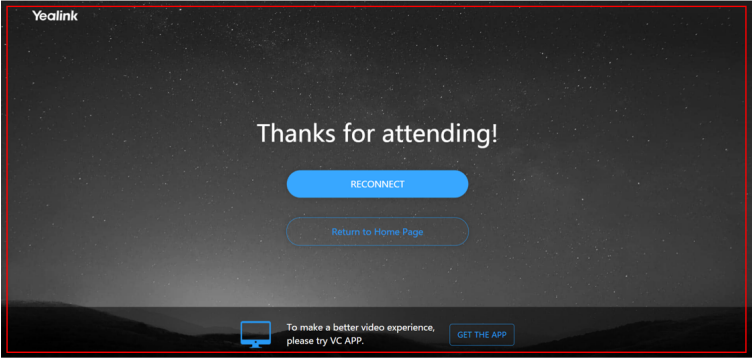
Parameter	Effect
Enterprise name	
Platform name	
Display copyright	
Display Outlook plug-in download	

Table 16: Parameters of the WebRTC Portal

Parameter	Effect
Background image for WebRTC home screen	
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.



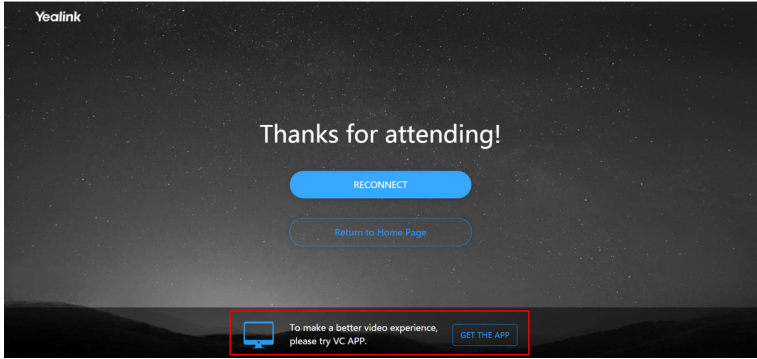
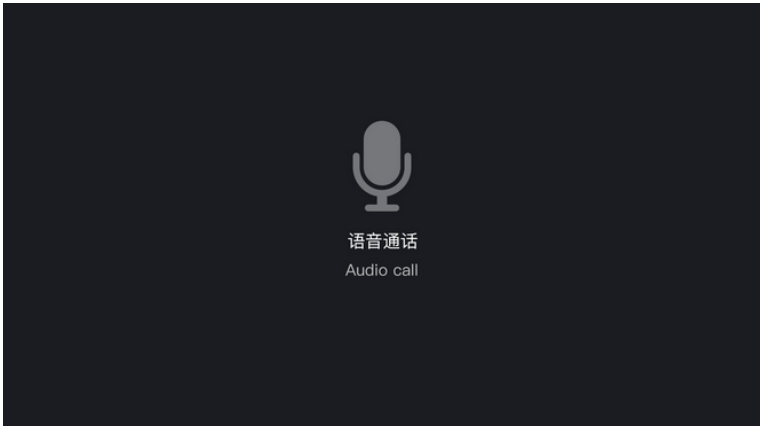

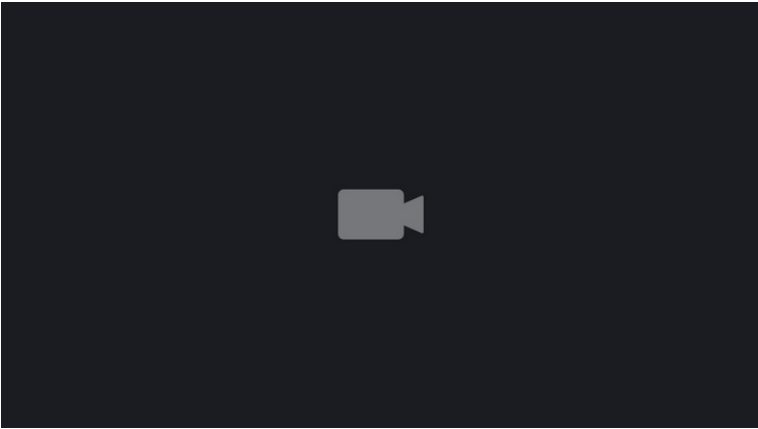

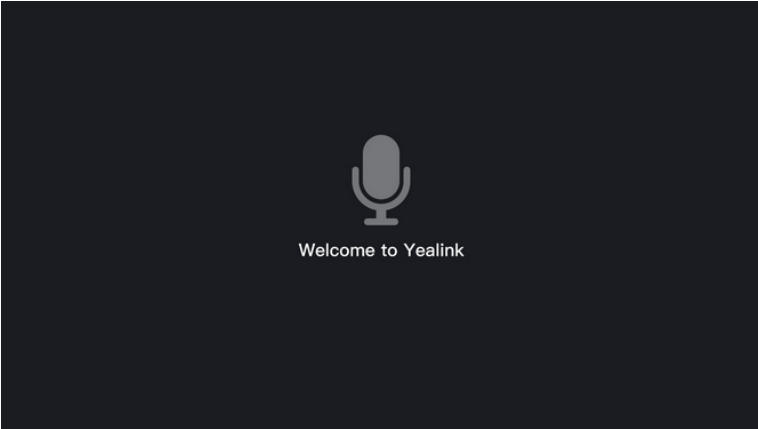
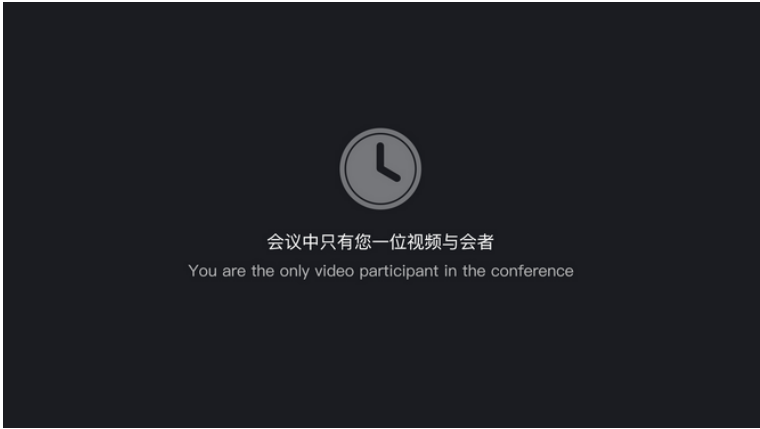
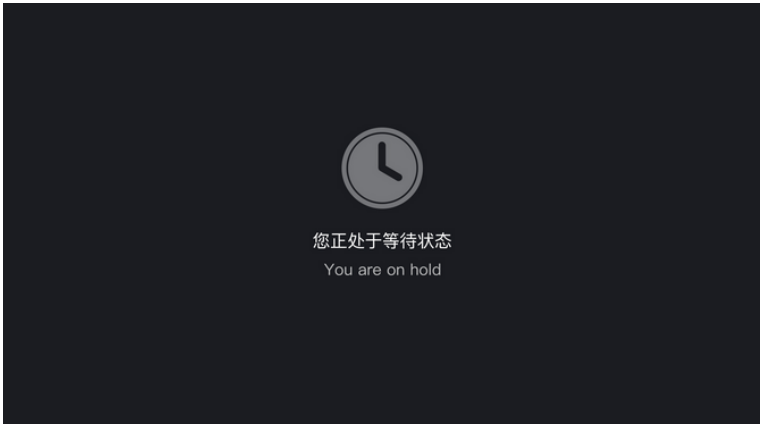

Parameter	Effect
Display PC soft-client download	
Windows	The address for downloading Yealink VC Desktop for Windows.
Mac	The address for downloading Yealink VC Desktop for Mac.

Table 17: Parameters of the Video Conference

Parameter	Effect
Audio call image	
License limited image	

Parameter	Effect
No video data image	
Camera OFF image	
Welcome screen image	

Parameter	Effect
The sole video call party image	 <p>会议中只有您一位视频与会者 You are the only video participant in the conference</p>
Conference lobby image	 <p>您正处于等待状态 You are on hold</p>
Waiting for the lecturer image	 <p>请等待演讲者 Please waiting for the lecturer</p>

Parameter	Effect
Waiting image	

### Procedure

1. Click **System Setting > Customization > Email Template**.
2. Configure the logo.
3. Configure the web portal.
4. Configure WebRTC portal.
5. Configure 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 email template 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 the Audio 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 will go to the audio IVR.

### Procedure

1. Click **System Setting > Customization > Audio IVR**.
2. Configure the voice prompt, and do one of the following:
  - Select **Default Greeting**. The language depends on the IVR language.
  - 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](#)
- [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](#)
- [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 18: Parameters of the Registration Service**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.

3. Configure the parameters of the service address.

**Table 19: Parameters of the Service Address**

Parameter	Description
<b>Network</b>	The IP address used by this node.
<b>TLS Port</b>	The TLS port used by this node. <b>Note:</b> it only provides TLS registration.

4. Configure the security policy.

**Table 20: Parameters of the Security Policy**

Parameter	Description
<b>Enable security policy</b>	Enable or disable the security policy. <b>Default:</b> disable.
<b>Mode</b>	Select a mode. The supported modes are as follows: <ul style="list-style-type: none"> <li>• <b>Whitelist:</b> allowing the person in this group to register.</li> <li>• <b>Blacklist:</b> forbidding the person in this group to register.</li> </ul>
<b>Security Group</b>	Select a security group.

5. Click **Save**.
6. Operate according to 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 21: Basic Parameters**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.
<b>Outgoing protocol</b>	Select a protocol for transmitting the SIP signaling.  The supported protocols are as follows: <ul style="list-style-type: none"> <li>• UDP—the optimal protocol for transmitting SIP signaling.</li> <li>• TCP—the reliable protocol for transmitting SIP signaling.</li> <li>• TLS—the safe protocol for transmitting SIP signaling. TLS is available only when the YMS is registered at a SIP gateway that supports TLS.</li> </ul> <b>Default:</b> UDP.

3. Configure the parameters of the service address.

**Table 22: Parameters of the Service Address**

Parameter	Description
<b>Network</b>	The IP address used by this node.
<b>UDP/TCP Port</b>	The UDP/TCP port used by this node. <b>Note:</b> 5060 port is compulsory.
<b>TLS Port</b>	The TLS port used by this node.

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 inviting 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.
8. Configure the security policy.

**Table 23: Security policy parameter**

Parameter	Description
<b>Enable security policy</b>	Enable or disable the security policy. <b>Default:</b> disable.
<b>Mode</b>	Select a mode.  The supported modes are as follows: <ul style="list-style-type: none"> <li>• <b>Whitelist:</b> allowing the person in this group to call into.</li> <li>• <b>Blacklist:</b> forbidding the person in this group to call into.</li> </ul>
<b>Security Group</b>	Select a security group.

9. Configure the outgoing call rule.

**Outgoing call rule**

Priority :	Callee regex match :	Callee regex replace string :
1	^10088	10.81.43.7
1	^conf_(\d{5})@	\$1@10.86.0.201.xip.io
<b>+ Add</b>		

Priority :	Caller regex match :	Caller regex replace string :
1	^3802	95588
2	.+	95599
<b>+ Add</b>		

SIP account 3802 can dial "10088" to call "10.81.43.7".

Account 8888 registered in YMS (IP address 10.86.0.33) can dial "conf\_5555" to call the conference (ID 5555) in YMS (IP address 10.86.0.201).

Make the caller ID displayed in the remote call or conference as "95588" but "3802".

Make the caller ID displayed in the YMS conference 5555 as "95599" but "3802@10.86.0.33.xip.io".

10. Configure the incoming call rule.



**Incoming call rule**

Priority :	Callee regex match :	Callee regex replace string :
2	^((\d{5}))"(\d{5})@	\$1@10.86.0.220.xip.io
<a href="#">+ Add</a>		

Priority :	Caller regex match :	Caller regex replace string :
1	10.81.43.7	10088
<a href="#">+ Add</a>		

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

Make the caller ID displayed in a conference as "10088" but "10.81.43.7".

11. Click **Save**.

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

#### Related concepts

[Common Perl Compatible Regular Expressions \(PCRE\) and Replacement Strings](#)

#### Related tasks

[Adding a Security Group](#)

## 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 in the server is not supported.

#### Procedure

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

**Table 24: Basic Parameters**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.

3. The parameters of the service address.

**Table 25: Parameters of the Service Address**

Parameter	Description
<b>Network</b>	The IP address used by this node.

Parameter	Description
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 third-party devices have a lower compatibility.
7. Configure the security policy.

**Table 26: Parameters of the Security Policy**

Parameter	Description
Enable security policy	Enable or disable the security policy. <b>Default:</b> disable.
Mode	Select a mode. The supported modes are as follows: <ul style="list-style-type: none"> <li>• <b>Whitelist:</b> allowing this group to make third-party registration.</li> <li>• <b>Blacklist:</b> forbidding this group to make third-party registration.</li> </ul>
Security Group	Select a security group.

8. Click **Save**.
9. Operate according to 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 network (such as the telephone), you need configure the PSTN gateway service.

#### Procedure

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

**Table 27: Basic Parameters**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.
<b>Network</b>	The IP address of this node.
<b>Port</b>	The source port on YMS to communicate with the PSTN gateway. <b>Note:</b> the value can be any integer from 0 to 65535.
<b>Gateway address</b>	The IP address or the domain name of the gateway.
<b>Gateway Port</b>	the port of the PSTN gateway. <b>Default port:</b> 5060. The value can be any integer from 0 to 65535.
<b>Transport protocol</b>	Select a protocol for transmitting the SIP signaling. The supported protocols are as follows: <ul style="list-style-type: none"> <li>• UDP—the optimal protocol for transmitting the SIP signaling.</li> <li>• TCP—the reliable protocol for transmitting the SIP signaling.</li> <li>• 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.</li> </ul> <b>Default:</b> UDP.
<b>Support video</b>	Enable it if the PSTN gateway supports video. <b>Default:</b> disable.
<b>Support content sharing</b>	Enable it if the PSTN gateway supports receiving or sending contents. <b>Default:</b> disable.
<b>Media Bypass</b>	Enable it to improve the server performance and to allow a larger number of participants in the conference. Note that the third-party devices has a lower compatibility. <b>Default:</b> disable.

### 3. Configure the security policy.

**Table 28: Security policy parameter**

Parameter	Description
<b>Enable security policy</b>	Enable or disable the security policy. <b>Default:</b> disable.
<b>Mode</b>	Select a mode.  The supported modes are as follows: <ul style="list-style-type: none"> <li>• <b>Whitelist:</b> allowing the person in this group to call into.</li> <li>• <b>Blacklist:</b> forbidding the person in this group to call into.</li> </ul>
<b>Security Group</b>	Select a security group.

## 4. Configure the outgoing call rule.

## Outgoing call rule

Outgoing call rule configuration interface showing two rule entries.

**Rule 1 (Callee):**

- Priority: 1
- Callee regex match: `^0(/d{11})`
- Callee regex replace string: `$1@10.88.0.97`

**Rule 2 (Caller):**

- Priority: 1
- Caller regex match: `^3802`
- Caller regex replace string: `95588`

The user whose phone number starts with 0 can be called through this PSTN gateway (IP address 10.88.0.97). For example, SIP account 3802 can call 018359710211.

Make the caller ID displayed in the remote party as "95588" but "3802".

## 5. Configure the incoming call rule.

## Incoming call rule

Incoming call rule configuration interface showing two rule entries.

**Rule 1 (Callee):**

- Priority: 1
- Callee regex match: `.*`
- Callee regex replace string: `main_ivr@10.86.0.220.xij`

**Rule 2 (Caller):**

- Priority: 1
- Caller regex match: `^183`
- Caller regex replace string: `10088`

The user whose phone number starts with 183 can call 0592-3792232 to go to the YMS conference lobby (IP address 10.86.0.220).

Make the caller ID displayed in the conference as "10088" but the number starts with 183.

6. Click **Save**.
7. Operate according to 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

To make users of two systems call each other by any number (for example, the communication of two YMSs), setting the peer trunk service and [Adding a Call Routing Rule](#) need to be done.

#### Procedure

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

**Table 29: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.
<b>Network</b>	The IP address of this node.
<b>Port</b>	The source port on YMS that communicates with the other YMS. <b>Note:</b> the value can be any integer from 0 to 65535.
<b>Transport protocol</b>	Select a protocol for transmitting the SIP signaling. The supported protocols are as follows: <ul style="list-style-type: none"> <li><b>UDP</b>— the optimal protocol for transmitting SIP signaling.</li> <li><b>TCP</b>—the reliable protocol for transmitting SIP signaling.</li> <li><b>TLS</b>—the safe protocol for transmitting SIP signaling. TLS is available only when the YMS is registered at a SIP gateway that supports TLS.</li> </ul> <b>Default:</b> UDP.
<b>Outbound proxy</b>	Enable or disable the outbound proxy server. <b>Default:</b> disable.

Parameter	Description
<b>Proxy address</b>	The IP address or domain name of the other system.
<b>Proxy port</b>	The port of the other system. <b>Note:</b> the value can be any integer from 0 to 65535.
<b>Support video</b>	If the other system supports the video, you can enable this. <b>Default:</b> enable.
<b>Support content sharing</b>	If the other system supports receiving or sending the content, you can enable this. <b>Default:</b> enable.
<b>Media Bypass</b>	Enable it to improve the server performance and to allow a larger number of participant in the conference. Note that third-party devices have a lower compatibility. <b>Default:</b> disable.

### 3. Configure the security policy.

**Table 30: Security policy parameter**

Parameter	Description
<b>Enable security policy</b>	Enable or disable the security policy. <b>Default:</b> disable.
<b>Mode</b>	Select a mode. The supported modes are as follows: <ul style="list-style-type: none"> <li>• <b>Whitelist:</b> allowing the person in this group to call into.</li> <li>• <b>Blacklist:</b> forbidding the person in this group to call into.</li> </ul>
<b>Security Group</b>	Select a security group.

### 4. Configure the outgoing call rule.

**Outgoing call rule**

Priority :	Callee regex match :	Callee regex replace string :
1	^0(d{4})	\$1@10.86.0.201.xip.io
<a href="#">+ Add</a>		

Priority :	Caller regex match :	Caller regex replace string :
1	^3802	95588
<a href="#">+ Add</a>		

Account 3802 registered in YMS (IP address 10.86.0.33.xip.io) can dial "03702" to call the account 3702 registered in YMS (IP address 10.86.0.201.xip.io).

Make the caller ID displayed in the remote party as "95588" but "3802".

**5. Configure the incoming call rule.****Incoming call rule**

Priority :	Callee regex match :	Callee regex replace string :
1	^1(id{4})	\$1@10.86.0.33.xip.io
<a href="#">+ Add</a>		

Priority :	Caller regex match :	Caller regex replace string :
1	^3702	96866
<a href="#">+ Add</a>		

Account 3702 registered in YMS (IP address 10.86.0.201.xip.io) can dial "13802" to call the account 3802 registered in YMS (IP address 10.86.0.33.xip.io).

Make the caller ID displayed in the local party as "96866" but "3702".

6. Click **Save**.

7. Operate according to 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 call into the conference in YMS, but cannot place P2P calls to YMS accounts.

## Procedure

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

**Table 31: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.
<b>Network</b>	The IP address of this node.
<b>Port</b>	The port on YMS to communicate with the third-party server. <b>Note:</b> the value can be any integer from 0 to 65535.
<b>Transport protocol</b>	Select a protocol for transmitting the SIP signaling. The supported protocols are as follows: <ul style="list-style-type: none"> <li>• <b>UDP</b>— the optimal protocol for transmitting the SIP signaling.</li> <li>• <b>TCP</b>—the reliable protocol for transmitting the SIP signaling.</li> <li>• <b>TLS</b>—the safe protocol for transmitting the SIP signaling. TLS is available only when the YMS is registered at a SIP gateway that supports TLS.</li> </ul> <b>Default:</b> UDP.
<b>Outbound proxy</b>	Enable or disable the outbound proxy server. <b>Default:</b> disable.
<b>Proxy address</b>	The IP address or the domain name of the third-party server.
<b>Proxy port</b>	The port of the third-party server. <b>Note:</b> the value can be any integer from 0 to 65535.
<b>Display name</b>	The name of the third-party server account.
<b>URL</b>	The IP address or the domain name of the third-party server.
<b>Auth name</b>	The authentication name of the third-party server account.
<b>Auth domain</b>	The authentication domain name of the third-party server account.



Parameter	Description
<b>Password</b>	The password of the third-party server account.
<b>Expires</b>	The registration timeout (in seconds) on YMS. If the time is out, the YMS will send the registration request to the third-party server again. <b>Default:</b> 3600 seconds.
<b>Support video</b>	Enable it if the remote supports video. <b>Default:</b> disable.
<b>Support content sharing</b>	Enable it if the remote supports receiving or sending contents. <b>Default:</b> disable.
<b>Media Bypass</b>	Enable it to improve the server performance and to allow a larger number of participants in the conference. Note that third-party devices have a lower compatibility. <b>Default:</b> disable.

### 3. Configure the outgoing call rule.

#### Outgoing call rule

Priority :
Callee regex match :
Callee regex replace string :

1
^9(d{3})
\$1@10.200.108.42

+

Add

Priority :
Caller regex match :
Caller regex replace string :

1
^3802
024@10.200.108.42

+

Add

Account 3802 registered in YMS (IP address 10.86.0.33.xip.io) can dial "9025" to call the 3CX account 025.

3802 is replaced by 024@10.200.408.42, because 3CX server cannot recognize 3802.

### 4. Configure the incoming call rule.

## Incoming call rule

Priority :	Callee regex match :	Callee regex replace string :
1	^024	conference_ivr@10.86.0.:
<a href="#">+ Add</a>		

Priority :	Caller regex match :	Caller regex replace string :
1	^025	9025
<a href="#">+ Add</a>		

When the 3CX account 025 calls 024, it will go to the YMS conference lobby (IP address 10.86.0.220).

Make the caller ID displayed in the local as "9025" but "025".

5. Click **Save**.

6. Operate according to 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:** SfB 2016 and 2015 are supported.

For more information about the deployment of YMS with SfB, refer to [Skype for Business and Yealink Meeting Server Deployment Guide](#).

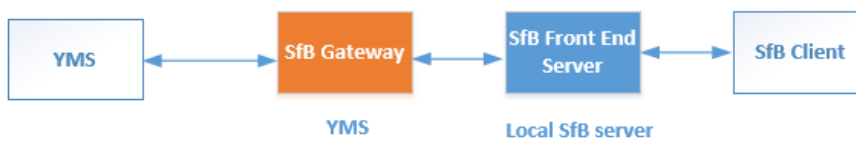
- [Communicating with the Local SfB Server](#)
- [Communicating with Microsoft Office 365](#)
- [Communicating with Other Enterprise SfB Servers](#)
- [Configuring the SfB Service](#)
- [Configuring the SfB Gateway Media Service](#)

### Communicating with the Local SfB Server

In the intranet, if you want the YMS and SfB communicates with each other and the users can use both of 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](#) .

#### Intranet



- [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 32:**

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.	<p>New-CsTrustedApplicationPool <b>-Identity</b> &lt;YMS DNS FQDN&gt; <b>-ComputerFqdn</b> &lt; YMS DNS FQDN&gt; <b>-Registrar</b> &lt;Front End Pool DNS FQDN&gt; <b>-Site</b> &lt; Site ID&gt; <b>-RequiresReplication</b> \$false <b>-ThrottleAsServer</b> \$true <b>-TreatAsAuthenticated</b> \$true</p> <p><b>Example command:</b></p> <p>New-CsTrustedApplicationPool <b>-Identity</b> sfb1.5060.space <b>-ComputerFqdn</b> sfb1.5060.space</p> <p><b>-Registrar</b> xiamenpool.xiamen.yealinksfb.com <b>-Site</b> 5 <b>-RequiresReplication</b> \$false <b>-ThrottleAsServer</b> \$true <b>-TreatAsAuthenticated</b> \$true</p>	<p><b>-Identity:</b> defines the name of the trusted application pool and the name should be DNS FQDN.</p> <p><b>-ComputerFqdn:</b> defines the YMS DNS FQDN which communicates with the SfB in the trusted application pool.</p> <p>The name of the trusted application pool should be consistent with the name of YMS, because when integrating SfB with YMS, there is only one YMS.</p> <p><b>-Registrar:</b> defines the DNS FQDN of the SfB Front-End Pool to which this trusted application pool belongs.</p> <p><b>-Site:</b> defines the SfB Site ID to which this trusted application pool belongs. Run command <b>Get-CsSite</b> to get the Site ID.</p> <p>Others are the same with the default value.</p> <p><b>Note:</b> When creating a trusted application pool (and a trusted application computer in the next step) in this way, SfB/Lync will issue a warning state: <b>"WARNING: Machine sfb1.5060.space from the topology you are publishing was not found in Active Directory and will result in errors during Enable-CsTopology as it tries to prepare Active Directory entries for the topology machines."</b>, and you should answer Yes to this warning.</p>

Procedure	Command	Syntax description
3. Add other trusted applications to the trusted application pool.	<p>New-CsTrustedApplication -  <b>ApplicationId</b> &lt;Application ID&gt; -  <b>TrustedApplicationPoolFqdn</b> &lt;YMS DNS FQDN&gt; -<b>Port</b> &lt;Available Port&gt;</p> <p><b>Example command:</b></p> <p>New-CsTrustedApplication -<b>ApplicationId</b> sfb1 -<b>TrustedApplicationPoolFqdn</b> sfb1.5060.space.space -<b>Port</b> 5067</p>	<p><b>-ApplicationId:</b> defines a friendly identifier for the YMS. You can customize the name and it is unique.</p> <p><b>-TrustedApplicationPoolFqdn</b> : defines the trusted application to pool to which this YMS belongs.</p> <p><b>-Port:</b> 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.</p>
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 a registrar to which you want to add the static routing configuration. If there is no desired registrar, run the command 6.	Get-CsStaticRoutingConfiguration	None
6. Create a new static routing configuration for the desired registrar.	<p>New- CsStaticRoutingConfiguration –<b>Identity</b> "Service:Registrar: &lt;Front End Pool DNS FQDN&gt;"</p> <p><b>Example command:</b></p> <p>New- CsStaticRoutingConfiguration –<b>Identity</b> "Service:Registrar:xiamenpool.xiamen.yealinksfb.com"</p>	<p><b>-Identity:</b> defines the registrar to which we want to apply the static routing configuration.</p>

Procedure	Command	Syntax description
7. Create the static SIP domain route, and associate this route with a trusted application.	<pre>\$newroute = New-CsStaticRoute -TLSSRoute -Destination&lt;YMS DNS FQDN&gt; -Port &lt;YMS Port&gt; -MatchUri &lt; YMS DNS FQDN&gt; -UseDefaultCertificate \$true</pre> <p><b>Example command:</b></p> <pre>\$newroute = New-CsStaticRoute -TLSSRoute -Destination "sfb1.5060.space" -Port 5067 -MatchUri "sfb1.5060.space"</pre>	<p><b>-Destination:</b> defines the YMS DNS FQDN where SfB should send SIP requests matching the domain specified in <b>-MatchUri</b>.</p> <p><b>-Port:</b> defines the 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.</p> <p><b>-MatchUri:</b> defines the matched YMS DNS FQDN.</p>
8. Apply your required static route to your registrars' static routing configuration.	<pre>Set-CsStaticRoutingConfiguration -Identity "Service:Registrar: &lt;Front End Pool DNS FQDN&gt;" -Route @{Add=\$newroute}</pre> <p><b>Example command:</b></p> <pre>Set-CsStaticRoutingConfiguration -Identity "Service:Registrar:xiamenpool.xiamen.yealinksfb.com" -Route @{Add=\$newroute}</pre>	<p><b>-Identity:</b> defines the registrar to which we want to apply the static routing configuration.</p> <p>Others are the same with the default value.</p>
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](#) .

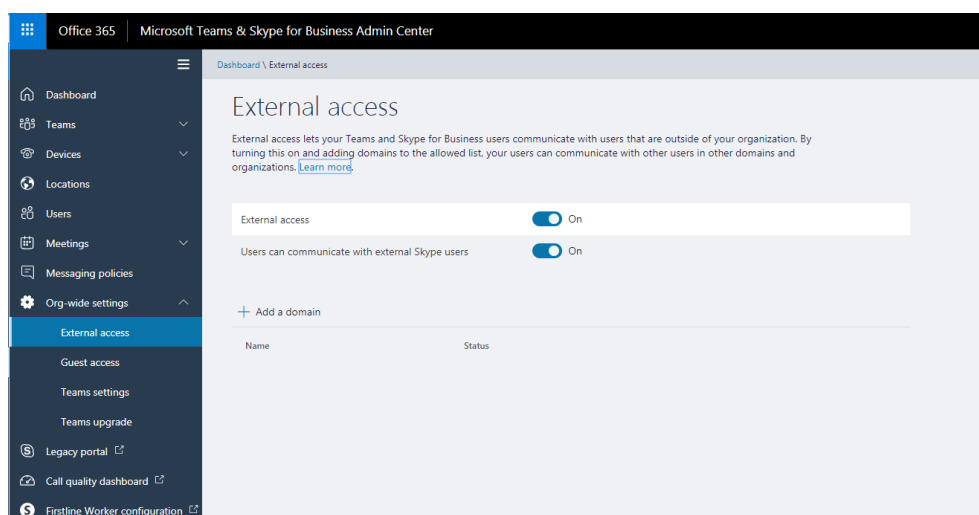
Note that you need enable the federation on Microsoft Office 365.

- [Configuring Microsoft Office 365](#)

### Configuring Microsoft Office 365

#### Procedure

1. Make sure that the federation is enabled on Office 365.



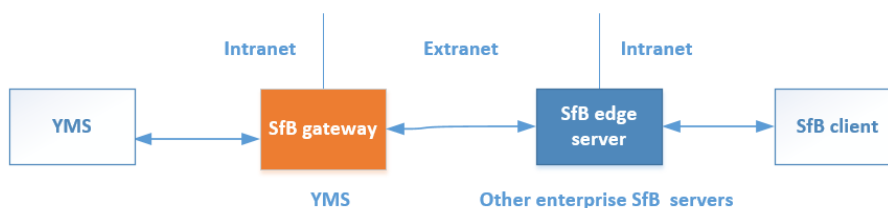
2. Make sure that the SRV record and the A record of YMS and SfB is configured on the public DNS server.

## Communicating with Other Enterprise SfB Servers

The YMS device communicate with the SfB device 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.

```

Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping sip.yealinksfb.com

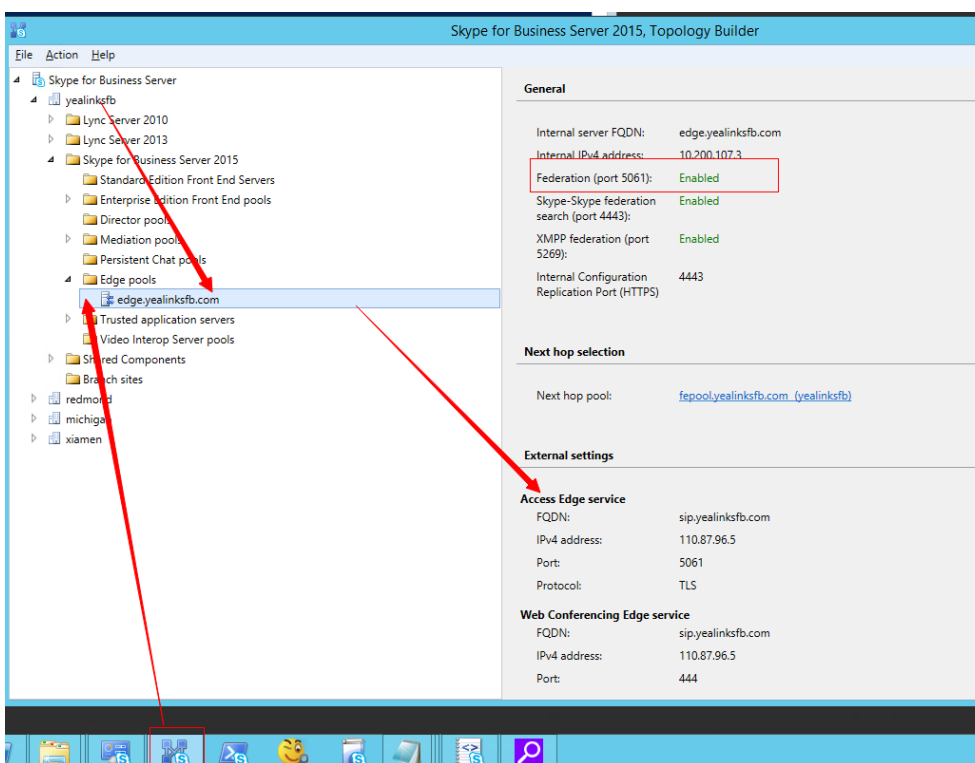
Pinging sip.yealinksfb.com [110.87.96.5] with 32 bytes of data:
Reply from 110.87.96.5: bytes=32 time<1ms TTL=128
Reply from 110.87.96.5: bytes=32 time<1ms TTL=128
Reply from 110.87.96.5: bytes=32 time<1ms TTL=128
Reply from 110.87.96.5: bytes=32 time<1ms TTL=128

Ping statistics for 110.87.96.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>_

```

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

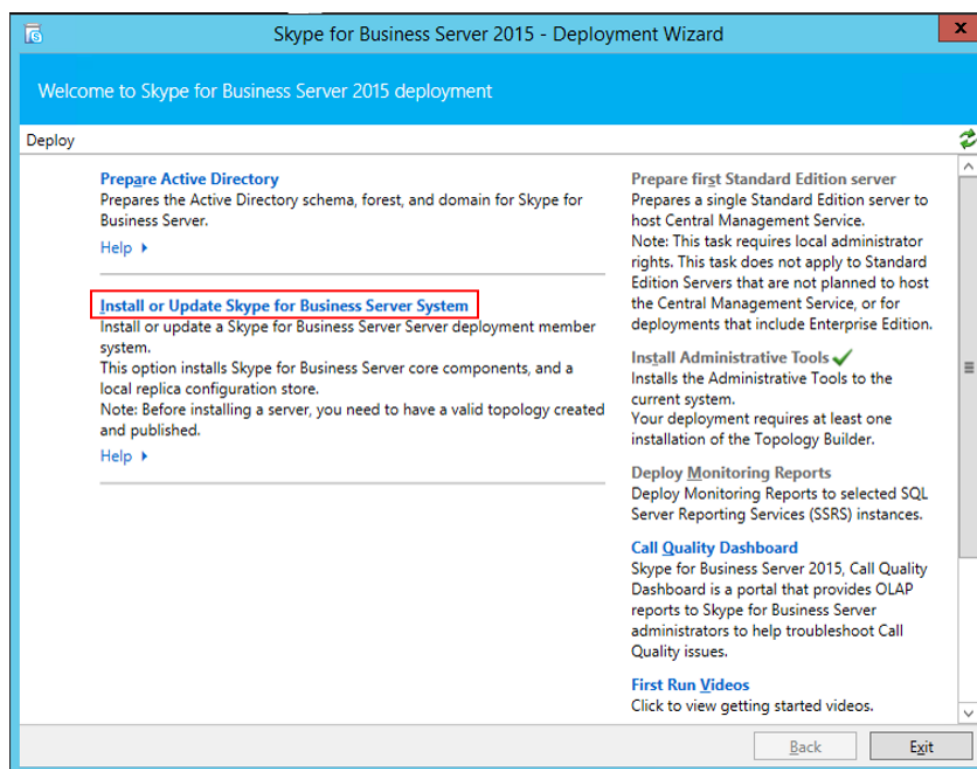


2. Make sure that the SRV record and the A record of both YMS and SfB are configured on the public DNS server.
  - Log into the public DNS server where the SfB edge server is located to view the SRV record and the A record. The host machine record must be `_sipfederationtls_tcp` in the SRV record.

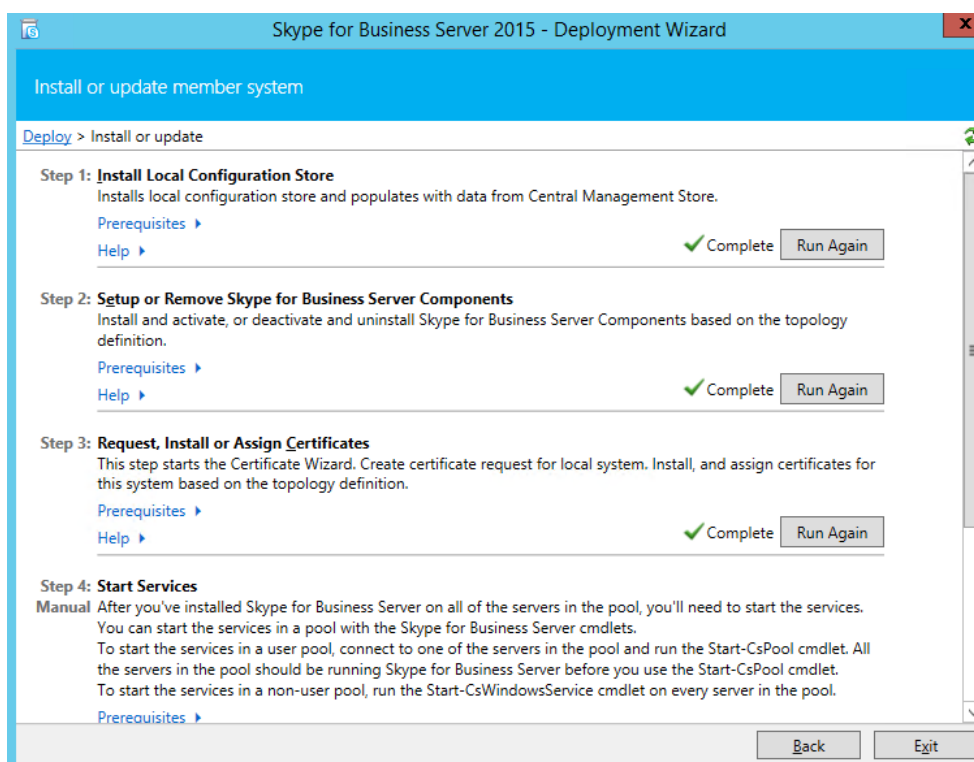


<input type="checkbox"/>	A	sip	默认	110.87.96.5
<input type="checkbox"/>	A	sipexternal	默认	110.87.96.5
<input type="checkbox"/>	SRV	_sip_tls	默认	0 100 5061 sip.yealinksfb.com
<input type="checkbox"/>	SRV	_sipfederationtls_tcp	默认	0 100 5061 sip.yealinksfb.com
<input type="checkbox"/>	SRV	_sip_tcp	默认	0 0 5060 sip.yealinksfb.com

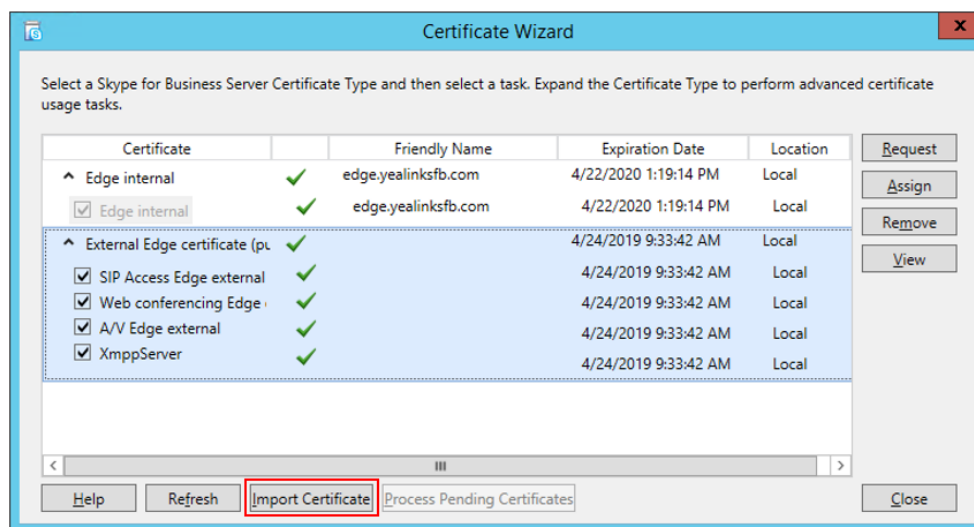
- Log into the public DNS server where the YMS is located to view the SRV record and the A record. The host machine record must be \_sipfederationtls\_tcp in the SRV record.
3. Make sure that you purchase the certificate of the SfB edge server from a trusted third-party organization. The procedure of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



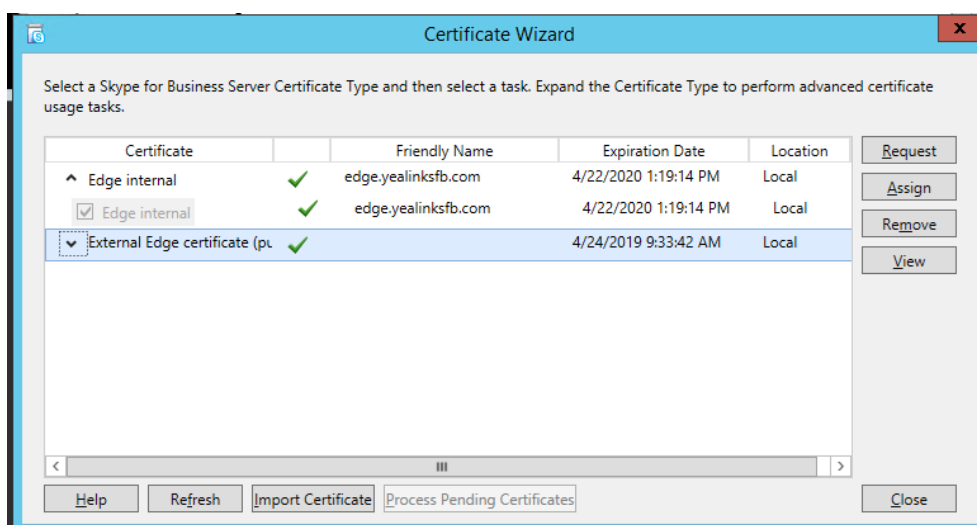
- b) Click **Run Again**.



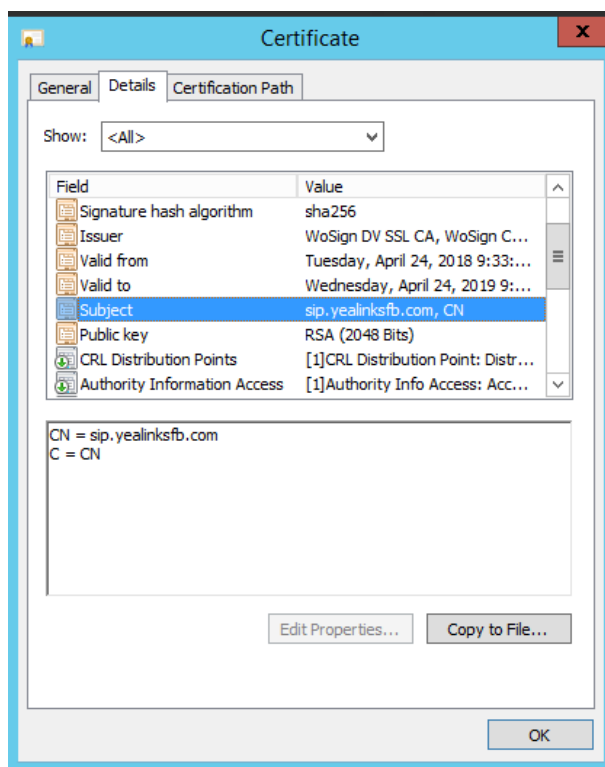
c) Click **Import Certificate** and import the external edge certificate.



After importing, the page is shown as below:

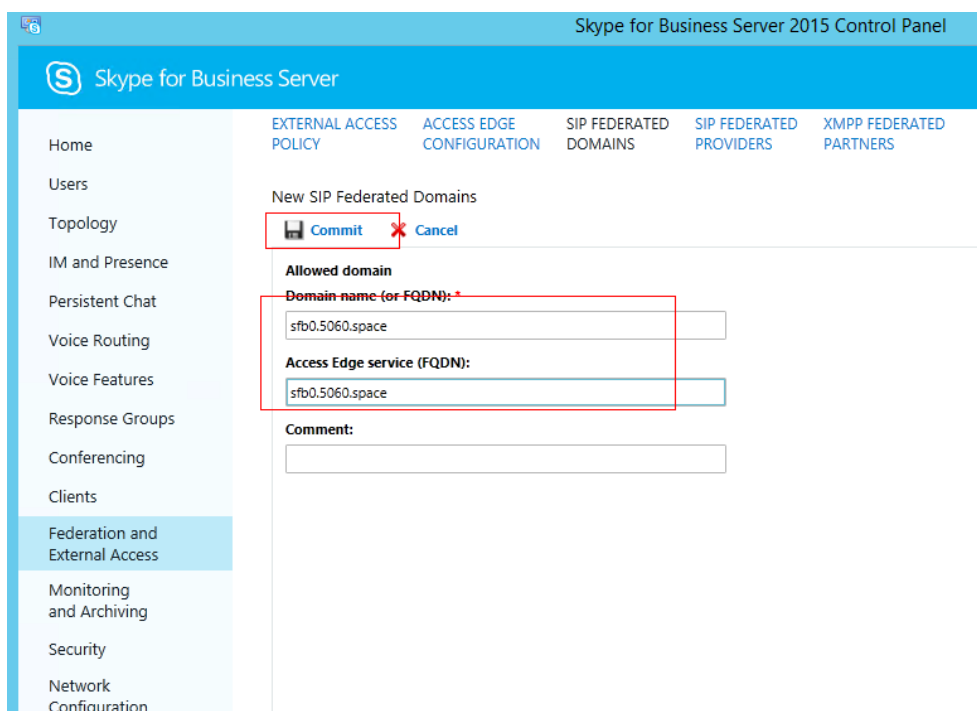
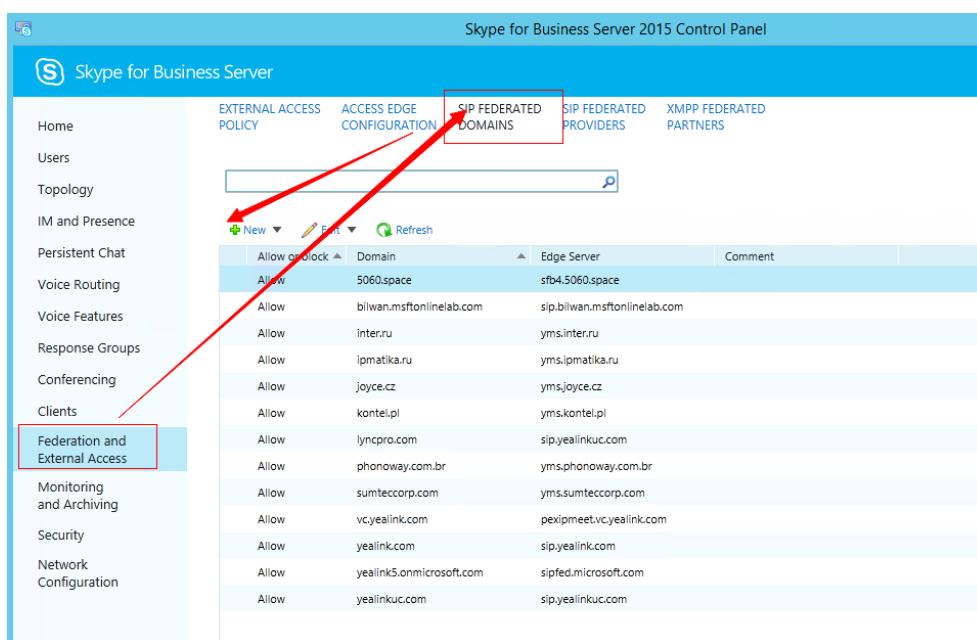


- d) Select the imported edge server certificate, click **View**, and make sure that the user name (commonName attribute) or the user optional name (altNames attribute) must contain the FDQN name of the edge server.



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 DNS 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

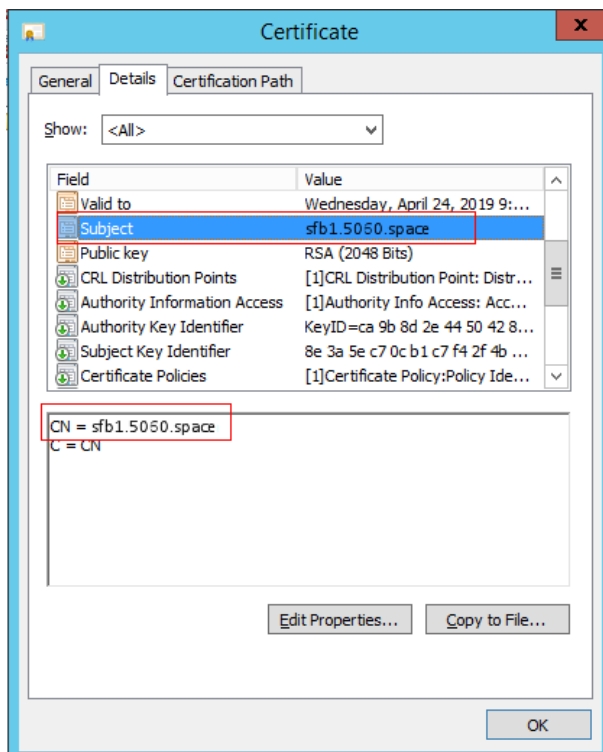
Make the SfB server trust this YMS by [Importing the TLS Certificate](#) on this YMS.

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 server, 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 business node.



- The certificate should contain the public key and the private key.

```
-----BEGIN CERTIFICATE-----
MIIECzCCA1ugAwIBAgIJALSy12RyrkNWMA0GCSqGSIb3DQEBBQUAME8xEzARBgoJ
kiaJk/IsZAEZFgNjb20xGjAYBgGjKiaJk/IsZAEZFgP5ZWfSaW5rc2ZiMRwGgYD
VQQDExN5ZWfSaW5rc2ZiLUFELUNBLUNBMB4XDTE3MTIyODAyMTIOM1oXDTI3MTIy
NjAyMTIOM1owGzAxZAJBGNVBAYTAkNOMQ8wDQYDVQQIEwZGdWppYW4xDzANBgNV
BAcTB1hpYW1lbjEQMA4GA1UEChMHWWVhbG1uazELMAkGA1UECmMCSVQxH2AdBgNV
BAMTFnBleGlwMm11ZXQueWVhbG1uay5jb20xH2AdBgkqhkiG9w0BCQEWEG1pbG9A
eWVhbG1uay5jb20wgGElMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCephdy
ddIJ9Rh/Ykx7kksD4bxK+qz50LLcIwY/qPI7ZcPUD0kf+zzd07/AQQkjza/c2gF
36R3oUBwrqJRRUZhdyHhXRyR/+wOCHrmcCkKPKLSmpKexjxTzd/x3Eq1MyM4jD8j
TbTbRLjt3dZum203a5gBzja2wnFwexQ7Fmb6e4EnViW7FNfDftrrlsQEcnUCDbc
bo+7LIPDPpP/trpYDB8U4fNuVHjko455jwTz3/wdsTwbosDISX46nywn01K8QpEB
9QlFKg1A6/Tzp5yNhoT6Zx0szAdOVZ6EBh0dZc8fduNiS8rIrVj+8Bfj14VktG2
eOJubaQcxHtZQ7k3AgMBAAAgggEOMIIBCjAMBGNVHRMEBTADAQH/MIHNBGNVHREE
gcUwgcKCFnBleGlwMm11ZXQueWVhbG1uay5jb22CD1NGQjAuNTA2MC5zcGFjZyYIP
U0ZCMS41MDYwLnNwYWNlGg9TRkIyLjUwNjAuc3BhY2WCD1NGQjMuNTA2MC5zcGFj
ZyYIPU0ZCNC41MDYwLnNwYWNlGg9TRkI1LjUwNjAuc3BhY2WCD1NGQjYuNTA2MC5z
cGFjZyYIPU0ZCNy41MDYwLnNwYWNlGg9TRkI4LjUwNjAuc3BhY2WCD1NGQjkuNTA2
MC5zcGFjZTAdBgNVHQ4EFgQUxXmjM3vh1JEgQX2WpmFTpNEJZcoowCwYDVR0PBAQD
AgXgMA0GCSqGSIb3DQEBBQUAA4IBAQBtP42PO5TXqPNvEqn1O4QcEBXbukKMeR0Q
CqxksUVyudOQ/5qqyd6x9K1M/6BmAS2Fi/1463PaoiQEZDAbDHw0UyAvisOyUDDw
WYEAy2vIe2tvE/NW7TFysWgHPWcvjLN91wtLNDVjJkb7r4Et7//TnRc5oHL5ok9
En43cfZ3inev1HgFhne3C6iHVip5X4T7rZ05j9G51QYp9Jw4GwiCT2syP2D010u/
Yf6h/yIwnYLE3s4MFwqk4fRjH8p+aCjabhjxUPWvk7PCctmaceWUg1VRDIgZB4L
xSzPaeywK+qgvYfAQFTB2OpAxVBXHbSwo/6oPmtvJso50R+Qdt
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAqYXcnXSCsfUYf2JMe5JLA+G8Svqs+dCy3CMGP6jyO2XD1Hd
JH/s83dO/wEEJI82v3GYBd+kd6FACk6iUUVGyXch4cUWK//sDgh65nApCjyi0pqs
```

## Procedure

- Click **Service > SIP Service > Skype for Business > Add**.
- Configure the basic parameters.

**Table 33: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable the SfB gateway server. <b>Default:</b> enabled.
<b>Name</b>	The name of SfB gateway.
<b>Node</b>	The node used by this SfB gateway.
<b>Network</b>	The IP address of this node.
<b>Transport protocol</b>	Only TLS is available if communicating with SfB.
<b>FQDN</b>	The name of YMS. Example: sfb1.5060.space <b>Method:</b> add this domain name on DNS server to which the A record of YMS is added.
<b>Port</b>	The source port on YMS that communicates with the SfB server.  <b>Note:</b> the value can be any integer from 0 to 65535. This port must be consistent with the port configured in SfB server and cannot be occupied. <b>Default:</b> 5067.  If the SfB enables federation, this port should be 5061. First of all, change the registration port to other port, and set the port as 5061, otherwise the port will be closed by the firewall.
<b>Domain</b>	The domain name of SfB server. For example: xiamen.yealinksfb.com.
<b>Port</b>	The source port on the SfB server that communicates with YMS. <b>Default:</b> 5061.
<b>Federation</b>	Enable or disable the federation. <b>Default:</b> disabled.  According to different SfB servers, you can enable or disable the federation in one of the following scenarios: <ul style="list-style-type: none"> <li>• If the SfB server is the local SfB server, you can disable the federation.</li> <li>• If the SfB server is Microsoft Office 365 or other enterprise SfB servers, you can enable federation.</li> </ul>
<b>Outbound proxy</b>	Enable or disable it to allow the SfB server to send requests to the outbound proxy server. <b>Default:</b> disabled.

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

3. Configure the security policy.

**Table 34: Parameters of the Security Policy**

Parameter	Description
<b>Enable security policy</b>	Enable or disable the security policy. <b>Default:</b> disabled.
<b>Mode</b>	Select a mode. The supported modes are as follows: <ul style="list-style-type: none"> <li><b>Whitelist:</b> allowing the person in this group to call into.</li> <li><b>Blacklist:</b> forbidding the person in this group to call into.</li> </ul>
<b>Security Group</b>	Select a security group.

4. Configure the outgoing call rule.

Outgoing call rule

Priority :
Callee regex match :
Callee regex replace string :

1
^888(d+}@
y!\$1@xiamen.yealinksfb.com

+ Add

Priority :
Caller regex match :
Caller regex replace string :

1
(.+}@
\$1@sfb1.5060.space

+ Add

Priority :
SfB conference regex match :
SfB conference regex replace string :

1
^666(d+}@
\$1@xiamen.yealinksfb.com

+ Add

Account 3802 registered in the local YMS can dial "888751" to call SfB account y!751@xiamen.yealinksfb.com.

Make the caller ID displayed in the remote call or conference as "3802@sfb1.5060.space" but " 3802".

Account 3802 registered in the local YMS can dial "66671920" to join SfB conference 71920@xiamen.yealinksfb.com.

5. Configure the incoming call rule.

**Incoming call rule**

Priority :	Callee regex match :	Callee regex replace string :
1	(+ )@	\$1@10.86.0.220.xip.io
<a href="#">+ Add</a>		

SfB account yl751@xiamen.yealinksfb.com can dial "3802" to call the account 3802 registered in the local YMS (IP address 10.86.0.220.xip.io).

Priority :	Caller regex match :	Caller regex replace string :
1	yl(d+ )@	888\$1@10.86.0.220.xip.io
<a href="#">+ Add</a>		

Make the caller ID displayed in the local call as "888751@10.86.0.220.xip.io" but "yl751@xiamen.yealinksfb.com".

Priority :	SfB conference regex match :	SfB conference regex replace string :
1	yl(d+ )@	666\$1@10.86.0.220.xip.io
<a href="#">+ Add</a>		

Make the caller ID displayed in the local conference as "666751@10.86.0.220.xip.io" but "yl751@xiamen.yealinksfb.com".

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 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 35: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.



Parameter	Description
<b>External media port</b>	Configure the port range for the SFB gateway media service.  <b>Default port range:</b> 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.
<b>All local networks</b>	The IP address used by this service.

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

## Configuring the GK Service

You can configure the GK service, so that a YMS Account can be registered in the H.323 device, therefore, 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 36: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable it to allow the server to send registration request to the GK server.  <b>Default:</b> enable.
<b>Name</b>	The server name.
<b>Node</b>	The server
<b>GK ID</b>	The network ID of the GK server in which YMS is registered.
<b>TTL timeout duration</b>	After YMS is registered at 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.  <b>Default:</b> 600 seconds.

Parameter	Description
<b>TTL timeout duration</b>	<p>The GK can decide whether or not the server can be called according to IRR (Information Request Response) sent by the server.</p> <p><b>Default:</b> 120 seconds.</p>
<b>RAS broadcast port (UDP)</b>	It defaults to 1718 and is not configurable.
<b>RAS port (UDP)</b>	It defaults to 1719 and is not configurable.
<b>H.225 listener (TCP)</b>	It defaults to 1722 and is not configurable.
<b>Q.931/H.245(TCP)</b>	<p>Configure the range of the Q.931/H.245 port used by the registration service.</p> <p><b>Default port range:</b> from 20000 to 23999. To avoid the port conflict, the gap between the maximum port and the minimum port should be not less than 200. For example, you set 20000 as the minimum port, the maximum port should be not less than 20199.</p>
<b>Media forwarding port ( UDP )</b>	<p>Specify the range of the media forwarding port.</p> <p><b>Default port range:</b> from 20000 to 29999. To avoid the port conflict, the gap between the maximum port and the minimum port should be not less than 200. For example, you set 20000 as the minimum port, the maximum port should be not less than 20199.</p>
<b>H.225 listener</b>	It defaults to 1721 and is not configurable.
<b>Q.931/H.245(TCP)</b>	<p>Configure the range of the Q.931/H.245 port used by the conference gateway.</p> <p><b>Default port range:</b> from 24000 to 26999. To avoid the port conflict, the gap between the maximum port and the minimum port should be not less than 200. For example, you set 24000 as the minimum port, the maximum port should be not less than 24199.</p>
<b>H.235 encryption</b>	<p>The supported types are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Optional</b>—negotiate with the remote whether or not H.235 encryption can be used in H.323 calls.</li> <li>• <b>Compulsory</b>—H.235 encryption has to be used in H.323 calls.</li> <li>• <b>Disable</b>—H.235 encryption cannot be used in H.323 calls.</li> </ul> <p><b>Default:</b> disable.</p>

Parameter	Description
<b>H.239</b>	Enable or disable the H.239.  <b>Default:</b> enable. 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.

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

## Configuring the H.323 Gateway

You can configure the H.323 gateway and [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 it in 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 37: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable the H.323 gatekeeper. <b>Default:</b> enable.
<b>Name</b>	The server name.
<b>Node</b>	The server.
<b>Username</b>	The authentication ID used by this gateway.
<b>GK address</b>	Configure the registration timeout (in seconds) on YMS.  If the time is out, YMS will send the registration request to the embedded GK server again. <b>Default:</b> 600 seconds.
<b>GK authentication</b>	It is the timeout of the status response message, which is sent by the H.323 gateway to the built-in GK server according to the interval or IRO set by the ACF command. <b>Default:</b> 120 seconds.
<b>GK auth name</b>	It defaults to 1718 and is not configurable.
<b>GK auth password</b>	It defaults to 1719 and is not configurable.
<b>H.225 listener (TCP)</b>	The H.225 listener should be 1722.

Parameter	Description
<b>Q.931/H.245(TCP)</b>	Configure the range of Q.931/H.245 port under YMS H.323 gatekeeper.  <b>Default port range:</b> from 20000 to 23999. To avoid the port conflict, the gap between the maximum port and the minimum port should be not less than 200. For example, you set 20000 as the minimum port, the maximum port should be not less than 20199.
<b>H.235 encryption</b>	The supported types are as follows: <ul style="list-style-type: none"> <li>• <b>Optional</b>—negotiate with the remote whether or not H.235 encryption can be used in H.323 calls.</li> <li>• <b>Compulsory</b>—H.235 encryption has to be used in H.323 calls.</li> <li>• <b>Disable</b>—H.235 encryption cannot be used in H.323 calls.</li> </ul> <b>Default:</b> disable.
<b>H.239</b>	Enable or disable the H.239.  <b>Default:</b> enable. 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.
<b>H.460</b>	Enable or disable the H.460 protocol to support firewall traversal for H.323 signaling.

3. Click **Advanced Option**, and configure the outgoing call rules.

Outgoing Rule :

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

The H.323 device 3501 registered in YMS (IP address 10.86.0.33.xip.io) can dial "003701" to call the H.323 device 3701 registered in YMS (IP address 10.86.0.201.xip.io).

Make the caller ID displayed in the remote party as "95588" but "3501".

4. Configure the incoming call rules.

Incoming Rule :

Priority :	Incoming regex match :	Incoming regex replace string :
1	^11(id{4})	\$1@10.86.0.33.xip.io
<a href="#">+ Add</a>		

The H.323 device 3701 registered in YMS (IP address 10.86.0.201 ) can dial "113501" to call the H.323 device 3501 registered in YMS (IP address 10.86.0.33.xip.io ).

Priority :	Outgoing regex match :	Outgoing regex replace string :
1	^3701	96866
<a href="#">+ Add</a>		

Make caller ID displayed as "96866" but "3701".

- Click **Save**.
- Operate according to 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

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

**Table 38: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.
<b>External media port</b>	The port range of the interactive media service. <b>Default port range:</b> from 50000 to 54999. To avoid the port conflict, the gap between the maximum port and the minimum port should be not less than 200. For example, you set 50000 as the minimum port, the maximum port should be not less than 50199.
<b>All local networks</b>	The IP address used by this service.

- Click **Save**.

4. Operate according to 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 39: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.
<b>External media port</b>	The port range of the broadcast media service. <b>Default port range:</b> from 55000 to 59999. To avoid the port conflict, the gap between the maximum port and the minimum port should be not less than 200. For example, you set 55000 as the minimum port, the maximum port should be not less than 55199.
<b>All local networks</b>	The IP address used by this service.

3. Click **Save**.
4. Operate according to 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 40: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.

Parameter	Description
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.
<b>External media port</b>	The port range of the RTMP media service.  <b>Default port range:</b> from 60000 to 60999. To avoid the port conflict, the gap between the maximum port and the minimum port should be not less than 200. For example, you set 60000 as the minimum port, the maximum port should be not less than 60199.
<b>All local networks</b>	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 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 participants, you can configure the media bypass service.

#### Procedure

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

**Table 41: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable this service.  <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.
<b>External media port</b>	The port range of the media bypass service.  <b>Default port range:</b> from 64000 to 64999. To avoid the port conflict, the gap between the maximum port and the minimum port should be not less than 200. For example, you set 64000 as the minimum port, the maximum port should be not less than 64199.
<b>All local networks</b>	The IP address used by this service.

3. Click **Save**.
4. Operate according to 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 42: Basic Parameter**

Parameter	Description
<b>Enable</b>	Enable or disable this service. <b>Default:</b> enable.
<b>Name</b>	The service name.
<b>Node</b>	The node used by this service.
<b>Listener (UDP &amp; TCP)</b>	Select the desired listener. <b>Default:</b> 3478.
<b>Spare listener (UDP &amp; TCP)</b>	Select the desired spare listener. <b>Default:</b> 3479.
<b>Relay port range</b>	Configure the range of the range port. <b>Default port range:</b> from 40000 to 49999. To avoid the port conflict, the gap between the maximum port and the minimum port should be not less than 200. For example, you set 40000 as the minimum port, the maximum port should be not less than 40199.

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

### Related concepts

[Introduction of the Deployment Structure](#)



## Call Settings

---

- [Call Control Policy](#)
- [Video Display Policy](#)
- [Restricting the Dialing 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 the Audio IVR language](#)
- [Configuring the Time for Joining Conference Beforehand](#)
- [Enabling Auto Dialing](#)
- [Enabling the Auto Redialing](#)
- [Displaying the Native Video](#)
- [Setting the Last Participant Backstop Timeout](#)
- [Setting the Auto End Conference Without Moderator](#)
- [Enabling the Content Only](#)
- [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 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 43: Parameters of video resolution**

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

3. Click **Save**.
4. Operate according to 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 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, the participants cannot place video calls to join the conference (except the permanent 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 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, the participants cannot place audio call to join the conference (except the permanent 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 prompts, and click **OK**.

## Setting the Audio 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 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.  
The default value is 60 minutes.
3. Click **Save**.
4. Operate according to 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 devices registered with YMS accounts and other third-party devices in the enterprise directory.

### About this task

The supported devices are: the VC880/VC800/VC500/VC400/VC200/VC120/VC200 videoconferencing system, SIP VP-T49G IP phone, SIP-T58V IP phone, and other 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 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 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 prompts, and click **OK**.

## Setting the Last Participant Backstop Timeout

If there are only the last participant staying 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 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 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 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 prompts, and click **OK**.

## Enabling the Content Only

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

### 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 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.  
the default address is <https://ios.push.yealinkvc.com:8443>.
3. Click **Save**.
4. Operate according to 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 enable 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 prompts, and click **OK**.

### Related tasks

[Configuring the Broadcast Media Service](#)

### Related information

[Activating a License](#)

## Configuring the RTMP Live

To allow users to watch the live conference, you can enable the **RTMP live**.

### Before you begin

- You obtain the information about You Tube live streaming service.
- [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 44: RTMP live parameters**

Parameter	Description
<b>Organizer Logo</b>	The logo displayed on the Live Broadcast page.
<b>Domain</b>	The domain name of the live server.
<b>Application name</b>	The application name in the authentication URL.
<b>Live domain</b>	The live video domain name.
<b>Enable GK authentication</b>	Enable or disable the authentication. <b>Default:</b> disable.
<b>Authentication key</b>	The authentication password.

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

### Related tasks

[Configuring the RTMP Media Service](#)

## Enabling the Conference Recording

If you enable the **Recording** feature, you can configure the recording server to record conferences.

### About this task

Before you configure the recording server, make sure that Yealink technical support engineer has deployed the 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 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 manage the packet loss when transmitting the audio and video packets. The value should be consistent with the one set in the switch or 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 prompts, and click **OK**.

## Video Display Policy

---

- [Setting the Default Layout](#)
- [Setting the 1+N Video Layout](#)
- [Setting the Equal N×N Video Layout](#)
- [Displaying the Participant Name](#)
- [Displaying the Participant Status](#)
- [Displaying the Participant Quantity](#)

## Setting the Default Layout

You can set the default conference layout, which takes effect for the participants in Meeting Now conferences, the participants in schedule conference of discussion mode, and the moderators in scheduled conference of training mode.

### Procedure

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

**Table 45: Parameters of the Default Layout**

Parameter	Description
Default layout	<p>The supported layouts are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Equal N×N</b>: participants are displayed in an equal image.</li> <li>• <b>1+N</b>: the first participant is given the prominence with the largest pane, and other participants are displayed in a strip around the first participant.</li> </ul> <p><b>Default:</b> 1+N.</p>

3. Click **Save**.

## Setting the 1+N Video Layout

In 1+N video layout, if the number of the current participants exceeds the maximum video images, the video carousel is enabled automatically 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 enable voice-activated feature so that the system will automatically identify the speaking participant. When the participant continues speaking for a specific time, he will be given prominence with the largest pane, other participants will be displayed in a strip around the speaking participant.

### Procedure

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

**Table 46: 1+N Video Layout Parameters**

Parameter	Description
OnePlusN	Configure the max number of small videos displayed in 1+N video layout. <b>Default:</b> 1+7.
	Set the interval per carousel.
	Configure the participant video image 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 Equal N×N Video Layout

In the Equal N×N video layout, if the current participants are more than the maximum video images, 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.

### Procedure

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

**Table 47: Parameters of Equal N×N video layout**

Parameter	Description
Equal N×N	Configure the maximum number of video images in Equal N×N video layout. <b>Default:</b> 4*4.
	Set the interval per carousel.

3. Click **Save**.



## Displaying the 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**

## Displaying the Participant Status

If you want to see status information on the video conference image, like muted/blocked/applying for speaking and so on, you can enable **Display participant name**.

### Procedure

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

## Restricting the Dialing Number

---

You can restrict the dialing number.

Restricting the dialing number: 1. [Add a Number Filter](#) is used to configure the dialing number; 2. [Adding a Call Routing Rule](#) defines 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 48: Basic Parameters**

Parameter	Description
<b>Enable</b>	Enable or disable this rule. <b>Default:</b> enable.
<b>Name</b>	The rule name.
<b>Note</b>	The additional description of this rule.

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

Add ×

\* Type : ☒ Extension section ☐ Regular expression

\* Origin extension :

\* Rear extension :

Description :

**Table 49:**

Parameter	Description
<b>Type</b>	The match type of this number. <ul style="list-style-type: none"> <li><b>Extension section</b></li> <li><b>Regular expression</b></li> </ul>
<b>Origin extension, Rear extension</b>	The length of these two extensions should be the same.
<b>Regular expression</b>	The Perl Compatible Regular Expressions (PCRE).
<b>Description</b>	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 50: Common Perl Compatible Regular Expressions (PCRE) are described as below:**

PCRE	Description
<code>^(1\d{10})\$</code>	Match an 11-digit number which starts with 1. For example: 12345678912
<code>^0(\d+)\$</code>	Match the number (2 or more digits) which starts with 0. For example: 02, 0157
<code>^(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}\$</code>	Match an 11-digit mobile phone number, the first 3 digits includes the following types, the rest digits can be any digits: <ul style="list-style-type: none"> <li>• Start with 13 and the third number is any digit from 0 to 9</li> <li>• Start with 14 and the third number is 5/7</li> <li>• Start with 15 and the third number is 0/1/2/3/5/6/7/8/9</li> <li>• Start with 18 and the third number is 0/1/2/3/5/6/7/8/9</li> </ul> For example: 13012345678, 14512345678, 15987654321 or 18243218765
<code>^(\d{3,4}-)?\d{7,8}\$</code>	The format for matching the number is described as follows: <ul style="list-style-type: none"> <li>• <b>XXX-XXXXXXXX, 10-digit</b></li> <li>• <b>XXX-XXXXXXXX, 11-digit</b></li> <li>• <b>XXXX-XXXXXXXX, 11-digit</b></li> <li>• <b>XXXX-XXXXXXXX, 12-digit</b></li> <li>• <b>XXXXXXXX, 7-digit</b></li> <li>• <b>XXXXXXXX, 8-digit</b></li> </ul> For example: XXXX-XXXXXXXX represents 07311234567 or other 7-digit number

PCRE	Description
<code>\d{3}-\d{8} \d{4}-\d{7}</code>	<p>The format for matching the number is described as follows:</p> <ul style="list-style-type: none"> <li>• <b>XXX-XXXXXXXX, 11-digit</b></li> <li>• <b>XXXX-XXXXXXXX, 11-digit</b></li> </ul> <p>For example: XXX-XXXXXXXX represents 012-12345678 or other 11-digit number, XXXX-XXXXXXXX represents 0123-1234567 or other 11-digit number</p>
<code>(\d{11}) ((\d{3,4})-(\d{7,8})-(\d{1,4}))?</code>	<p>The format for matching the number is described as follows:</p> <ul style="list-style-type: none"> <li>• <b>11-digit mobile phone number</b></li> <li>• <b>XXXXXXXX, 8-digit number</b></li> <li>• <b>XXXXXXXX, 7-digit number</b></li> <li>• <b>XXX/XXXX-XXXXXXXX/XXXXXXXX, 4 formats in total</b></li> <li>• <b>XXX/XXXX-XXXXXXXX/XXXXXXXX-X/XX/XXX/XXXX, 16 formats in total</b></li> <li>• <b>XXXXXXXX/XXXXXXXX-X/XX/XXX/XXXX, 8 formats in total</b></li> </ul> <p>For example: XXXX-XXXXXXXX represents 0731-8784888 or other 11-digit number</p>

Table 51: Regex replace string

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

## Adding a Call Routing Rule

### Procedure

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

**Table 52: Parameters of the Call Routing Rule**

Parameter	Description
<b>Enable</b>	<p>Enable or disable the call routing rule.</p> <p><b>Default:</b> enable.</p> <p>All the disabled rules are ignored, though they are displayed in the rule list.</p>
<b>Name</b>	The name of the call routing rule.
<b>Priority</b>	<p>The priority of the call routing rule. The smaller the number is, the higher the priority is.</p> <p>When you place a call, the server will look up the first appropriate call routing rule according the priority in ascending order.</p>
<b>Destination regex match</b>	<p>The Perl Compatible Regular Expressions (PCRE) used to match the target call number.</p> <p>If the match succeeds, the server will use this call routing rule.</p>
<b>Call target</b>	<p>The call target.</p> <p>The supported type are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Reject</b></li> <li>• <b>IP Call</b></li> <li>• <b>Peer Trunk</b></li> <li>• <b>PSTN</b></li> <li>• <b>SfB</b></li> <li>• <b>Register Trunk</b></li> <li>• <b>H.323 GW</b></li> </ul>
<b>Outgoing location</b>	<p>The gateway used to place the call.</p> <p>If the call number matches this call routing rule, it is called via this gateway.</p>

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

**Table 53:**

Parameter	Description
<b>Mode</b>	<p>Select a mode.</p> <p>The supported modes are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Whitelist:</b> if a call number in this whitelist matches the target regular expression, it will be called by this call routing rule.</li> <li>• <b>Blacklist:</b> even if a call number in this blacklist matches the target regular expression, it will not be called by this call routing rule.</li> </ul>
<b>Caller filtering policy</b>	Select the filtering policy.

4. Click **Save**.
5. Operate according to 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 meet the regular expression set in the call routing rule, your call will be rejected.

### Procedure

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

#### Routing Information

\* Enabled : ?

ON ☒

\* Name :

Rejection

\* Priority : ?

10

(Only 1~200)

#### Rule Settings

\* Destination regex match : ?

^(1\d{10})@

\*Call target :

\*Outgoing location :

Reject

+ Add

3. If you want to forbid 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. Click **Save**.
5. Operate according to prompts, and click **OK**.

## Account Management

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](#)
- [Group Management](#)
- [Adding an User Account](#)
- [Adding a Room System Account](#)
- [Adding Other Account](#)
- [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	Users can log into devices using the account. 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 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	The devices that are added by entering IP address or URL. Those devices do not have 4-digit YMS account.	No limit.

## Group Management

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 an User Account

You can add user account and users can use it to log into YMS.

- [Parameters of User Account](#)
- [Adding an User Account Manually](#)
- [Importing a Batch of User Accounts](#)

## Parameters of User Account

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

Method	Parameter	Description
Adding Manually or adding in batch	Name	The user name.
	Account	The account to log into YMS.
	AD account	If <b>Obtain from AD server</b> is selected, it is the account on AD server 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 is added.



Method	Parameter	Description
	<b>Authority</b>	<p>The user authority.</p> <p>The available rights are as follows:</p> <ul style="list-style-type: none"> <li>• <b>A:</b> this account can see all user accounts, room system accounts, and the permanent VMRs synced to the directory.</li> <li>• <b>B:</b> this account can see only the user accounts, room system accounts, and the permanent VMRs (synced to the directory) in his group and the same level group. If the user is in root node, this account can also see the third-party devices.</li> <li>• <b>C:</b> this account can see only the user accounts, room system accounts, and the permanent VMRs (synced to the directory) in his group.</li> <li>• <b>D:</b> this account can only see himself, and cannot see any meeting room when scheduling conferences.</li> <li>• <b>Custom:</b> you can customize the authority for this account.</li> </ul>
	<b>Email</b>	The user email. It is used to receive the initial password and the conference notification.
<b>Adding Manually</b>	<b>Account Information</b>	<p>If the LDAP feature is enabled, select the way to add account.</p> <p>The supported ways are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Manual:</b> you need add account information manually.</li> <li>• <b>Obtain from AD server:</b> you can obtain the account information from the specified AD server.</li> </ul>
	<b>Obtain</b>	Obtain the AD account name and account number from the specified account on AD server.
	<b>Enable schedule</b>	<p>Enable or disable this account to schedule meeting room or video conference.</p> <p><b>Default:</b> enable.</p>

Method	Parameter	Description
	<b>Enable Meet Now</b>	Enable or disable this account to create a Meet Now conference. <b>Default:</b> enable.
	<b>Enable call authority</b>	Enable or disable this account to use call authority. If it is enabled, the account with lower authority cannot call the account with the higher authority. For example, if the authority of account 2549 is A and account 2550 is B, 2549 can call 2550, but 2550 cannot call 2549. <b>Default:</b> disable.
	<b>Support H.323 registration</b>	If <a href="#">Configuring the GK Service</a> is done, you can enable or disable this account to use H.323 to register at a device. <b>Default:</b> disable.
	<b>GK REG</b>	If this feature is enabled, the account need password to register in GK servers. <b>Note:</b> it is recommended to enable.
<b>Adding in Batch</b>	<b>Password</b>	You can customize the password.

**Related tasks**[Adding an User Account Manually](#)[Importing a Batch of User Accounts](#)[Configuring the LDAP](#)[Editing the Authority](#)**Adding an User Account Manually**

If you want to add a single user account, you can add it manually.

**Procedure**

1. Click **Account > User Account > Add Account**.
2. Configure the parameters.
3. Click **OK**.
4. If you enter the email address, click **Send email**, the account information will be sent to the user by email.



### Add Account Successful

Account :	2584
Name :	Amada
Password :	304107
Group :	Test-2

5. Click **OK**.



**Note:** If you do not add email when adding the user account, you can inform the user of the initial password, and remind the user to change password promptly.

#### Related concepts

[Parameters of User Account](#)

## Importing a Batch of User Accounts

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

#### About this task

You can import up to 5000 user accounts at one time.

#### Procedure

1. Click **Account > User Account > Import**.
2. Click **Download Template** to download the template.
3. Add the user account parameters to the template and save it on your computer.
4. Click the dotted box area to upload the template.
5. Click **OK**.

#### Related concepts

[Parameters of User Account](#)

## Adding a Room System Account

You can add a room system which can be used to associate with the device in the video meeting room.

#### Procedure

1. Click **Account > Room System Account > Add**.
2. Configure the parameters.

Parameter	Description
<b>Account Information</b>	<p>If the LDAP feature is enabled, select the method to add an account.</p> <p>The supported methods are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Manual:</b> you need add the account information manually.</li> <li>• <b>Obtain from AD server:</b> you can obtain the account information from the specified AD server.</li> </ul>
<b>Name</b>	The user name.
<b>Account</b>	The account to log into YMS.
<b>AD account</b>	<p>If <b>Obtain from AD server</b> is selected, it is the account (on AD server) used to obtain the AD account name and the account number.</p> <p>The account on AD server can be obtained from the AD server administrator.</p>
<b>Obtain</b>	Obtain the AD account name and account number from the specified account on AD server.
<b>Email</b>	The user email. It is used to receive the initial password and the conference notification.
<b>Authority</b>	<p>The user authority.</p> <p>The available rights are as follows:</p> <ul style="list-style-type: none"> <li>• <b>A:</b> this account can see all user accounts, room system accounts, and permanent VMRs synced to the directory.</li> <li>• <b>B:</b> this account can see only the user accounts, the room system accounts, and the permanent VMRs (synced to the directory) in his group and the same level group. If the user is in root node, this account can also see the third-party devices.</li> <li>• <b>C:</b> this account can see only the user accounts, the room system accounts, and the permanent VMRs (synced to the directory) in his group.</li> <li>• <b>D:</b> this account can only see himself, and cannot see any meeting room when scheduling conferences.</li> <li>• <b>Custom:</b> you can customize the authority for this account.</li> </ul>
<b>Enable schedule</b>	<p>Enable or disable this account to schedule meeting room or video conference.</p> <p><b>Default:</b> enable.</p>

Parameter	Description
<b>Enable Meet Now</b>	Enable or disable this account to create a Meet Now conference. <b>Default:</b> enable.
<b>Enable call authority</b>	Enable or disable this account to sync the call authority. If it is enabled, the account with lower authority cannot call the account with the higher authority, but the account with higher authority can. For example, if the authority of account 2549 is A and account 2550 is B, 2549 can call 2550, but 2550 cannot call 2549. <b>Note:</b> disable.
<b>Support H.323 registration</b>	If <a href="#">Configuring the GK Service</a> is done, you can enable or disable this account to register at a device via H.323 protocol. <b>Note:</b> disable.
<b>GK REG</b>	Enable or disable this account to use a password to register in GK server. <b>Note:</b> it is recommended to enable.

3. Click **OK**.

4. If you enter the email address, click **Send email**, and the account information will be sent to the user by email.



### Add Account Successful

Account : 3223  
Name : Video room-a  
Password : 899526

Email

OK

5. Click **OK**.

### Related tasks

[Editing the Authority](#)

## Adding Other Account

If you want to invite other devices to join the conference, you can add them into the directory.

- [Parameters of Other Devices](#)
- [Adding Other Account Manually](#)
- [Adding a Batch of Other Accounts](#)

## Parameters of Other Devices

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

**Table 54: Parameters of Other Devices**

Parameter	Description
<b>Name</b>	The name of this device.
<b>Protocol</b>	The call protocol used by the device.
<b>Number</b>	The URL of this device.
<b>Group</b>	The name of the group to which the device belongs.
<b>Email</b>	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 Other Account Manually

If you want to add other account one by one, you can add them manually.

### Procedure

1. Click **Account > Other Account > Add**.
2. Configure the parameters.
3. Click **Save**.

### Related concepts

[Parameters of Other Devices](#)

## Adding a Batch of Other Accounts

If want to add other accounts at one time, you can import other accounts by template (excel file). Note that you cannot customize template, you need download a blank template first.

### Procedure

1. Click **Account > Other Account > Import**.
2. Click **Download Template** to download the template.
3. Enter parameters of other accounts to the template and save it on your computer.
4. Click the dotted box area to upload the template.
5. Click **OK**.

### Related concepts

[Parameters of Other Devices](#)

## 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**.

Test-2  

Selected 2
 Adjust Grouping
 Modify Authority
 GK REG
 Email
 Delete

	Name 	Account 	Status 	Group	GK REG	Device	Operation
<input checked="" type="checkbox"/>	 Mike	2846	Offline	Test-2	No	<a href="#">Details</a>	
<input checked="" type="checkbox"/>	 2888	2888	Offline	Test-2	Yes	<a href="#">Details</a>	

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

## Editing the Authority

You can configure the authority for the user accounts and the room system accounts, including scheduling conference authority, creating Meet Now conference 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 is registered in the device by H.323 protocol, and whether or not the account need a 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 to 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 devices by importing template, you can edit account details in the template, and import this template to YMS to complete editing.

### Procedure

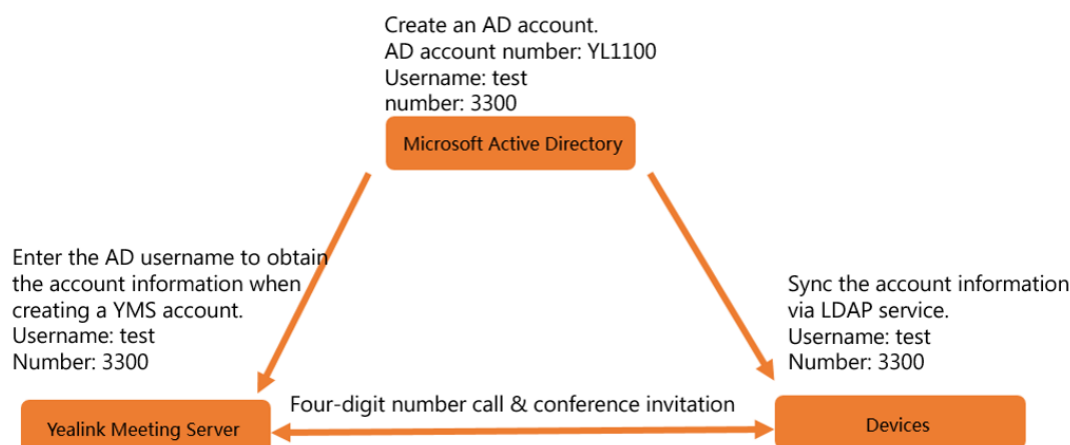
1. Click **Account > User Account/Other Account > Export**.
2. Edit the parameters in the exported file.
3. Click **Import**.
4. Click the dotted box area to upload the template.
5. Click **OK**.

## 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, you 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.

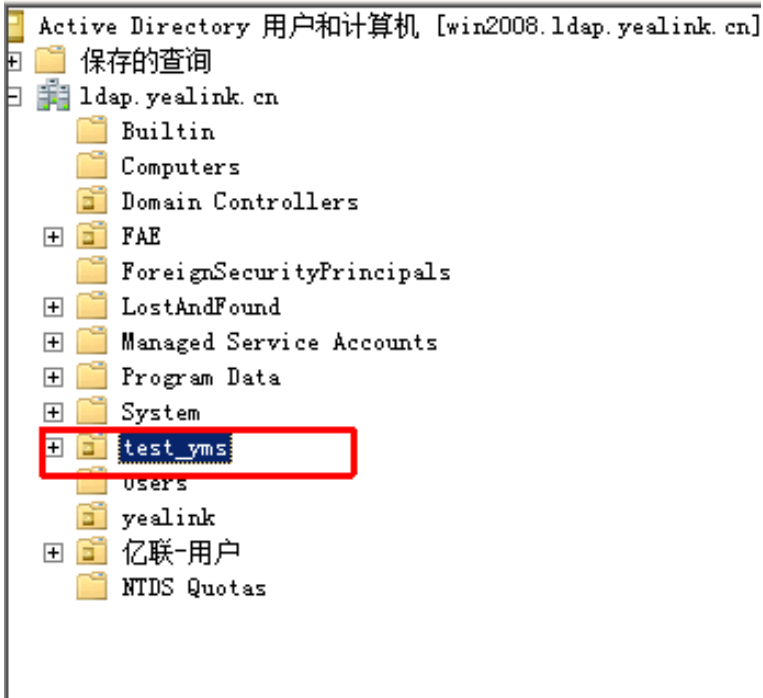


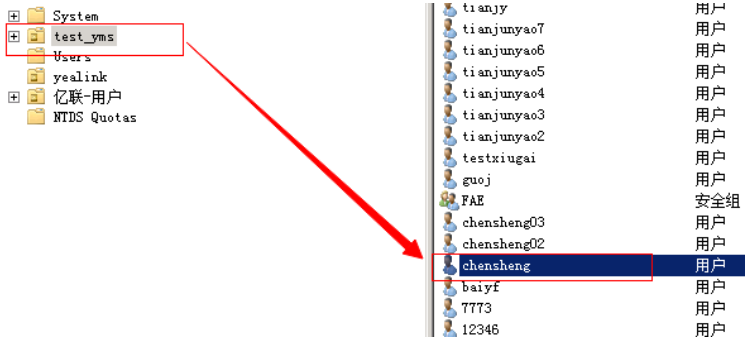
The organizational structure of YMS and LDAP server are independent. If you want to edit the organizational structure, the organizational structure viewed by the third-party devices should be edited via AD server, and the one viewed by YMS devices should be edited via YMS.

## Procedure

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

**Table 55: LDAP parameters**

Parameter	Description
<b>Enable</b>	Enable or disable the LDAP. <b>Default:</b> disable.
<b>Server address</b>	The domain name or IP address of the AD server.
<b>Port</b>	The port of the AD server.
<b>Base DN</b>	<p>The root path that YMS obtains the AD account.</p> <p><b>For example:</b> OU=test_ym,DC=ldap,DC=yealink,DC=cn</p> <p><b>Obtaining method:</b> the image below is the contents of AD server, if you want to obtain the user information under this directory, right click <b>test_ym</b>-&gt;<b>Attribute</b>-&gt;<b>Attribute Editor</b>-&gt; and view the distinguishedname, and the value is OU=test_ym,DC=ldap,DC=yealink,DC=cn. Enter the value in the <b>Base</b> field on YMS.</p>  <p>The screenshot shows the Active Directory console with the following structure:</p> <ul style="list-style-type: none"> <li>Active Directory 用户和计算机 [win2008.ldap.yealink.cn] <ul style="list-style-type: none"> <li>保存的查询</li> <li>ldap.yealink.cn <ul style="list-style-type: none"> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>FAE</li> <li>ForeignSecurityPrincipals</li> <li>LostAndFound</li> <li>Managed Service Accounts</li> <li>Program Data</li> <li>System</li> <li><b>test_ym</b> (highlighted)</li> <li>Users</li> <li>yealink</li> <li>亿联-用户</li> <li>NTDS Quotas</li> </ul> </li> </ul> </li> </ul>

Parameter	Description
<b>Username</b>	<p>The username used to log into the AD server.</p> <p><b>Note:</b> The user name is provided by the AD server administrator.</p> <p>For example, the “chensheng” account in the test_ym contents. The user in the test_ym contents is all acceptable. Username is “chensheng@ldap.yealink.cn”.</p> 
<b>Password</b>	<p>The password used to log into the LDAP server.</p> <p><b>Note:</b> The password is provided by the LDAP server administrator.</p> <p>For example, the AD username is “chensheng@ldap.yealink.cn”</p> <p>Enter the password of this username.</p>
<b>Name attribute</b>	<p>The name attribute of the AD account returned by the LDAP server.</p> <p><b>Example:</b> 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.</p>
<b>Number attribute</b>	<p>The number attribute of the AD account returned by the LDAP server.</p> <p><b>Example:</b> 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 <a href="#">Allocating the Number Resource</a>) and cannot be null. If it does not meet the condition, there will be an error when creating a YMS account by obtaining from the AD server.</p>
<b>AD account attribute</b>	<p>The AD account attribute.</p> <p><b>Example:</b> sAMAccountName</p>

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

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

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

### Related concepts

[Parameters of User Account](#)

# Meeting Room Management

---

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

- [The Entity Meeting Room and the Permanent VMR](#)
- [Managing the Meeting Room Group](#)
- [Adding a General Meeting Room](#)
- [Adding a Video Meeting Room](#)
- [Discussion Mode and Training Mode](#)
- [Adding a Permanent VMR](#)
- [Adjusting the Meeting Room Group](#)
- [Sending Emails about Joining the Conference](#)

## The Entity Meeting Room and the Permanent VMR

---

The meeting room includes the entity meeting room and the permanent VMR.

Difference	Type	Description	
Definition	Entity meeting room	The entity meeting rooms can be used to schedule OA conferences. For more information, refer to <a href="#">Yealink Meeting Server User Guide</a> .	
	Permanent VMR	Users can join the permanent VMR at any time. But the permanent 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.
	Permanent VMR	No	

## Managing the Meeting Room Group

---

In order to manage meeting rooms by group, you can customize the organization relationship according to meeting room location.

The organization root is the enterprise name by default. You can manage meeting rooms in your group and your subordinate groups.

- [Adding the Meeting Room Group](#)
- [Editing/Deleting the Meeting Room Group](#)

## Adding the Meeting Room Group

You can add a group according to the location of meeting room.

### Procedure

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



2. In **Group name** field, enter the group name.
3. In **Upper department**, 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 56:**

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 permanent 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 permanent VMR but are not set as moderators.  If the broadcasting interactive feature is enabled, the guests are the broadcasting parties by default.
Feature Privilege	The moderators can configure the layout during the discussion mode conferences or meet now conferences.		The moderators can configure the layout in the training mode conference, they can also allow/reject/ignore the participant application for speaking and switch the roles between lecturers and moderators/guests.	
	The moderators can edit conferences and delete conferences, and during the conference, they can also send messages, invite participants, invite the third parties, invite participants by email, 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, and leave conferences/end conferences.			
	Other participants can only view the conference details.			

Difference	Discussion Mode	Training Mode
<b>Layout</b>	Moderators and guests can view all participants. For setting the default layout, refer to <a href="#">Setting the Default Layout</a> .	<ul style="list-style-type: none"> <li>The moderators can view all participants by default. For setting the default layout, refer to <a href="#">Setting the Default Layout</a> .</li> </ul> <p>If the broadcasting interactive feature is enabled, the moderators can view all interactive parties by default.</p> <ul style="list-style-type: none"> <li>For 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.</li> </ul> <p>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.</p>
<b>Speaking rule</b>	Free speaking.	All guests and moderators are muted by default. After cancelling the mute status, the moderators can speak. The guests can speak only when the moderators allow their application for speaking.
<b>Contents</b>	All moderators and guests can share contents by default.	Only moderators and lecturers can share contents. The guests cannot share contents.

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

## Adding a Permanent VMR

You can add a permanent VMR, so that users can call into the permanent VMR to join the video conference anytime.

**Before you begin**

You add the meeting room group.

**Procedure**

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

**Table 57: Parameters of the permanent VMR**

Parameter	Description
<b>Mode</b>	The mode of the permanent VMR. For more information, refer to <a href="#">Discussion Mode and Training Mode</a> .
<b>Conference ID</b>	<p>The conference ID used to call into this meeting room.</p> <p><b>Default range:</b> from 20000 to 89999.</p>

Parameter	Description
<b>Password</b>	<p>Enable or disable it to join the conference with the password.</p> <p>If it is enabled, a password is needed to join the conference.</p> <p><b>Default:</b> disable.</p>
<b>Group</b>	The group name of this meeting room.
<b>Moderator</b>	<p>They can control the permanent VMR at any time.</p> <p>For more information, refer to <a href="#">Yealink Meeting Server User Guide</a>.</p>
<b>Favorites</b>	During a conference, you can select the favorites to invite them to join the permanent VMR.
<b>Sync contacts</b>	<p>Enable or disable it to sync this meeting room to the device enterprise directory.</p> <p><b>Default:</b> enable.</p>
<b>Max video parties</b>	<p>The max video parties of this meeting room.</p> <p>Reserving the video party can meet the concurrent needs of other important conferences. If the video parties in this meeting room exceed the max number, the user cannot place a video call to this meeting room.</p>
<b>Max audio-only parties</b>	<p>The max audio-only parties for this meeting room. Reserving the audio party can meet the concurrent needs of other important conferences.</p> <p>If the audio-only parties exceed the max number, the participants cannot place an audio call to this meeting room.</p>
<b>Max video resolution</b>	<p>The max video resolution.</p> <p><b>Default:</b> 720P/30FPS.</p>
<b>Max content resolution</b>	<p>The max content resolution.</p> <p><b>Default:</b> 1080P/5FPS</p>
<b>Max call bandwidth</b>	According to the limit of the enterprise bandwidth, you can limit the media bandwidth sent by YMS to conference participants.
<b>Default layout</b>	The default layout which takes effect for participants in permanent VMRs of discussion mode and for moderators in permanent VMRs of training mode.
<b>Display native video</b>	<p>Enable or disable the native video to be displayed in the conference.</p> <p><b>Note:</b> disable.</p>

Parameter	Description
<b>Content Only</b>	If the device does not support dual-stream protocol, you can enable <b>Content only</b> feature. When other devices share content in a call, this kind of devices can only receive the content and the audio. <b>Default:</b> enable.
<b>Roll call setting</b>	In <b>Training</b> mode, enable or disable it to unmute the participant whose name is called out on the list.  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 <b>Roll call setting</b> . <b>Default:</b> enable.
<b>Broadcasting interactive</b>	In <b>Training</b> mode, enable or disable it to create a broadcasting interactive conference.  If it is enabled, you can create a conference with a large number of participants.
<b>IP Call Blacklist</b>	If it is enabled, the user can join the conference by IP call.
<b>Join with browser</b>	If it is enabled, the user can join the conference by Yealink Web app.

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 permanent 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 single conference in the permanent 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**.

## Conference Management

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

- [Viewing the Conference](#)
- [Viewing the Meeting Room Usage](#)
- [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 permanent VMRs. Conference information contains the subject, the type, the number, the password, the organizer, the start time and the duration.

#### Procedure

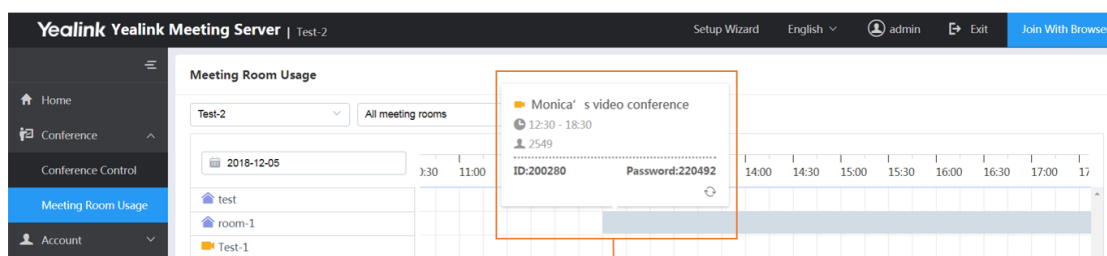
Click **Conference > Conference Control**.

### 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**.



The progress bar in gray means the conference room has been reserved and you cannot reserve it during this time. Hover your mouse over the progress bar, you can view the pop-up window, click the pop-up window and you can view the conference details.

## 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 a recurrence conference, click **Cancel occurrence/Cancel series** to delete conferences.
4. If you want to delete a single conference, click **OK** to delete conferences.

## Controlling the Conference

---

You can control the unoccupied permanent VMRs, the ongoing conference, and the scheduled conference that can join in advance (refer to [Configuring the Time for Joining Conference Beforehand](#)). 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](#)

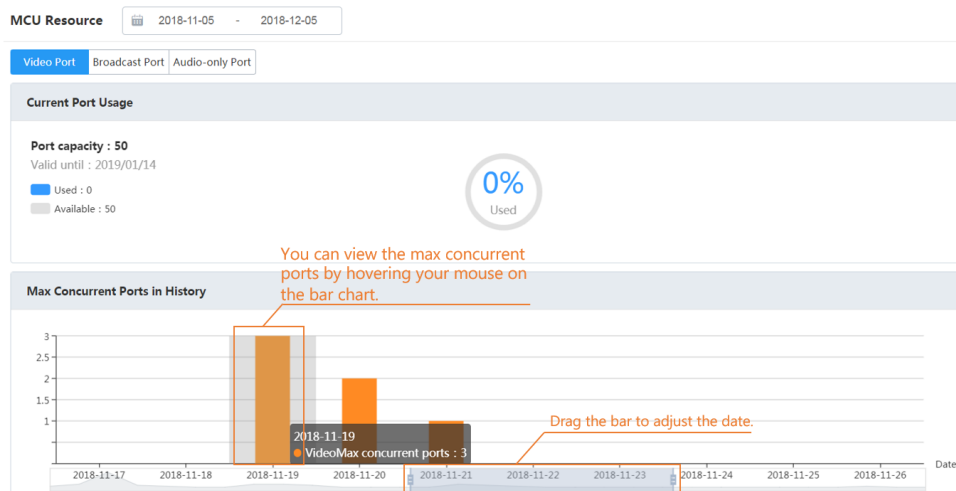
## Viewing the MCU Resource

---

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**.

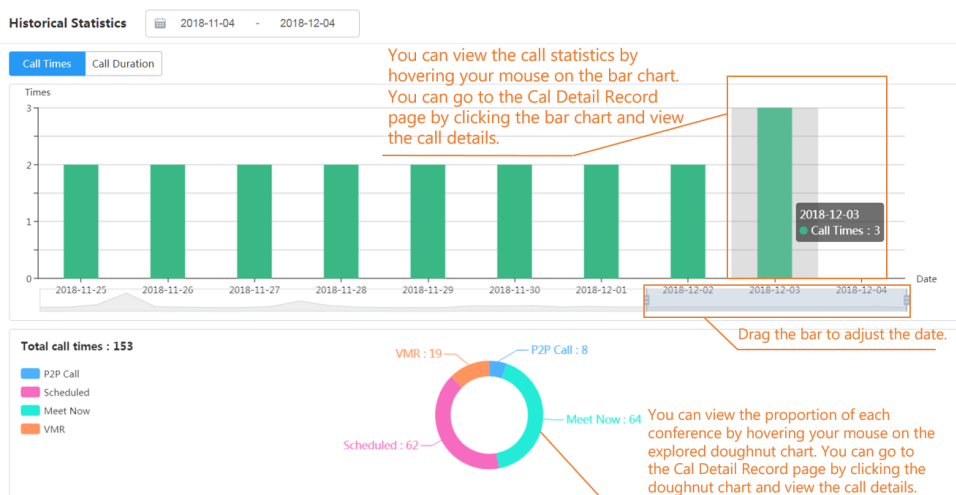


## Viewing the Conference Statistics

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 > Historical Statistics**.
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 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](#)
- [Clearing up All Accounts and the Conference Statistics](#)
- [Viewing the Operation Log](#)
- [Viewing the System Log](#)
- [Viewing the Device 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 contact Yealink to upgrade your YMS to the latest version.

#### Procedure

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

## Enabling the Device Upgrade

After you enable it, you can remotely update VC800/VC500/VC400/VC120/VC110 video conferencing endpoint, SIP VP-T49G IP phone and SIP-T58V IP phone which are registered with the YMS accounts.

### Procedure

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

The screenshot shows the 'Device Upgrade' tab in the 'System Upgrade' section. The 'Enable' checkbox is checked and highlighted with a red box. Below it is a table with columns: File Name, Version, Model, Upload Time, Up to Date, and Operation. The table is currently empty, showing 'No data'.

## 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 of the important information automatically.

### Procedure

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

## Clearing up All Accounts and the Conference Statistics

---

You might need clear up all of the accounts and the conference statistics to solve some problem you may encounter in YMS.

### Procedure

1. Click **Maintenance > System Restart > Clear**.
2. 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 > Export 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 **Operation Log**.

## 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.

Operation Log   System Log   **Device Log**

☒ Enabled   Search    Please select the desired time to export logs :  -

Name	Account	Device Model	IP Address	Online/Offline	Operation
1001	1001	T49G	10.81.48.13	Online	

3. Click on the right side of desired file.

## Troubleshooting

---

- [Users Do Not Receive Emails](#)
- [Users Fail to Register Accounts](#)
- [Failing to Activating a License Online](#)
- [Failing to Activating a License Offline](#)

### 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.

### Users Fail to Register Accounts

---

#### Condition

Users fail to register accounts.

#### Cause

- Account information error.
- The IP address of the user is set as abnormal IP.



## Remedy

### Procedure

1. Check whether or not the account information is correct.
2. Check whether or not the IP address of the user is set as abnormal IP, if it is, refer to [Delete the Abnormal IP](#).

## Failing to Activating a License Online

---

### Situation:


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

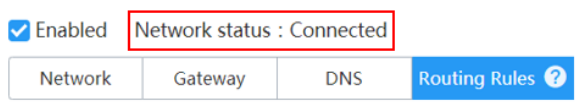
### Cause:

- 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](#)

## Appendix-Time Zones

---

Time zone
(UTC-11:00) Coordinated Universal Time-11
(UTC-11:00) Samoa
(UTC-10:00) Hawaii
(UTC-09:00) Alaska
(UTC-08:00) Baja California
(UTC-08:00) Pacific Time (US & Canada)
(UTC-07:00) Arizona
(UTC-07:00) Chihuahua, La Paz, Mazatlan
(UTC-07:00) Mountain Time (US & Canada)
(UTC-06:00) Central America
(UTC-06:00) Central Time (US & Canada)
(UTC-06:00) Guadalajara, Mexico City, Monterrey
(UTC-06:00) Saskatchewan
(UTC-05:00) Bogota, Lima, Quito
(UTC-05:00) Eastern Time (US & Canada)
(UTC-05:00) Indiana (East)
(UTC-04:00) Asuncion
(UTC-04:00) Atlantic Time (Canada)
(UTC-04:00) Cuiaba
(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
(UTC-04:00) Santiago
(UTC-03:30) Newfoundland
(UTC-03:00) Brasilia
(UTC-03:00) Buenos Aires

Time zone
(UTC-03:00) Cayenne, Fortaleza
(UTC-03:00) Greenland
(UTC-03:00) Montevideo
(UTC-02:00) Coordinated Universal Time-02
(UTC-02:00) Mid-Atlantic
(UTC-01:00) Azores
(UTC-01:00) Cape Verde Is.
(UTC) Casablanca
(UTC) Coordinated Universal Time
(UTC) Dublin, Edinburgh, Lisbon, London
(UTC) Monrovia, Reykjavik
(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
(UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb
(UTC+01:00) West Central Africa
(UTC+01:00) Windhoek
(UTC+02:00) Amman
(UTC+02:00) Athens, Bucharest, Istanbul
(UTC+02:00) Beirut
(UTC+02:00) Cairo
(UTC+02:00) Damascus
(UTC+02:00) Harare, Pretoria
(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(UTC+02:00) Jerusalem
(UTC+02:00) Minsk
(UTC+03:00) Baghdad
(UTC+03:00) Kuwait, Riyadh
(UTC+03:00) Moscow, St. Petersburg, Volgograd
(UTC+03:00) Nairobi
(UTC+03:30) Tehran
(UTC+04:00) Abu Dhabi, Muscat
(UTC+04:00) Baku
(UTC+04:00) Port Louis

Time zone
(UTC+04:00) Tbilisi
(UTC+04:00) Yerevan
(UTC+04:30) Kabul
(UTC+05:00) Ekaterinburg
(UTC+05:00) Islamabad, Karachi
(UTC+05:00) Tashkent
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
(UTC+05:30) Sri Jayewardenepura
(UTC+05:45) Kathmandu
(UTC+06:00) Astana
(UTC+06:00) Dhaka
(UTC+06:00) Novosibirsk
(UTC+06:30) Yangon (Rangoon)
(UTC+07:00) Bangkok, Hanoi, Jakarta
(UTC+07:00) Krasnoyarsk
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
(UTC+08:00) Irkutsk
(UTC+08:00) Kuala Lumpur, Singapore
(UTC+08:00) Perth
(UTC+08:00) Taipei
(UTC+08:00) Ulaanbaatar
(UTC+09:00) Osaka, Sapporo, Tokyo
(UTC+09:00) Seoul
(UTC+09:00) Yakutsk
(UTC+09:30) Adelaide
(UTC+09:30) Darwin
(UTC+10:00) Brisbane
(UTC+10:00) Canberra, Melbourne, Sydney
(UTC+10:00) Guam, Port Moresby
(UTC+10:00) Hobart
(UTC+10:00) Vladivostok
(UTC+11:00) Magadan
(UTC+11:00) Solomon Is., New Caledonia
(UTC+12:00) Auckland, Wellington

Time zone
(UTC+12:00) Coordinated Universal Time+12
(UTC+12:00) Fiji
(UTC+13:00) Nuku'alofa