Yealink

Yealink Meeting Server and Skype for Business Deployment Guide

Version 20.0.0.5
Dec.2018

About This Guide

This guide introduces how to make YMS communicate with SfB server.

Related Document

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

- Yealink Meeting Server Administrator Guide: it introduces how to deploy and use all YMS features.

In This Guide

This guide contains the following:

- Chapter 1 Structure Overview
- Chapter 2 Delploying the SfB ServerDelploying the SfB Server
- Chapter 3 Setting YMS
- Chapter 4 Introduction of the Call Method
- Chapter 5 Instruction of SfB ClientIntroduction of the Call Method

Table of Conents

About This Guide iii

Related Document iii
In This Guide iii

Table of Conents v

Structure Overview 1

Communicating with the Local SfB Server 1
Communicating with Microsoft Office 365 1
Communicating with Other Enterprise SfB Servers 1

Delploying the SfB Server 3

Delploying the Local SfB Server 3
Delploying Microsoft Office 365 6
Deploying Other Enterprise SfB Servers 6

Setting YMS 13

Importing the TLS Certificate 13
Common Perl Compatible Regular Expressions (PCRE) and Its Replacement Strings 14
Setting the SfB Gateway 16
Configuring the SfB Gateway Media Service 18
Adding the Call Routing Rule 18

Introduction of the Call Method 21

Placing a Point-to-Point Call 21
Joining the Conference 21

Instruction of SfB Client 23

Point-to-Point Call 23
Placing a Call 23
Parking a Call 24
Transferring a Call 24
Holding/Resuming a Call 24
Setting the Voice Message 24
Setting the Simultaneous Ring/Call Forwarding 25
Sharing the Content 25
SfB Conference 26
Creating a Meeting Now Conference 26
Scheduling a Conference 27
Inviting/Removing a Participant 28
Switching the Role of the Participant 29
Locking a Conference 30
Pinning a Participant to Gallery 31

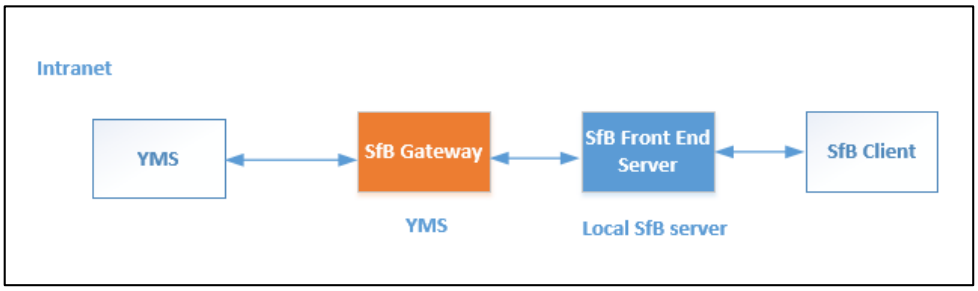
Muting/Unmuting the Audience..... 31

Structure Overview

Communicating with the Local SfB Server

When YMS and the SfB are deployed in the internal network only for the user in the internal network, you can configure two servers to realize the communication between YMS devices and the SfB devices.

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



Communicating with Microsoft Office 365

To communicate with Microsoft Office 365, you need do the following: Delploying Microsoft Office 365, Importing the TLS Certificate, Setting the SfB Gateway, Configuring the SfB Gateway Media Service, and Adding the Call Routing Rule.

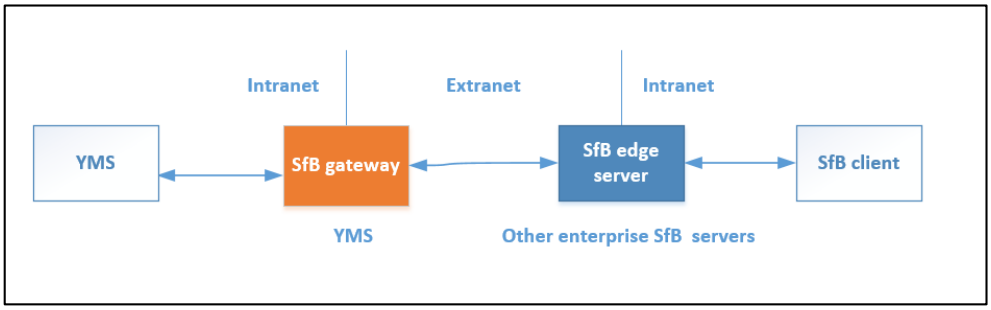
Note that the federation should be enabled on Microsoft Office 365.

Communicating with Other Enterprise SfB Servers

Because the YMS device should 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: Communicating with Other Enterprise SfB Servers, Deploying Other Enterprise SfB Servers, Importing the TLS Certificate, Setting the SfB Gateway, Configuring the SfB Gateway Media Service, and Adding the Call Routing Rule.

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



Delploying the SfB Server

Delploying 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.

Take the local environment as an example, you need run the example command below to complete the configuration:

- If it is a cluster version and you plan to use the business node in YMS to connect to SfB, the DNS FQDN of this node is "sfb1.5060.space" and the A record of this busines node is added to DNS server.
- The DNS 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 about the command, refer to https://docs.microsoft.com/en-us/powershell/module/skype/?view=skype-ps.

Procedure	Command	Syntax description
1 Get the Site ID of SfB Front-End Pool.	Get-CsSite	None
2 Add YMS into the trusted application pool created by the SfB server.	New-CsTrustedApplicationPool **-Identity** <YMS DNS FQDN> **-ComputerFqdn** <YMS DNS FQDN> **-Registrar** <Front End Pool DNS FQDN> **-Site** < Site ID> **-RequiresReplication** $false **-ThrottleAsServer** $true **-TreatAsAuthenticated $true** **Example command:** New-CsTrustedApplicationPool **-Identity** sfb1.5060.space **-ComputerFqdn** sfb1.5060.space **-Registrar** xiamenpool.xiamen.yealinksfb.com **-Site** 5 **-RequiresReplication** $false **-ThrottleAsServer** $true **-TreatAsAuthenticated** $true	**-Identity**: defines the name of the trusted application pool and the name should be DNS FQDN. **-ComputerFqdn**: defines the YMS DNS FQDN which communicates with the SfB in the trusted application pool. The name of the trusted application pool should be consistent with the name of YMS, because when integrating SfB with YMS, there is only one YMS in the trusted application pool. **-Registrar**: defines the DNS FQDN of the SfB Front-End Pool to which this trusted application pool belongs. **-Site**: defines the SfB Site ID to which this trusted application pool belongs. Run command **Get-CsSite** to get the Site ID. Others are the same with the default value. **Note**: When creating a trusted application pool (and a trusted application computer in the next step) in this way, SfB will issue a warning state: "**WARNING: Machine sfb1.5060.space from the topology you are**

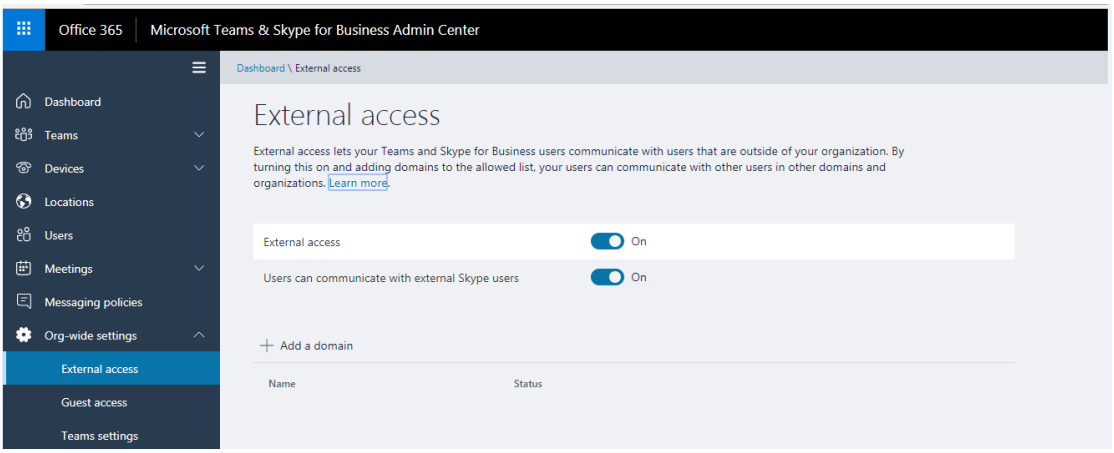
Procedure	Command	Syntax description
		publishing was not found in Active Directory and will result in errors during Enable-CsTopology as it tries to prepare Active Directory entries for the topology machines.", and you should answer Yes to this warning.
3 Add the other trusted applications to the trusted application pool.	New-CsTrustedApplication **-ApplicationId** <Application ID> **-TrustedApplicationPoolFqdn** <YMS DNS FQDN> **-Port** <Available Port> **Example command**: New-CsTrustedApplication **-ApplicationId** sfb1 **-TrustedApplicationPoolFqdn** sfb1.5060.space**-Port** 5067	**-ApplicationId**: defines a friendly identifier for the YMS. You can customize the name and it is unique. **-TrustedApplicationPoolFqdn**: defines the trusted application pool which this YMS belongs to. **-Port**: defines the source port on YMS that communicates with SfB server. It can be any unoccupied port from 0 to 65535. In YMS, the default port is 5067, which is recommended.
4 View the trusted application to ensure that YMS is added into the trusted application pool.	Get-CsTrustedApplication	None
5 View information about whether or not there is 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.	New-CsStaticRoutingConfiguration **–Identity** "Service:Registar: <Front End Pool DNS FQDN>" **Example command:** New-CsStaticRoutingConfiguration **–Identity** "Service:Registrar:xiamenpool.xiamen.yealinksfb.com"	-**Identity**: defines the registrar to which we want to apply the static routing configuration.
7 Create the static SIP domain route, and associating this route with a trusted application.	$newroute = New-CsStaticRoute -TLSRoute **-Destination** <YMS DNS FQDN> **-Port** <YMS Port> **-MatchUri** < YMS DNS FQDN> **-UseDefaultCertificate $true**	**-Destination**: defines the YMS DNS FQDN where SfB should send SIP requests matching the domain specified in -MatchUri. **-Port**: defines the source port on YMS that communicates with SfB server. It can be any unoccupied port from 0 to 65535. In YMS, the default port is 5067, which is recommended. -**MatchUri**: efines

Procedure	Command	Syntax description
	Example command: $newroute = New-CsStaticRoute -TLSRoute **-Destination** "sfb1.5060.space" **-Port** 5067 **-MatchUri** "sfb1.5060.space"	the matched YMS DNS FQDN.
8 Apply your required static route to your registrars' static routing configuration.	Set-CsStaticRoutingConfiguration **-Identity** “Service:Registar: <Front End Pool DNS FQDN>” -Route @{Add=$newroute} **Example command:** Set-CsStaticRoutingConfiguration **-Identity** "Service:Registrar:xiamenpool.xiamen.yealinksfb.com" **-Route** @{Add=$newroute}	**-Identity**: defines the registrar to which we want to apply the static routing configuration. Others are the same with the default value.
9 View all routes in your static routing configuration to ensure that your required static route is added successfully.	Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty Route	None
10 Enable the new topology.	Enable-CsTopology	None

Delploying Microsoft Office 365

Procedure:

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



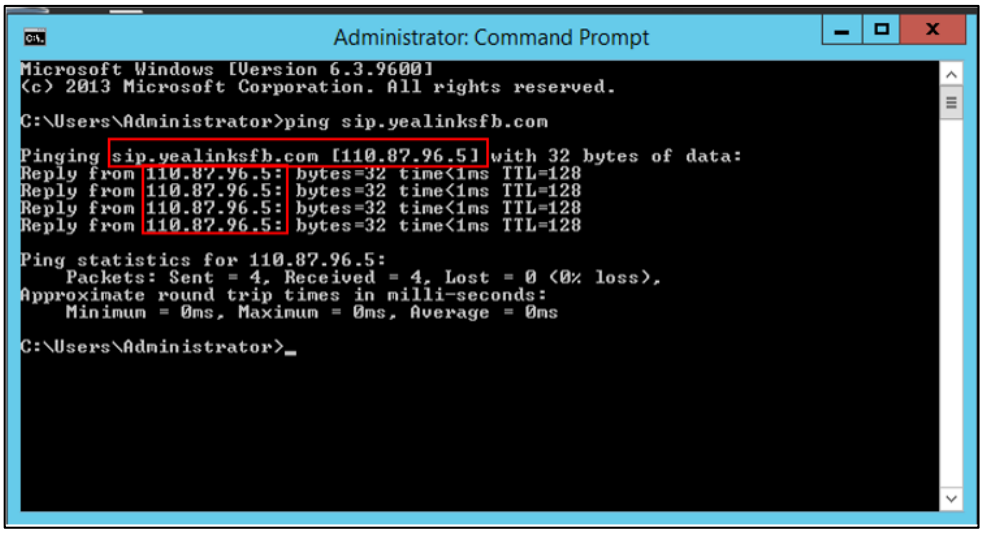
2. Make sure that the SRV record and the A record of both YMS and SfB are configured on the public DNS server.

Deploying Other Enterprise SfB Servers

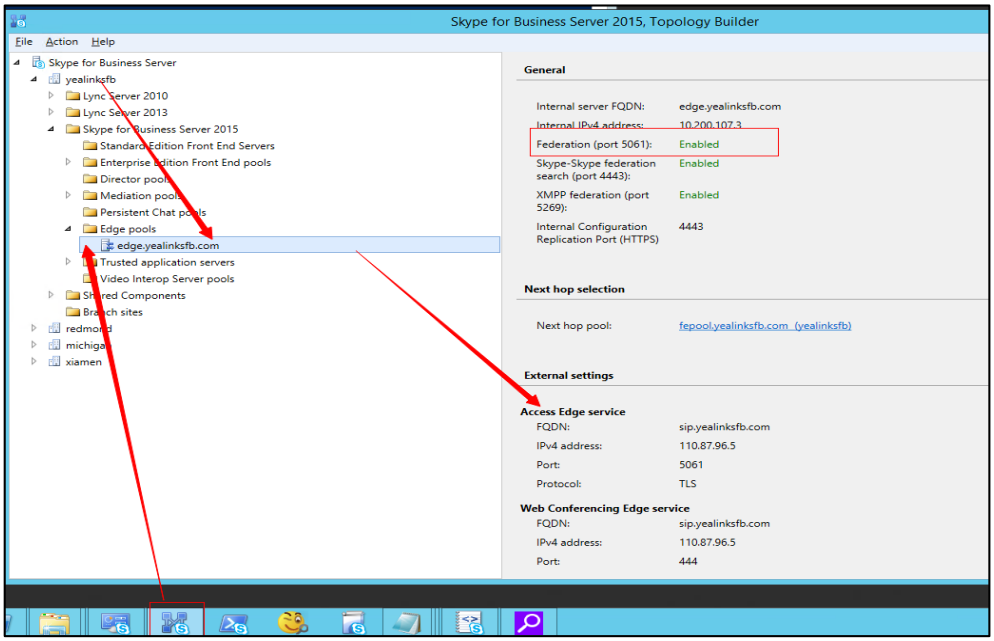
Procedure：

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 in the Command Prompt, for example, ping sip.yealinksfb.com. If the verification fails, you need check the DNS A record of the SfB edge server.

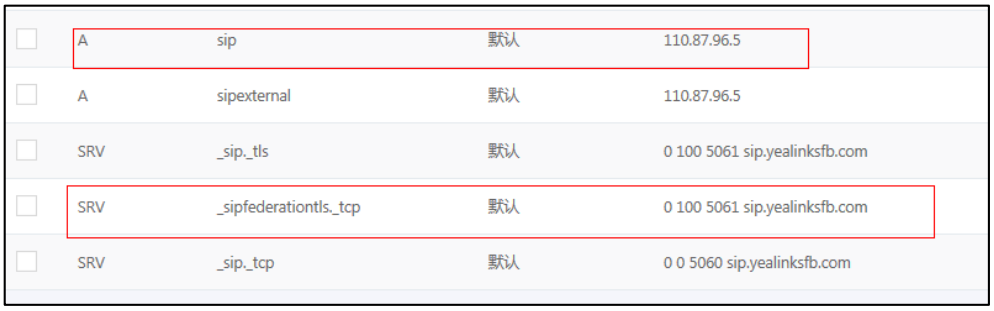


- View the information of the SfB edge server in the Front End topology. The information includes whether or not the federation is enabled on the SfB edge server.



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

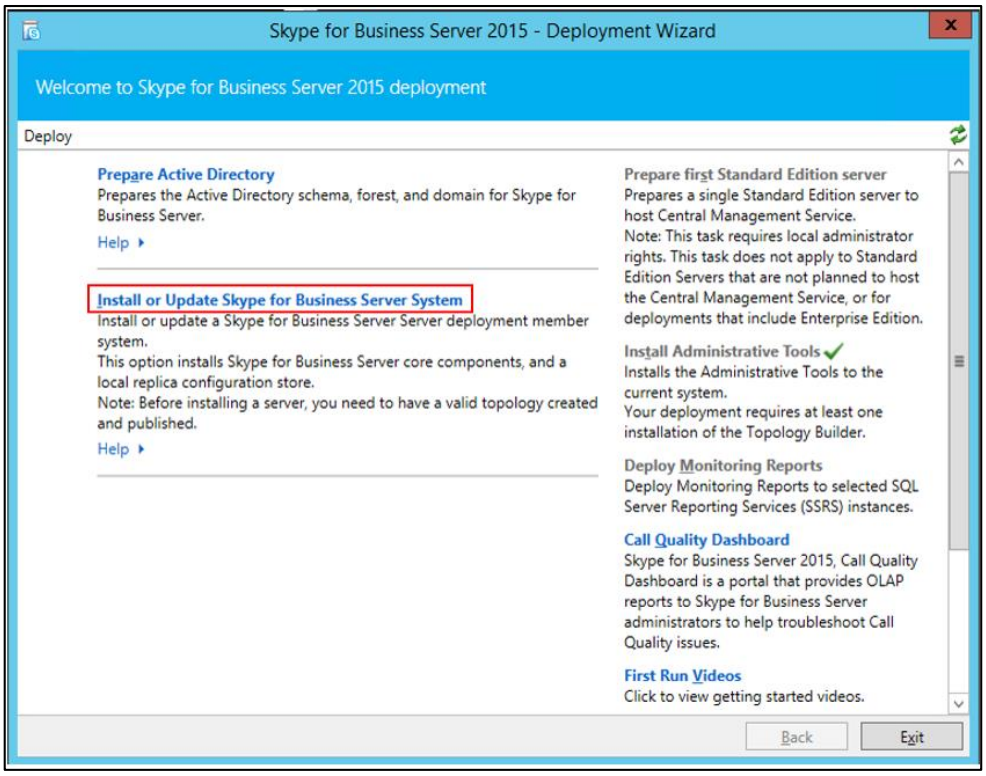
a. Log into the public DNS server where the SfB edge server is located to view the SRV record and the A record. The host machine record must be_sipfederationtls_tcp in the SRV record.



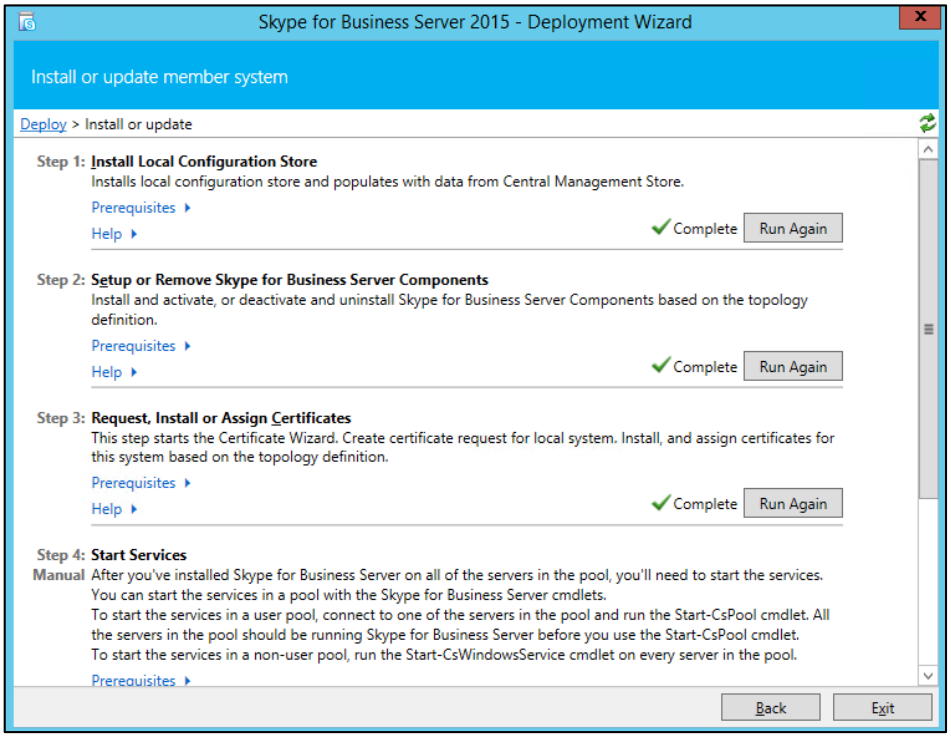
b. Log into the public DNS server where the YMS is located to view the SRV record and the A record. The host machine record must be_sipfederationtls_tcp in the SRV record.

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:

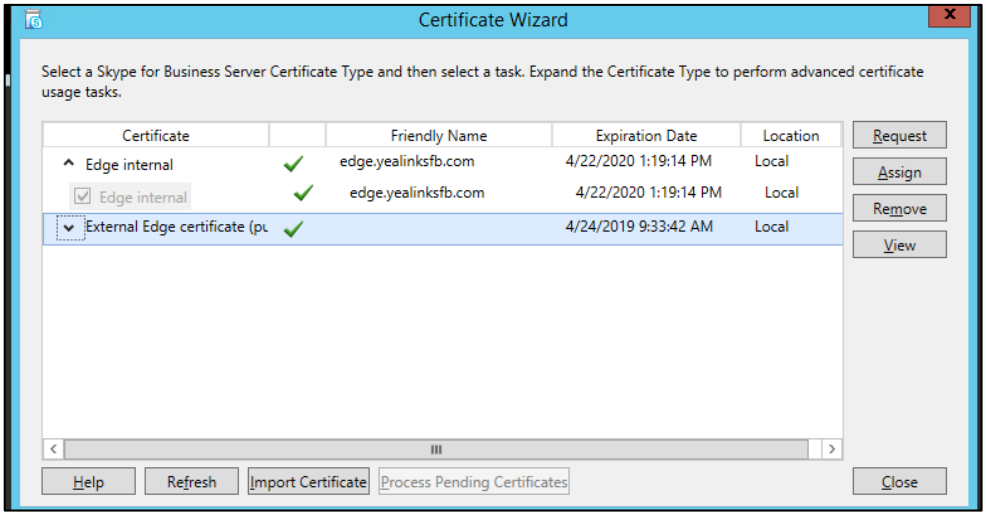
a. Go to the Deployment Wizard of the Lync Server, and click **Install or Update Skype for Business Server System**.



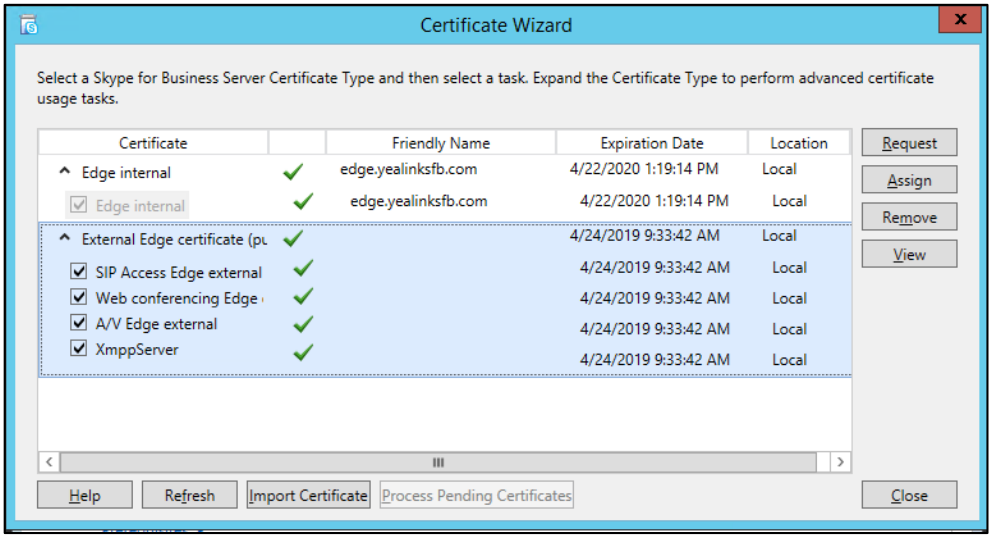
b. Click **Run Again**.



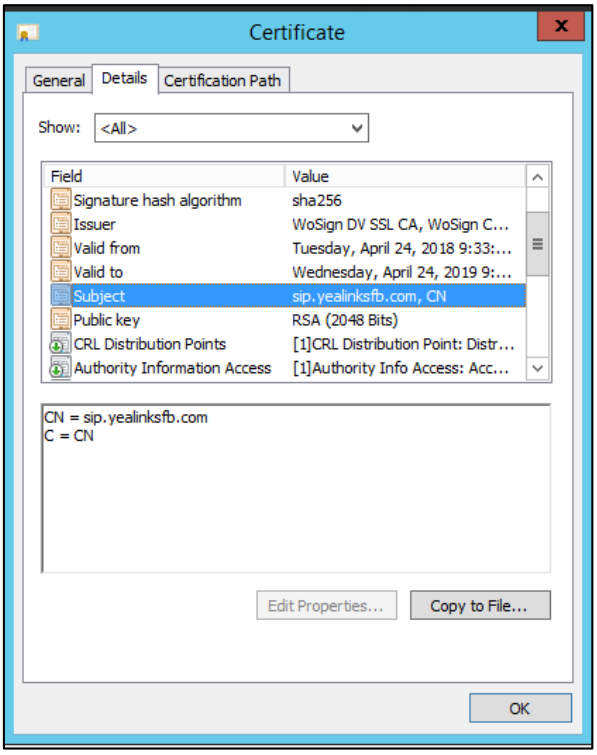
c. Click **Import Certificate** and import the external edge certificate.



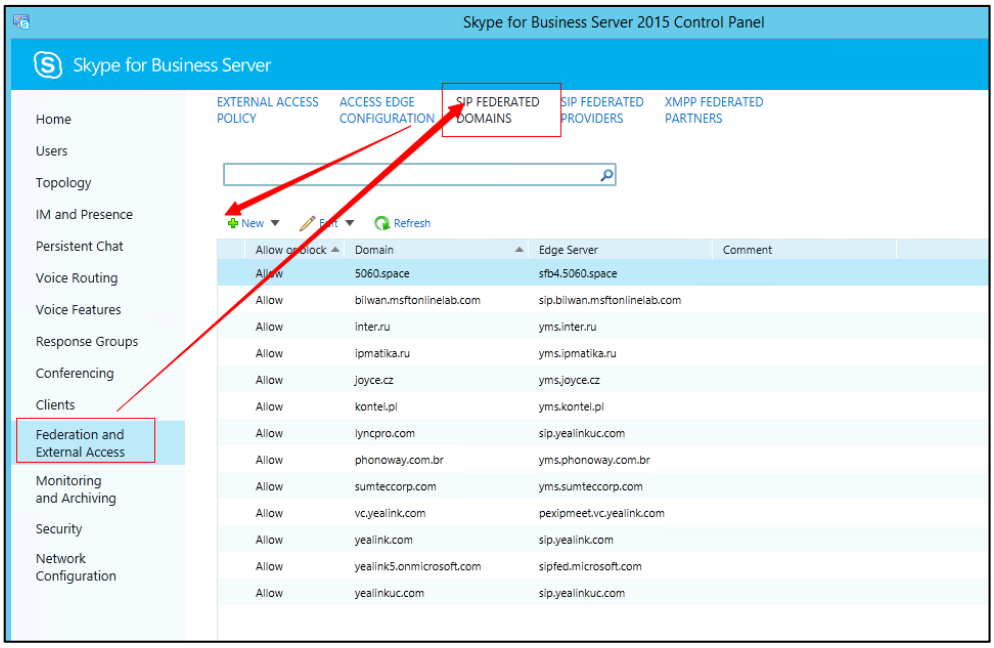
After importing, the page is shown as below:

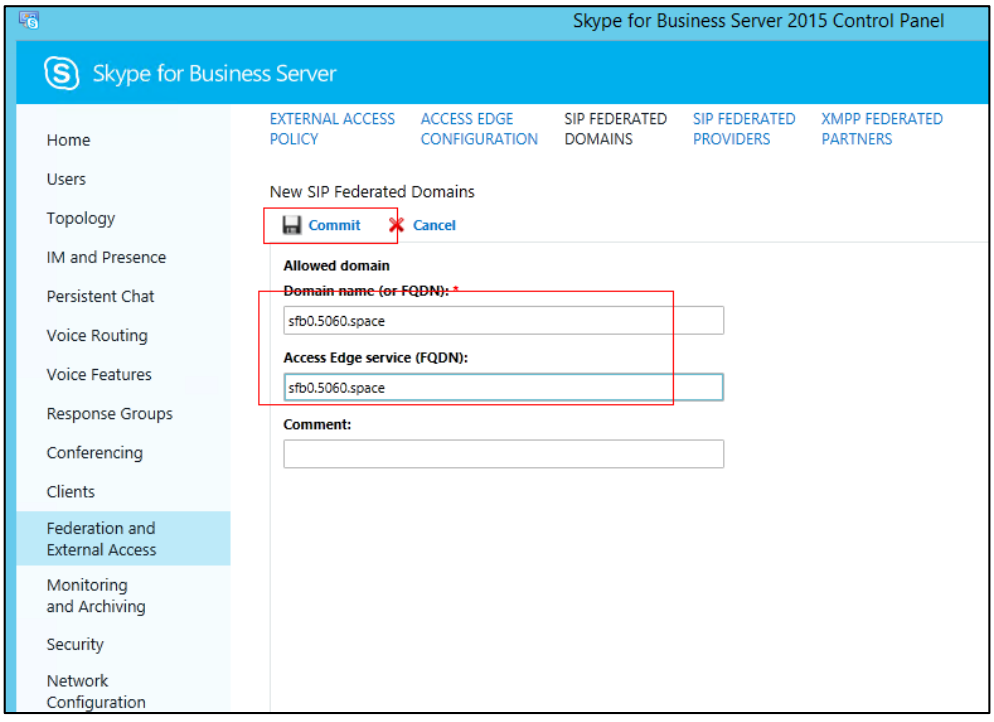


d. Select the imported edge server certificate, click **View**, and make sure that the user name (commonName attribute) or the user optional name (altNames attribute) must contain the FDQN name of the edge server.



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.





Setting YMS

You need do the following steps to set YMS:

1. Importing the TLS
2. Setting the SfB Gateway
3. Configuring the SfB Gateway Media Service
4. Adding the Call Routing Rule

Importing the TLS Certificate

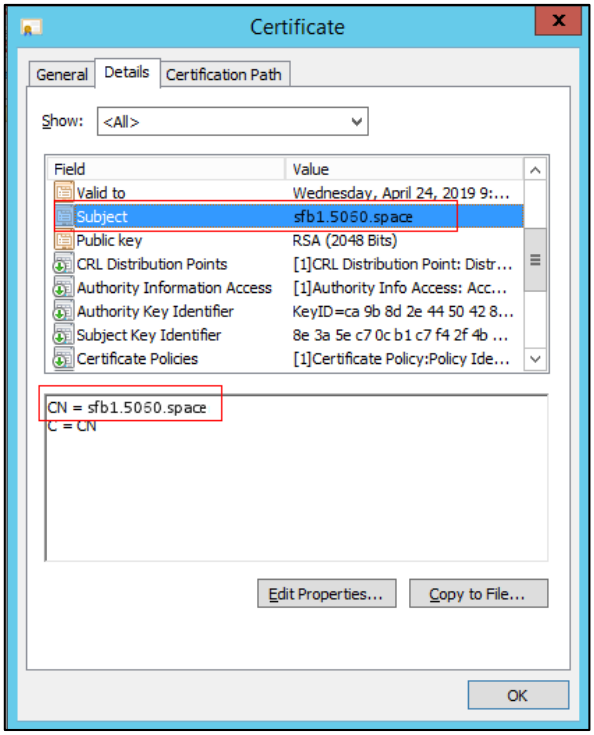
You need import the TLS certificate to make the SfB trust YMS.

The method of obtaining the TLS is described as follows:

- If it is a local SfB server, you can use a certificate issued by a public CA, or a certificate issued by the organization's internal CA (trusted by SfB and YMS).
- If it is Microsoft office 365 or other enterprise SfB servers, you can use the certificate issued by a public CA.

The certificate should meet the following:

- The Subject name (commonName attribute) or the Subject Alternative Name (altNames attribute) of the certificate must contain the DNS FQDN name of the YMS business node.



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

Procedure:

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

Common Perl Compatible Regular Expressions (PCRE) and Its Replacement Strings

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

PCRE	Description
^(1\d{10})	Match an 11-digit number which starts with 1. For example: 12345678912
^0(\d+)	Match the number (2 or more digits) which starts with 0. For example: 02, 0157
^(13[0-9]|14[5|7]|15[0|1|2|3|5|6|7|8|9]|18[0|1|2|3|5|6|7|8|9])\d{8}	Match an 11-digit mobile phone number, the first 3 digits includes the following types, the rest digits can be any digits: • **Start with 13 and the third number is any digit from 0 to 9** • **Start with 14 and the third number is 5/7** • **Start with 15 and the third number is 0/1/2/3/5/6/7/8/9** • **Start with 18 and the third number is 0/1/2/3/5/6/7/8/9** For example: 13012345678, 14512345678, 15987654321 or 18243218765

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

The common replacement string of Perl Compatible Regular Expressions (PCRE) is described as below：

PCRE	Description
$1@$2	Transform the originally dialed alias (if a match was found). For example: the compatible regular expression is avmcu\.(\d{1,10})@(xiamen.yealinksfb\.com), after transformation, it is (\d{1,10}@(xiamen.yealinksfb\.com).

Setting the SfB Gateway

To make the YMS find the desired SfB server, you need add SfB gateway server on YMS to provide the destination gateway for the call routing.

About this task:

YMS can communicate with SfB server version and 2016.

Procedure:

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

The basoic parameters of SfB gateway is described as below:

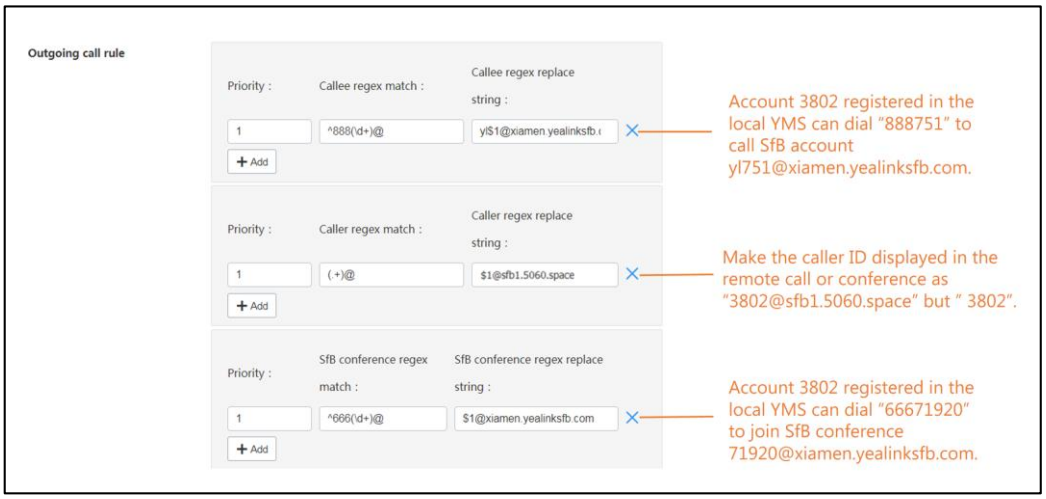
Parameter	Description
Enable	Enable or disable the SfB gateway server. **Defaul**t: enabled.
Name	The name of SfB gateway server.
Node	The node used by this SfB gateway server.
Network	The IP address of this node.
Transport protocol	Only TLS is available if communicating with SfB devices.
FQDN	The name of YMS. Example: sfb1.5060.space **Method**: add this domain name to DNS server to which the A record of YMS is added.
Port	The source port on YMS that communicates with the SfB server. **Note**: the value can be any integer from 0 to 65535. This port must be consistent with the port configured in SfB server and cannot be occupied. **Default**: 5067. If the SfB enables the federation, this port should be 5061. Firstly, change the registration port to other port; secondly, make the port as 5061, otherwise the port will be closed by the firewall.
Domain	The domain name of SfB server. For example: xiamen.yealinksfb.com.
Port	The source port on the SfB server that communicates with YMS. **Default**: 5061.
Federation	Enable or disable the federation. **Default**: disabled. According to different SfB servers, you can enable or disable the federation in one of the following scenarios: If it is a local SfB server, you can disable the federation. If it is Microsoft Office 365 or other enterprise SfB servers, you can enable the federation.
Outbound proxy	Enable or disable it to allow the SfB server to send requests to the outbound proxy server.
Proxy address	The IP address or the domain name of this outbound proxy server.
Proxy port	The port of this outbound proxy server. **Note**: the value can be any integer from 0 to 65535.
Support video	If you enable this, you can place video calls to the remote that

Parameter	Description
	supports video call. **Default:** enabled.

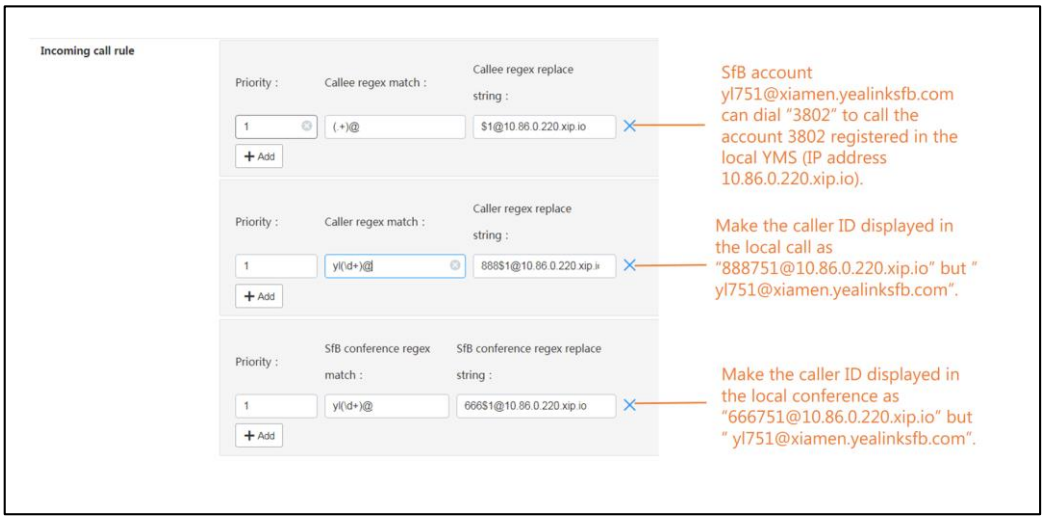
3. Configure the parameters of the security policy.
   Parameters of the Security Policy is described as below：

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

4. Configure the outgoing call rule.



5. Configure the incoming call rule.



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

Configuring the SfB Gateway Media Service

If you want to make YMS communicate with the SfB server, you need configure the SfB gateway media service.

Procedure:

1. Click **Service**->**MCU Service**->**SfB Gateway Media Service**->**Add**.
2. Configure the basic parameters.

The basic parameters are described as below:

Parameter	Description
Enable	Enable or disable this service. **Default**: enabled.
Name	The service name.
Node	The node used by this service.
External media port	The port range of the SFB gateway media service. **Default port range**: from 61000 to 64999. To avoid the port conflict, the gap between the maximum port and the minimum port should be more than 200. For example, you set 61000 as the minimum port, and the maximum port should be more than 61199.
All local networks	The IP address used by this service.

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

Adding the Call Routing Rule

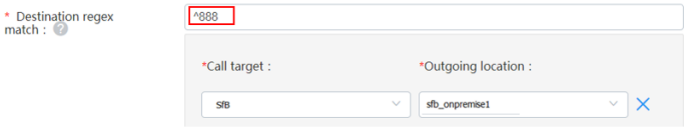
To make the call be routed to the specified destination, you can add the call routing rule.

Procedure:

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

   Parameters of the Call Routing Rule are described as below:

Parameter	Description
Enable	Enable or disable the call routing rule. **Default**: enabled. All the disabled rules are ignored, though they are displayed in the rule list.
Name	The name of the call routing rule.
Priority	The priority of the call routing rule. The smaller the number is, the higher the priority is. When you place a call, the server will look up the first appropriate call routing rule according the priority in ascending order.

Parameter	Description
Destination regex match	The Perl Compatible Regular Expressions (PCRE) used to match the target call number. For more information, refer to Common Perl Compatible Regular Expressions (PCRE) and Its Replacement Strings on page 14. If the match succeeds, the server uses this call routing rule. The call routing expression match of both the device and the SfB conference need correspond to the outgoing call routing rule set on SfB gateway, otherwise, the call cannot be reached. For example: the outgoing call rule of SfB gateway is shown as the image below: And the call routing expression match need to be the one shown as the image below: 
Call target	The call route is SfB.
Outgoing location	The gateway used to place the call. If the call number matches this call routing rule, it is called via this gateway.

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

   The parameters are described as below：

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

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

Introduction of the Call Method

The following parts take the case below as an example:

An SfB account yl713@xiamen.yealinksfb.com, and a YMS account 1001 which is registered on server 10.86.0.220 (its domain name is sfb1.5060.space).

Placing a Point-to-Point Call

If the outgoing and incoming call routing rules are not configured on SfB gateway but only the call routing rule is configured, the SfB account and the YMS account can call each other by the following rules.

The SfB account calls the YMS account:

Call rule: YMS account number@the server domain name

Example: 1001@sfb1.5060.space

The YMS account calls the SfB account:

Call rule: SfB account number

Example: yl713@xiamen.yealinksfb.com

Joining the Conference

If the outgoing and incoming call routing rules are not configured on SfB gateway but only the call routing rule is configured, the SfB account and the YMS account can join each other's conference.

The SfB account creates a conference (including the Meet Now conference and the calendar conference) with the conference ID 54782, and the YMS account creats a conference with the conference ID 888888 and the password 123456.

The SfB account joins the YMS conference:

Call rule: YMS conference ID**password@the server domain name

Example: 88888 ** 123456@sfb1.5060.space

The YMS account joins the SfB conference:

Calling rule: SfB conference ID**password@the SfB domain name

Example: 54782@xiamen.yealinksfb.com

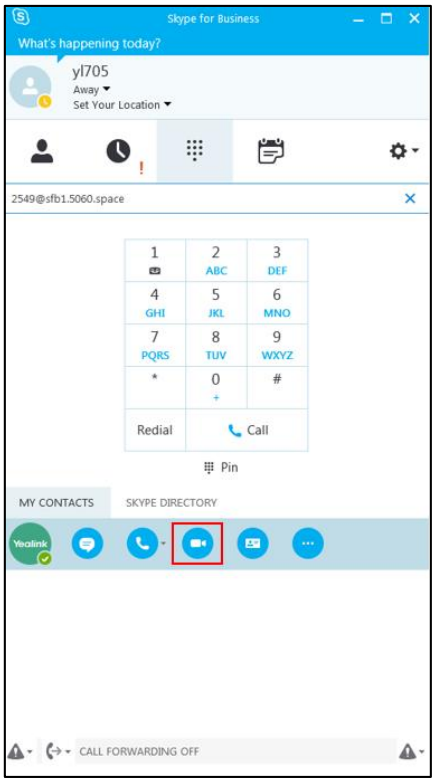
Note You can hold the SfB conference and the YMS conference together by inviting other conferences in the Conference Control page, and the rule is the same with the one of joining the conference.

Instruction of SfB Client

Point-to-Point Call

Placing a Call

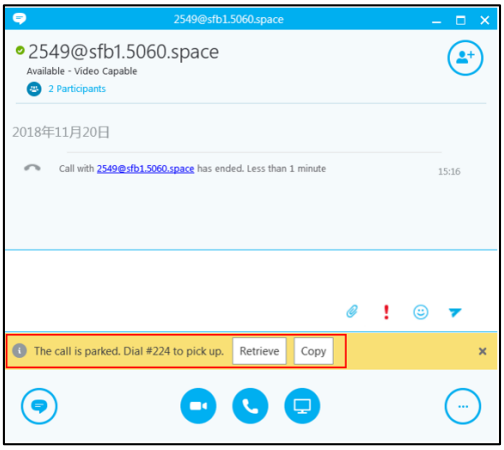
Enter the number in the Contact or the Dial window, and select the video call or the audio call in the search result to place the call.



Parking a Call

During a call, click **Call Controls**->**Transfer**->**Call Park**, to park the call and exit the Call window.

Click **Retrieve** in the call history or dial the retrieving ID to pick up the call.

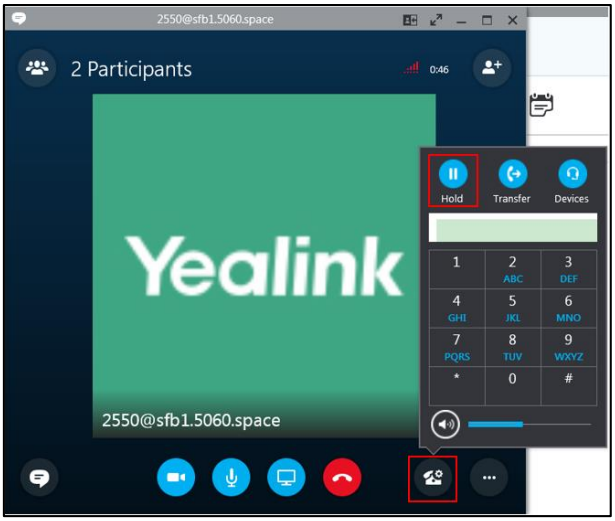


Transferring a Call

During a call, click **Call Controls**, enter the desired number and click **Transfer** to transfer the call to the desired number.

Holding/Resuming a Call

During a call, click **Call Controls**->**Hold** to hold the call, and you can click **Resume** to resume the call later.

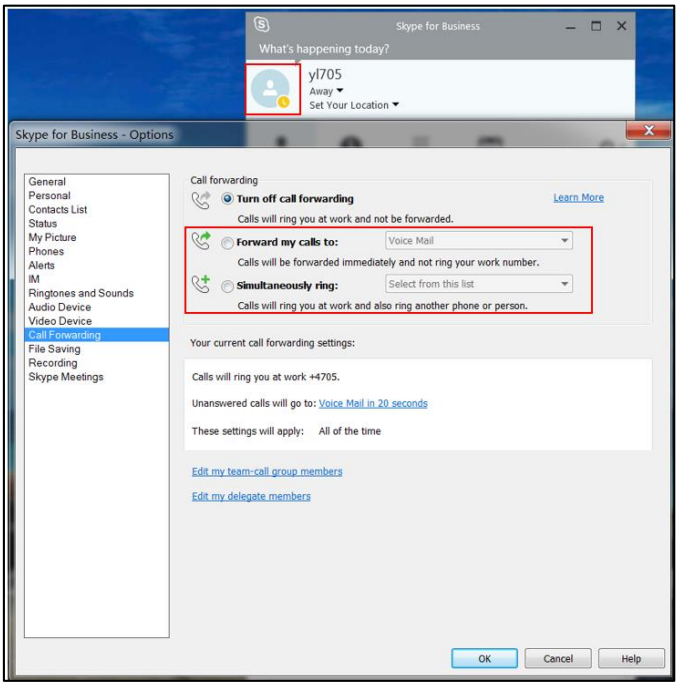


Setting the Voice Message

Contact the IT staff to enable the voice message. If you enable it and someone calls you, the call will ring but it is set to refuse to answer, the caller can do the corresponding operations according to the voice prompts.

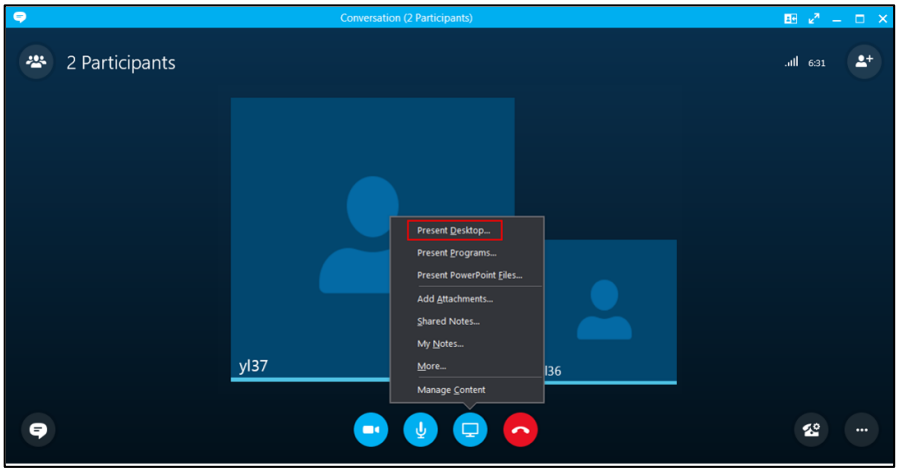
Setting the Simultaneous Ring/Call Forwarding

You can set the simnltaneous ring or call forwarding to other accounts for the SfB account. Follow the steps below: click the avatar icon->**Call Forwarding**->**Forwarding my calls to/Simultaneously ring**, and then set the desired number. Therefore, when someone calls your SfB account, the call will be forwarded or simultaneously ringing to the desired number.



Sharing the Content

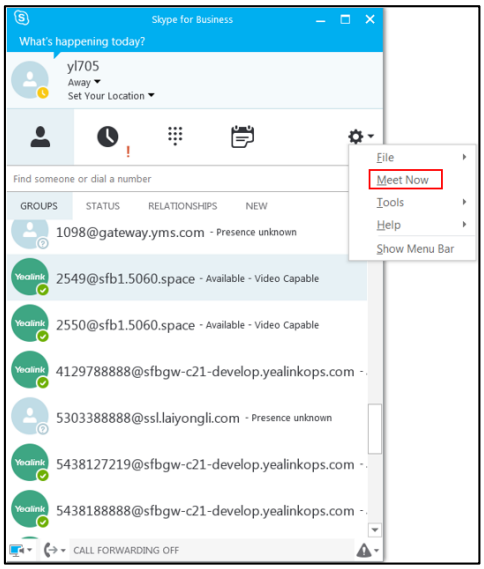
Click the present icon in the Call window to share the content with other parties.



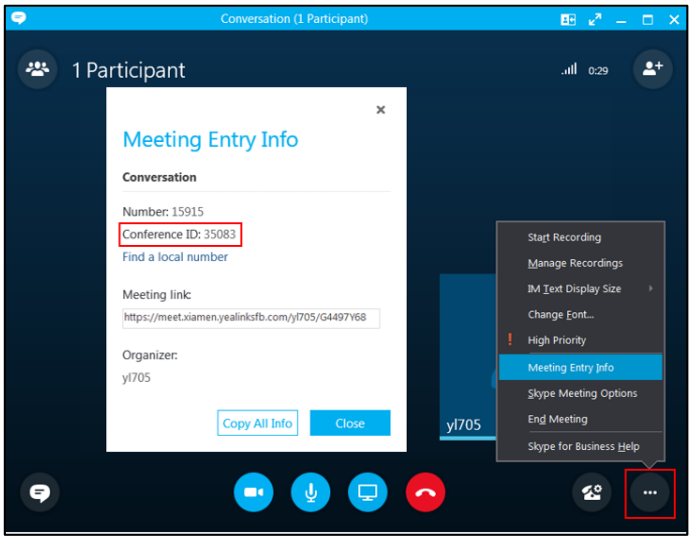
SfB Conference

Creating a Meeting Now Conference

Click Options icon->**Meeting Now** to creat a conference.



In the Conference window, click More Options icon->**Meeting Entry Info** to view the conference ID which can be used by other person to join the conference.

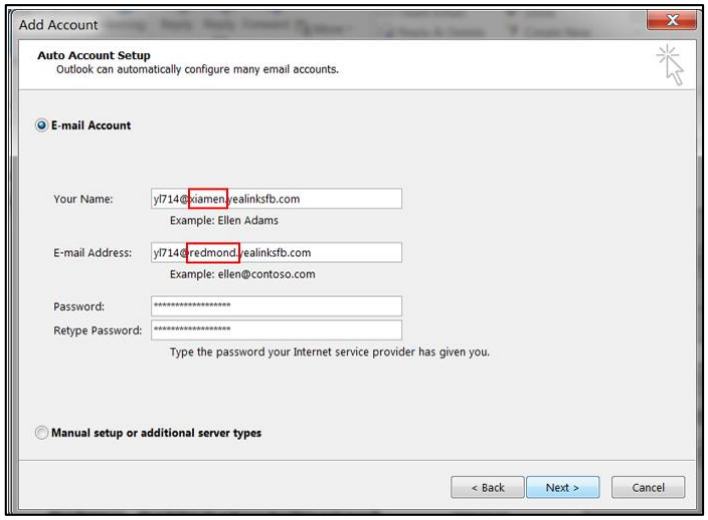


Scheduling a Conference

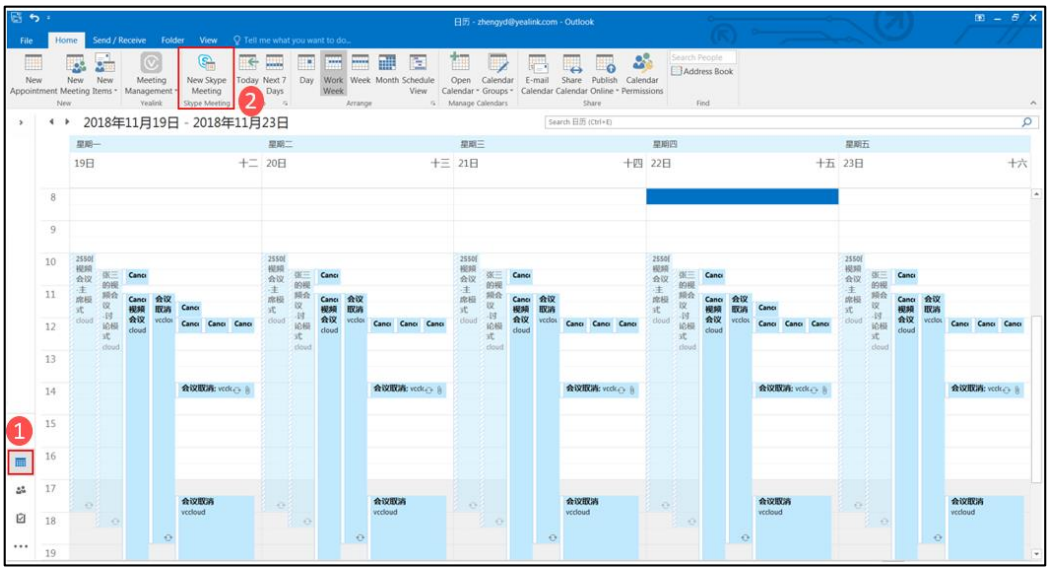
The calendar conference in SfB, consistent with the scheduled conference in YMS, can be scheduled via Outlook or Outlook web app (some accounts cannot be used to schedule conferences via Outlook web app). Here is an example of scheduling the conference via Outloook.

When scheduling an SfB conference, you need use the same account to log into SfB and Outlook.

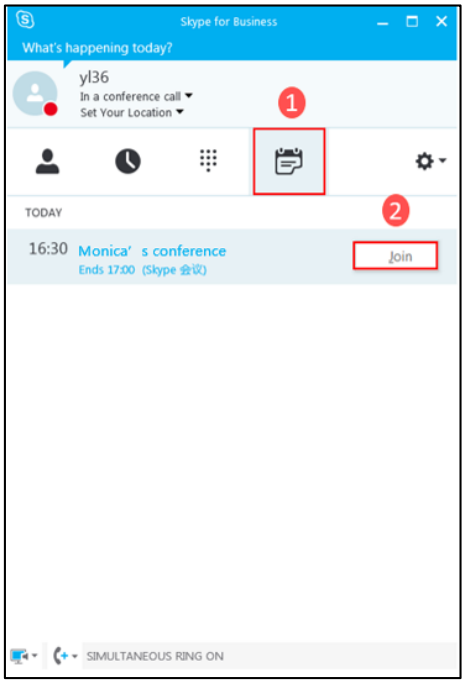
1） Add an email account, enter the corresponding parameters and click **Next**. Accounts with different types have different names and email addresses. For more information, contact your company IT staff.



2） Go to the Calendar window, click **Skype Meeting** to go to the Schedule Conference window, and you can schedule a conference.

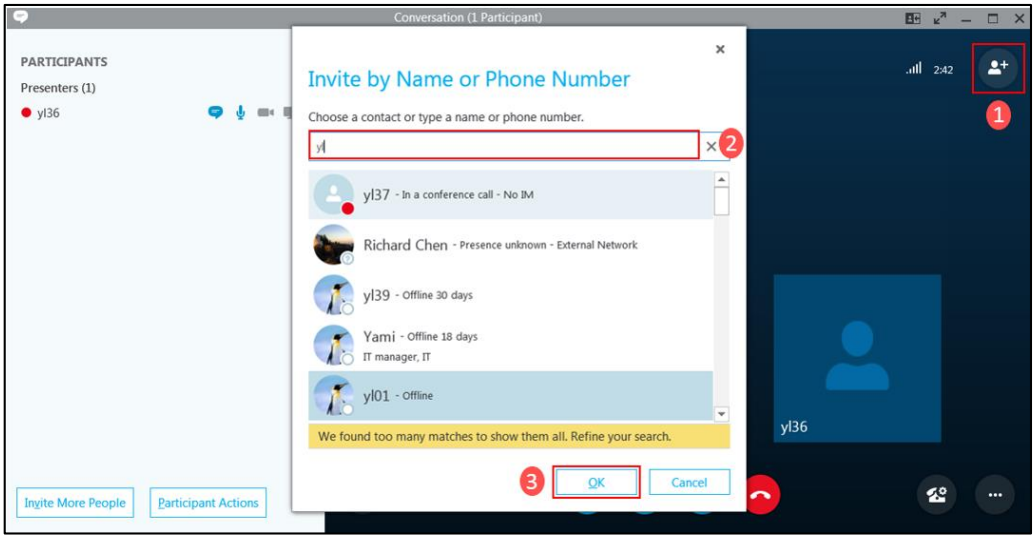


3） After scheduling, you can view the scheduled conference on the SfB or on the SfB phone. Right click the desired conference and click **Join** to join the conference.

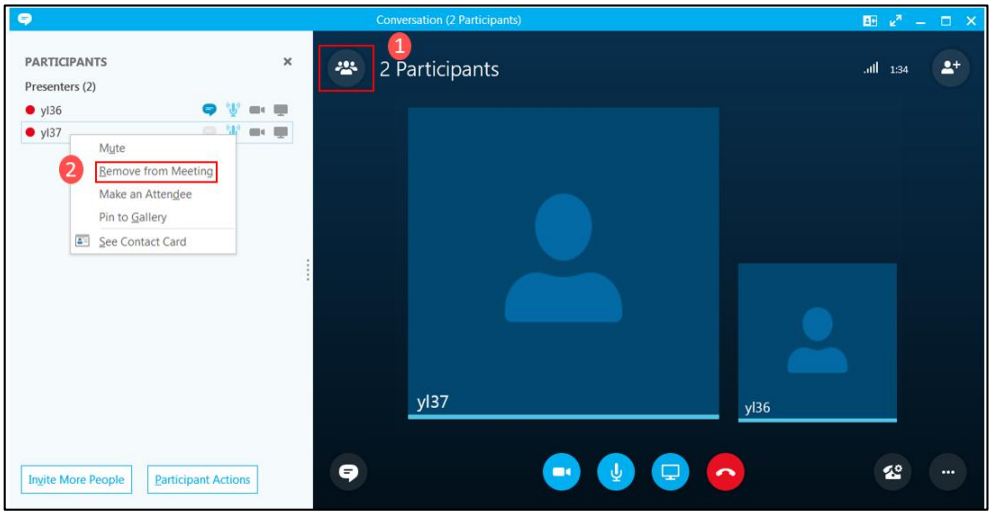


Inviting/Removing a Participant

During a conference, click the Invite icon, enter the number in the search box, select the desired contact from the serach result, and click **OK**.



If you want to remove a participant, click the Participant avatar icon, right click the desired participant, and click **Remove from Meeting**.



Switching the Role of the Participant

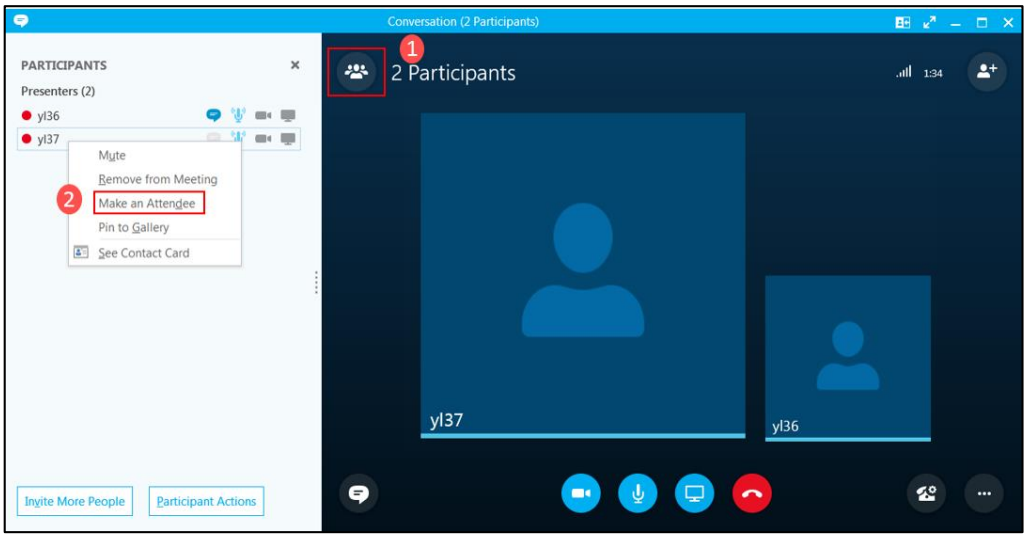
During a conference, there are three roles: the organizer, the presenter and the attendee.

The organizer: the conference creator, with the higest authority, can do all operations on the conference.

The presenter: with the second higest authority, he can do all operations except removing the organizer.

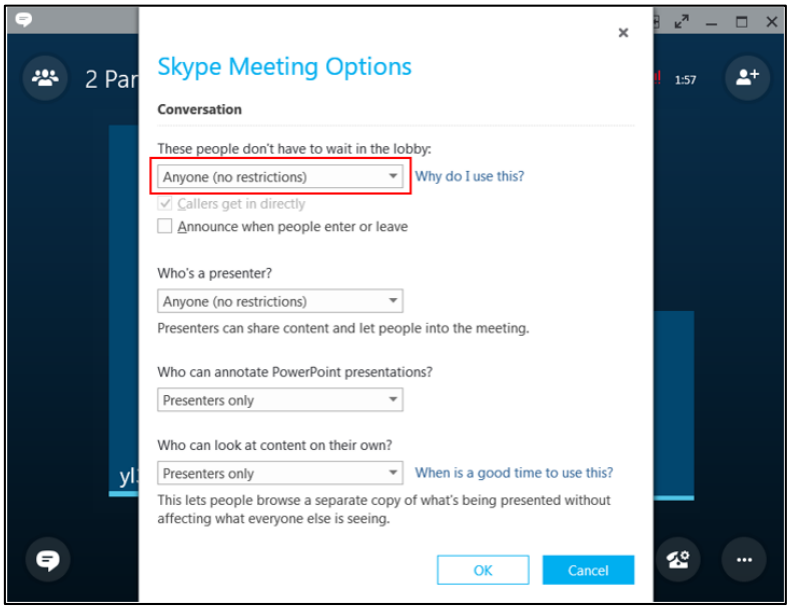
The attendee: with the lowest authority, he can only hold/resume/hang up the call, invite participants, view the conference information and the participant information.

In the Participant list, the organizer and the presenter can change the participant role by right clicking the participant and selecting the corresponding option. It is shown as in the picture below:

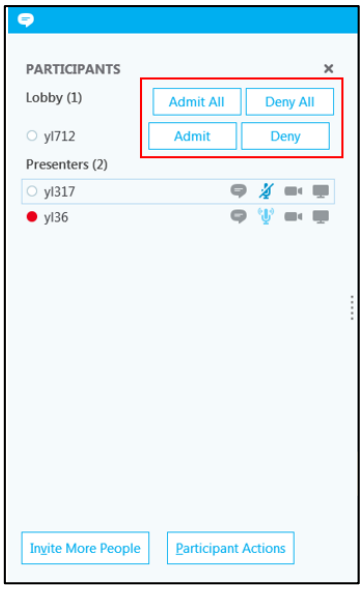


Locking a Conference

After the conference is locked, the person who is not allowed to join the conference will go to the conference lobby. The organizer or the presenter can allow them to join the conference. Click **More Options**->**Skype Meeting Options**. Select the person who does not have to wait in the lobby, click **OK** and the conference will be locked.

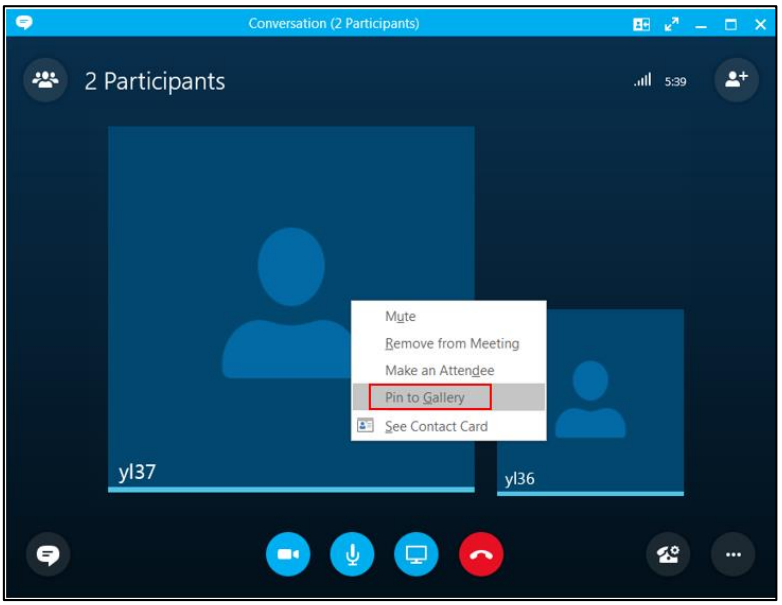


If the person who is not allow to join the conference place a call to join the conference, he will go to the lobby first, and the organize and the presenter can allow or reject him to join the conference.



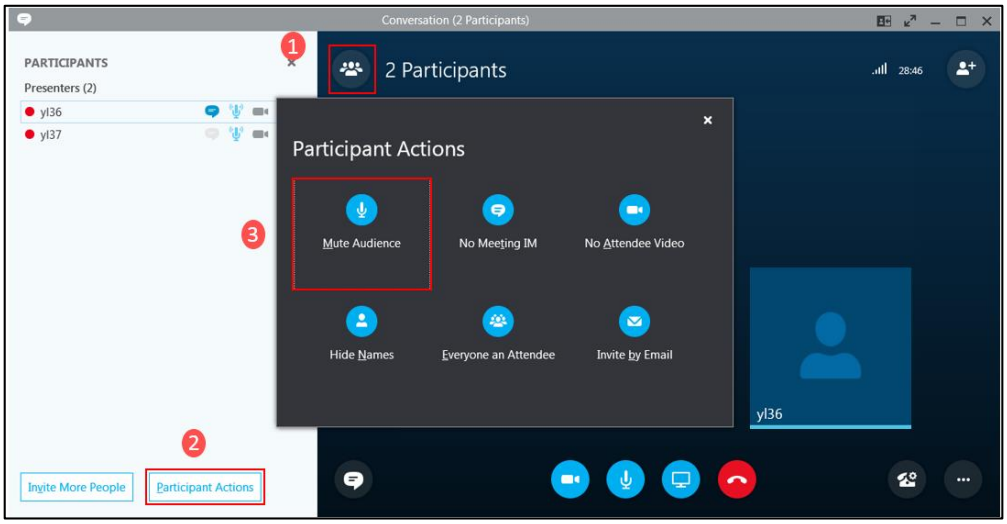
Pinning a Participant to Gallery

During a conference, right click a participant video image. Click **Pin to Gallery**, and the participant video image is displayed in a full screen.



Muting/Unmuting the Audience

Click the participant avatar icon. Click **Participant Actions**->**Mute Audience/Unmute Audience**.



Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to *DocsFeedback@yealink.com*.

Technical Support

Visit Yealink WIKI (*http://support.yealink.com/*) for the latest firmware, guides, FAQ, Product documents, and more. For better service, we sincerely recommend you to use Yealink Ticketing system (*https://ticket.yealink.com*) to submit all your technical issues.