



Pexip Infinity

Microsoft Lync / Skype for Business Deployment Guide

Software Version 14

Document Version 14.a

January 2017

Contents

Introduction	5
Architecture overview.....	5
On-prem deployment.....	5
Public DMZ deployment.....	6
Integration features	7
Pexip Infinity as a Lync / Skype for Business gateway.....	7
Simulcast from Pexip Infinity to Lync / Skype for Business AVMCU.....	7
Multistreaming from Lync / Skype for Business AVMCU to Pexip Infinity.....	8
Merging a Lync / Skype for Business meeting with a Pexip Infinity conference.....	9
Supported codecs and protocols.....	10
Limitations.....	11
Example on-prem deployment	12
Pexip Infinity configuration for an on-prem Lync / Skype for Business environment.....	13
Prerequisites.....	13
Configuration summary.....	14
Assigning a server certificate to the Pexip Infinity Conferencing Nodes.....	14
Configuring a Lync / Skype for Business server per location.....	15
Configuring DNS records and DNS servers.....	15
Configuring the SIP TLS FQDN setting for every Conferencing Node.....	16
Configuring the Pexip Infinity domain.....	16
Configuring a TURN server per location (optional).....	16
Configuring a STUN server per location.....	17
Lync / Skype for Business server configuration for an on-prem deployment.....	19
Creating a trusted application pool for the Conferencing Nodes.....	19
Adding the other Conferencing Nodes to the trusted application pool.....	20
Creating a trusted application for the pool of Conferencing Nodes.....	20
Creating a static SIP domain route and associating this route with a trusted application.....	20
Enabling the new topology.....	21
Reverting configuration.....	21
Adding more nodes or locations to an existing on-prem Lync / Skype for Business deployment.....	22
Adding a new Conferencing Node to an existing location.....	22
Adding new Front End pools (FEPs), locations and Conferencing Nodes.....	22
Example public DMZ deployment	24
Pexip Infinity configuration for public DMZ deployments.....	25
Planning DNS names for your environment.....	26

Assigning publicly-issued TLS server certificates to Conferencing Nodes	26
Configuring the SIP TLS FQDN setting for the Conferencing Nodes	27
Configuring the Pexip Infinity domain	27
Creating a Lync / Skype for Business federation DNS SRV record for your domain and its associated A-records	27
Ensuring that Lync / Skype for Business servers are not associated with a location	29
Adding additional Conferencing Nodes for extra media capacity	29
Configuring Pexip Infinity as a Lync / Skype for Business gateway	30
Using the Pexip Distributed Gateway service	30
Certificate creation and requirements	45
Creating a certificate signing request (CSR)	45
Public DMZ environment requirements	45
On-prem environment requirements	45
Comparison of public DMZ and on-prem examples	45
Adding additional nodes in the future	46
Assigning a certificate to a Conferencing Node	46
Certificates issued by intermediate CAs	46
Configuring the SIP TLS FQDN for a Conferencing Node	47
Certificate signing requests (CSRs)	48
Creating a certificate signing request	48
Uploading the signed certificate associated with a certificate signing request	49
Modifying a CSR	50
Presence and contact lists	51
Publishing presence information	51
Customizing the contact list avatar	51
Appendix 1: Public DMZ deployment with multiple SIP domains	52
Adding an additional subdomain	52
Adding an additional top-level domain	53
Appendix 2: Configuring Pexip Infinity nodes to work behind a NAT device	54
Appendix 3: Firewall ports	55
Appendix 4: Troubleshooting and limitations	56
Lync/SfB client does not connect to Pexip Infinity conference	56
Checklist	56
Detail	56

Lync/SfB client can successfully connect to the Pexip Infinity conference, but audio and/or video is not working in one or both directions	56
Checklist	56
Collecting SIP logs using the Lync/SfB Server Logging Tool	57
Conference status shows backplanes to a merged Lync meeting with no participants	58
Poor image quality and delays when sharing content from Lync/SfB	58
Received content can be slow to update	58
DNS resolution failures	58
Sending messages from a Lync/SfB client to a locked conference	58
Lync/SfB participants do not receive presentations / content sharing	58
Video calls from a Lync 2010 client for iOS only connect with audio	59
Lync/SfB presenter sees "Someone has joined and can't see what's being presented or shared" notification	59
Lync/SfB users see low-resolution presentations in small scale	59
Can only make audio calls when using a Cisco VCS for call control	59
No video on Lync for Mac or Lync 2010 (PC) in Lync meetings	59
Poor sound quality	59
Problems connecting to Lync meetings via the Virtual Reception (IVR gateway)	59
Audio-only calls when using a VCS for call control	60
Pexip VMR participants can't see shared PowerPoint files	60

Introduction

This guide describes how to deploy Microsoft Lync and Skype for Business with the Pexip Infinity distributed conferencing platform.

Pexip Infinity allows Microsoft Lync and Skype for Business* users to meet with other people regardless of the system they are using – Lync / Skype for Business, web browsers or traditional video conferencing systems. All participants can enjoy wideband audio, high definition video and cross-platform presentation sharing.

Pexip Infinity can be integrated with Lync/SfB as part of an existing, on-premises Lync/SfB environment inside an enterprise network, or as a standalone Pexip environment deployed in a public DMZ, leveraging direct federation with remote Lync/SfB environments. It enables full interoperability between Microsoft's H.264 SVC/RTV/RDP and H.263, H.264, VP8 (WebRTC) and BFCP/H.239 for truly seamless video and content sharing in any-to-any configurations, such as multiparty conferences.



In addition to enabling Lync/SfB participants to join conferences hosted on Pexip Infinity, Pexip Infinity can act as a gateway between Lync/SfB and standards-based endpoints. This enables Lync/SfB clients to receive and initiate point-to-point calls with H.323/SIP endpoints and registered Infinity Connect clients, and invite those devices into a Lync meeting while retaining the native meeting experience on each device.

The version 14 release of Pexip Infinity is interoperable with:

- Lync 2010 and 2013 desktop clients for Windows
- Lync 2011 desktop clients for Mac OS X
- Lync 2013 mobile clients for Apple iOS and Android devices
- Skype for Business.

* Note that where this documentation refers to "Lync/SfB", it represents both Microsoft Lync and Skype for Business unless explicitly stated otherwise.

Architecture overview

Pexip Infinity can be integrated with Lync/SfB in two different ways:

- as part of an existing, on-premises Lync/SfB environment inside an enterprise network (referred to in this document as **on-prem deployment**)
- as a standalone Pexip environment deployed in a public DMZ, leveraging direct federation with remote Lync/SfB environments (referred to in this document as **public DMZ deployment**).

This deployment guide covers both deployment methods. You will typically choose one of the above two methods, depending on requirements and preference. Each deployment method has a set of pre-requisites and configuration steps which are covered in detail in the relevant sections.

On-prem deployment

To integrate Pexip Infinity with an existing, on-premises Lync/SfB environment, one or more SIP domains are statically routed from the Lync/SfB environment towards one or more Pexip Infinity Conferencing Nodes. Then, when a Lync/SfB user dials a conference alias, such as `meet.john@example.com`, or the alias of a standards-based endpoint, the user is placed into the appropriate Pexip-hosted conference. The Lync/SfB user can also pin one or more such aliases to their contact list for easy access later.

Pexip Infinity supports routing on the same domain as the main Lync/SfB installation, or a different domain/subdomain. If the same domain is used, Pexip Infinity services (such as a Virtual Meeting Room), or standards-based endpoints, cannot have a URI that is already in use by a Lync/SfB-enabled user in Active Directory. For example, if a user's Lync/SfB URI is `john@example.com` this could not be used as their VMR alias; however `meet.john@example.com` could be used.

With Lync/SfB environments that are geographically spread, for instance with Lync/SfB infrastructure in both Europe and US, it may be desirable to deploy a pool of one or more Conferencing Nodes in each location, to ensure efficient media routing between a Conferencing Node and the Lync/SfB user. In these cases, a static SIP domain route should be created from the local Front End pool (FEP) towards a redundant pool of Conferencing Nodes in its nearest geographic location. If two Lync/SfB users from different geographic areas dial into a conference via Conferencing Nodes at different locations, the two local conferences are automatically merged together by the virtual backplane between the two respective Conferencing Nodes.

In a similar manner, to support dialing out from a conference to a Lync/SfB participant, Lync/SfB servers are configured for each location. This allows Pexip Infinity to dial out to the Lync/SfB server from a Conferencing Node at the most appropriate geographic location.

For further information, see [Example on-prem deployment](#).

Public DMZ deployment

As Pexip Infinity supports Lync/SfB natively, it can be deployed to enable Lync/SfB interoperability without having any existing, on-prem Lync/SfB infrastructure. In such a deployment, Pexip Infinity can federate directly with remote Lync/SfB environments (on-prem environments as well as Lync/SfB Online/Office 365), without the need for a local Lync/SfB environment.

In this mode, Pexip Infinity can be deployed in a single datacenter, or if desired, multiple geographically-dispersed datacenters, optionally leveraging call control and/or GeoDNS functionality for ensuring optimal/shortest path signaling and media routing across public networks.

If required, Pexip Infinity nodes can be deployed in a DMZ behind a static NAT firewall.

For further information, see [Example public DMZ deployment](#).

Integration features

Pexip Infinity enhances the feature set of Microsoft Lync and Skype for Business by providing users with their own personal Virtual Meeting Room that is available at all times, and can be used for ad-hoc and scheduled meetings for any number of people.

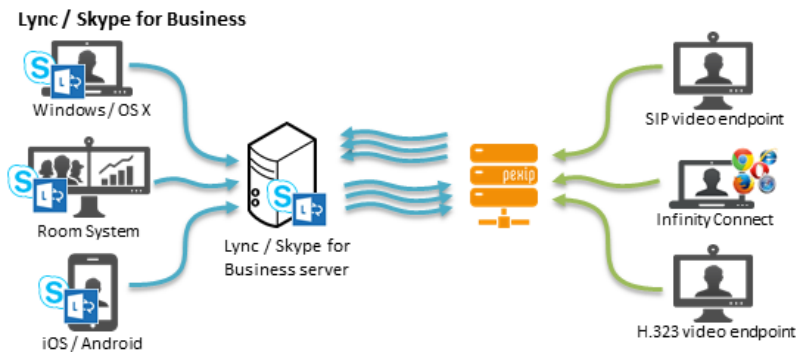
In addition, Pexip Infinity can be used as a direct [gateway](#) between any two users, regardless of device or technology. As a gateway, Pexip Infinity enables users to join from any system to a Lync meeting. This allows non-Microsoft users with anything from web browsers to traditional group videoconferencing systems to join a Lync meeting just like any Lync / Skype for Business user.

Pexip's tight integration with Lync/SfB includes Pexip Fusion features such as [simulcasting](#), [multistreaming](#) and even the ability to [merge](#) a Pexip VMR conference with a Lync meeting to provide a native experience for all participants.

Pexip Infinity as a Lync / Skype for Business gateway

Pexip Infinity can act as a gateway between Lync/SfB and standards-based endpoints. This enables Lync/SfB clients to:

- invite H.323/SIP endpoints and registered Infinity Connect clients into a Lync meeting
- use the Pexip Distributed Gateway service to route incoming calls directly into an ad hoc or scheduled Lync meeting
- when dialed into a Pexip VMR conference, invite other Lync/SfB or external contacts into that same Pexip VMR (this creates a new Lync meeting which is merged with the existing Pexip VMR)
- receive and initiate person-to-person calls with standards-based devices.



The Pexip Distributed Gateway is configured as a series of Call Routing Rules which specify which calls should be interworked and to where.

For information about how to configure the Lync/SfB gateway functionality, see [Configuring Pexip Infinity as a Lync / Skype for Business gateway](#).

Simulcast from Pexip Infinity to Lync / Skype for Business AVMCU

Pexip Infinity can send the video streams of gateway participants at multiple resolutions to a Lync/SfB meeting hosted on the Lync/SfB AVMCU.

This means that if Lync/SfB clients request different video resolutions from the AVMCU, Pexip Infinity will support the equivalent request for that resolution from the AVMCU.



This optimizes the Lync/SfB user experience for all Lync meeting participants, and for all device sizes from a mobile client to the Microsoft Surface Hub.

When viewing the status of the backplane media streams via the Pexip Infinity Administrator interface, a separate stream is shown for every resolution currently being sent. This example shows 3 current simulcast streams:

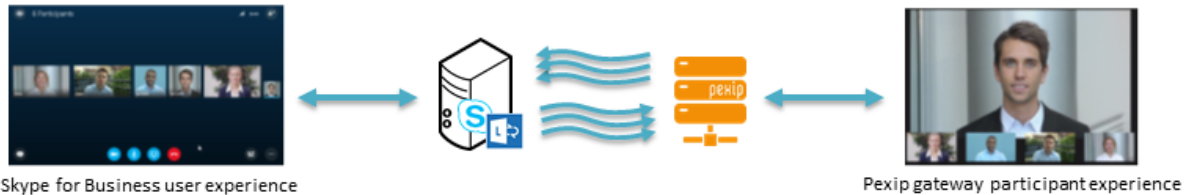
Media streams													
Type	Start time	Tx codec	Tx bitrate (kbps)	Tx resolution	Tx packets sent	Tx packets lost	Tx jitter (ms)	Rx codec	Rx bitrate (kbps)	Rx resolution	Rx packets received	Rx packets lost	Rx jitter (ms)
Audio	2015-11-13 16:44:11 (GMT)	G.722	0		0	0	0.0	G.722	0		0	0	0.0
Video	2015-11-13 16:44:11 (GMT)	H.264 UC	2500	1280x720	46926	0	0.02	Off	0		0	0	-0.0
Video	2015-11-13 16:44:11 (GMT)	H.264 UC	170	320x180	46240	0	0.0	Off	0		0	0	-0.0
Video	2015-11-13 16:44:11 (GMT)	H.264 UC	518	640x360	31009	0	0.0	Off	0		0	0	-0.0

Simulcast to Lync/SfB AVMCU is automatically enabled on Pexip Infinity from version 11 and requires no administrator configuration.

Multistreaming from Lync / Skype for Business AVMCU to Pexip Infinity

Pexip Infinity can receive multiple video streams from an AVMCU multi-party conference. This provides an enhanced conferencing experience for all participants connected to a Lync meeting:

- Participants in a Pexip VMR that has been **merged** with a Lync meeting see a combined set of Pexip VMR and Lync meeting participants.
- Participants connected to a Lync meeting via the Pexip Distributed Gateway see a full combined set of both Lync/SfB participants and any other Pexip gateway participants in the conference. They always see the default Pexip 1 +7 layout (large main speaker and up to 7 other participants), and at a resolution optimized for the participant's device, as shown below:



Note that:

- There are always 6 video streams negotiated with the AVMCU, one in HD and the others at thumbnail resolution. However, no unnecessary resource capacity is used on Pexip Infinity if a stream is not active.

When viewing the status of the backplane media streams via the Pexip Infinity Administrator interface, each of the 6 negotiated media streams is shown. In this example, only 2 of the 6 streams are currently active:

Type	Start time	Tx codec	Tx bitrate (kbps)	Tx resolution	Tx packets sent	Tx packets lost	Tx jitter (ms)	Rx codec	Rx bitrate (kbps)	Rx resolution	Rx packets received	Rx packets lost	Rx jitter (ms)
Video	2015-11-13 16:44:11 (GMT)	Off	0		0	0	0	H.264 UC	9	320x180	12137	0	4.73
Video	2015-11-13 16:44:11 (GMT)	Off	0		0	0	0	H.264 UC	14	424x240	42840	0	1.31
Video	2015-11-13 16:44:11 (GMT)	Off	0		0	0	0	Off stage	0		0	0	0.0
Video	2015-11-13 16:44:12 (GMT)	Off	0		0	0	0	Off stage	0		0	0	0
Video	2015-11-13 16:44:12 (GMT)	Off	0		0	0	0	Off stage	0		0	0	0
Video	2015-11-13 16:44:12 (GMT)	Off	0		0	0	0	Off stage	0		0	0	0
Video	2015-11-13 16:44:11 (GMT)	H.264 UC	150	320x180	108312	14	0.0	Off	0		0	0	0.0

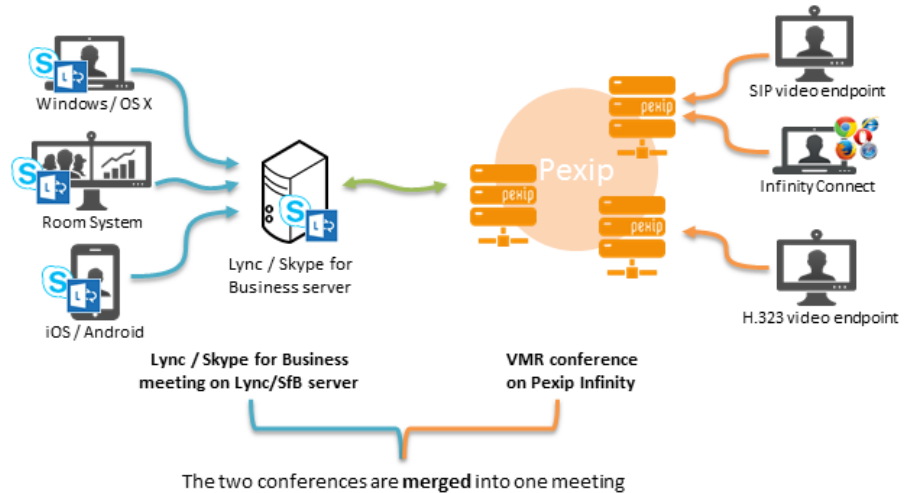
- As the AVMCU can only send a maximum of 6 video streams, if more than 6 AVMCU participants are shown on the stage in a Pexip Infinity layout (as seen by Pexip VMR participants or a Pexip gateway participant), those additional AVMCU participants display as a broken camera.
- When an AVMCU participant is spotlighted, all other AVMCU participants switch to audio only:
 - Pexip VMR participants see audio indicators instead of video for all of the other AVMCU participants, but still see video from other VMR participants.
 - Pexip gateway participants see audio indicators instead of video for all other participants.

Lync/SfB AVMCU multistreaming is automatically enabled on Pexip Infinity from version 11 and requires no administrator configuration.

Merging a Lync / Skype for Business meeting with a Pexip Infinity conference

A Lync meeting can be merged with a conference being hosted on the Pexip Infinity platform. This means that, for example:

- A Lync/SfB user dialed into a Pexip VMR can use drag-and-drop to add a contact (such as a Microsoft Surface Hub system, or an external SIP/H.323 device) into the meeting. This will create an adhoc Lync meeting and merge it with the Pexip VMR.
- A Lync/SfB user in a Lync meeting can drag and drop a Pexip VMR contact into the Lync meeting to manually merge the conferences together.



The ability to merge a Lync meeting with a Pexip VMR is automatically enabled on Pexip Infinity from version 11 and requires no specific administrator configuration, however appropriate Call Routing Rules need to be configured on Pexip Infinity to enable calls to be routed to Lync/SfB contacts that are external SIP/H.323 devices.

Pexip Fusion

The participant experience when a Lync meeting and a Pexip VMR conference are merged together depends upon whether the participant is connected to the Lync meeting or the Pexip VMR. Pexip's Fusion technology delivers a native experience that ensures that both sets of participants retain their native conferencing experience for their device or platform.

For participants connected to the Pexip VMR:

- All participants see a combined set of Pexip VMR and Lync meeting participants.
- Standard rules apply (based on current and most recent speakers) for who takes the main speaker view and which participants appear as thumbnails in the VMR's stage layout.
- Infinity Connect clients see the complete roster for the merged conference, including all remote Lync meeting participants, however they cannot control those remote participants (disconnect, mute and so on).

For participants connected to the Lync meeting:

- All participants in the Lync meeting see the Pexip VMR stage as a participant alongside the other Lync meeting participants (all participant video streams are displayed as normal to Lync/SfB clients according to its selected viewing mode).
- The participant list includes a single entry representing the Pexip VMR (displayed as the name of the service).
- If there are no participants currently in the Pexip VMR, the VMR stage participant displays as a broken camera.

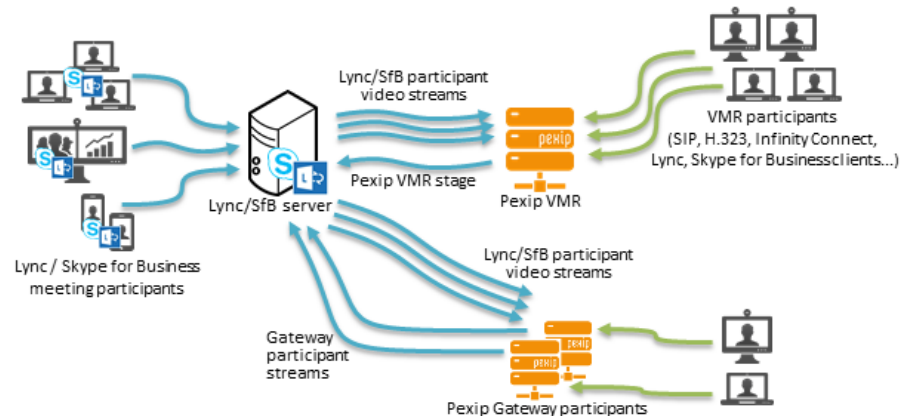
In addition, in their contacts list, Lync/SfB clients can see a Presence status for their Pexip service contacts and Pexip Distributed Gateway contacts (see [Presence and contact lists](#) for more information).

Merged Lync meeting and Pexip Infinity conference with additional Pexip Distributed Gateway participants

This diagram shows a Pexip VMR conference that has been merged with a Lync meeting that has native Lync/SfB participants plus additional participants connected to the Lync meeting via the Pexip Distributed Gateway.

In this scenario:

- The Lync/SfB AVMCU multistreams all Lync meeting participants — including the Pexip Distributed Gateway participants — to the Pexip VMR.
- Each Pexip Distributed Gateway participant receives a multistream from the AVMCU containing the Pexip VMR stage, native Lync/SfB clients, plus any other gateway participants connected to that Lync meeting.
- Native Lync/SfB client participants see the Pexip VMR stage as a participant alongside all of the other Lync meeting participants (including each Pexip Distributed Gateway participant) according to the Lync/SfB client's layout mode.



Supported codecs and protocols

Supported codecs for calls between Pexip Infinity and Lync / Skype for Business:

- Video: H.264 UC and multistream H.264SVC (Lync 2013 and Skype for Business), and Microsoft RTVideo (Lync 2010, Lync 2013 and Skype for Business).
- Audio: G.722.

Desktop/application window sharing, RDP and VbSS:

- Desktop and single application windows can be shared from Lync / Skype for Business for Windows, and Lync / Skype for Business for Mac.
- Pexip Infinity supports bi-directional RDP. Lync / Skype for Business users can send and receive dual streams.
- Pexip Infinity supports Video-based Screen Sharing (VbSS). This is a "tech preview" feature and is currently only supported when the Skype for Business client is either calling another endpoint via the Pexip Distributed Gateway, or calling into a Virtual Meeting Room or Virtual Auditorium. For information about enabling VbSS on your Skype for Business infrastructure see <https://technet.microsoft.com/en-us/library/mt756736.aspx>.

Presenting PowerPoint files via PSOM:

- Participants connected to the Pexip VMR in a Lync / Skype for Business Fusion or gateway call can see shared content if a Lync / Skype for Business user presents PowerPoint files. Pexip Infinity supports the Persistent Shared Object Model (PSOM).
- Supported for desktop Lync 2013 and Skype for Business clients.
- Requires Office Web Apps (OWA) Server.
- Slide animation is not supported; Pexip participants will see a composite JPEG image. Also, annotations are not supported.

Packet loss resiliency:

- Pexip Infinity supports FEC only on content received from Lync 2010 clients, as defined in [MS-RTVPF].
- Pexip Infinity does not support FEC with Lync 2013 / Skype for Business clients.

Limitations

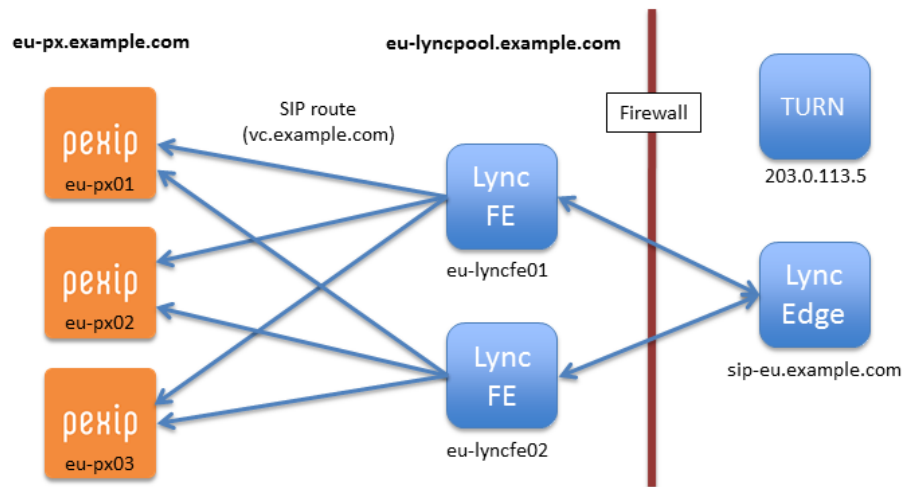
For an on-prem Pexip Infinity deployment, if there are any firewalls in between the Lync/SfB server and the Conferencing Nodes, or between the internal Lync/SfB clients and the Conferencing Nodes, these firewalls have to be configured to permit the relevant traffic (see [Appendix 3: Firewall ports](#)).

There are some limitations with merging and escalating Lync meetings with PIN-protected Pexip conferences:

- When using drag and drop to merge a PIN-protected Pexip conference into a Lync meeting, you need to include the PIN in the Lync/SfB contact address using the format `<vmr_alias>**<PIN>@<domain>`. Note that this will make the PIN visible to other Lync meeting participants. You can only merge a locked Pexip conference into a Lync meeting if the Pexip conference is also PIN-protected.
- If a Lync/SfB client dials a PIN-protected VMR directly without the PIN in the URI, and then enters the PIN manually, it may not be able to present a PowerPoint file or escalate that call to a Lync Meeting (e.g. by drag-and-dropping other Lync/SfB participants into the call). Presentation and escalation is always possible if the Lync client initially dials the VMR with the PIN in the URI.

Example on-prem deployment

This section explains how to integrate Pexip Infinity with an existing, on-prem Lync / Skype for Business environment. If you want to deploy Pexip Infinity in a public DMZ deployment, see [Example public DMZ deployment](#) instead.



Example on-prem deployment used in this guide

The diagram above shows the example deployment which forms the basis of the on-prem integration between Lync/SfB and Pexip Infinity. As Pexip Infinity is a truly distributed platform, it does not matter where messages arrive in the Pexip platform, as it will always ensure that the appropriate Conferencing Nodes get the message or the media for the conference.

This example deployment uses a setup where all components are geographically located in Europe. The local Lync/SfB infrastructure has two Lync/SfB Front End Servers in a Front End pool (**eu-lyncpool.example.com**), and a Lync/SfB Edge server. It also has three Pexip Conferencing Nodes that are all associated with the same Pexip system location (Europe), and will be set up in an application pool (**eu-px.example.com**) and integrated with Lync/SfB.

The example environment contains the following pools:

- Lync/SfB FEP **eu-lyncpool.example.com** containing:
 - **eu-lyncfe01.example.com**
 - **eu-lyncfe02.example.com**

(Note that the Lync/SfB pool is assumed to be working already; this guide does not cover how to install Lync/SfB in general.)

- Pexip Conferencing Nodes **eu-px.example.com** containing:
 - **eu-px01.example.com**
 - **eu-px02.example.com**
 - **eu-px03.example.com**

The environment also contains a Lync/SfB Edge server **sip-eu.example.com**, and a standards-based TURN server at **203.0.113.5**. Note that the Lync/SfB Edge server cannot be used as a TURN server as it does not support the relevant RFC.

i Your actual Pexip Infinity environment may differ from the example, in which case you should make relevant adjustments accordingly. This guide covers the specifics of one geographic location. Large enterprises with multiple Lync/SfB locations would simply apply the same configuration model for the other locations towards their local Pexip Conferencing Nodes (see [Adding new Front End pools \(FEPs\), locations and Conferencing Nodes](#)).

Integration objectives

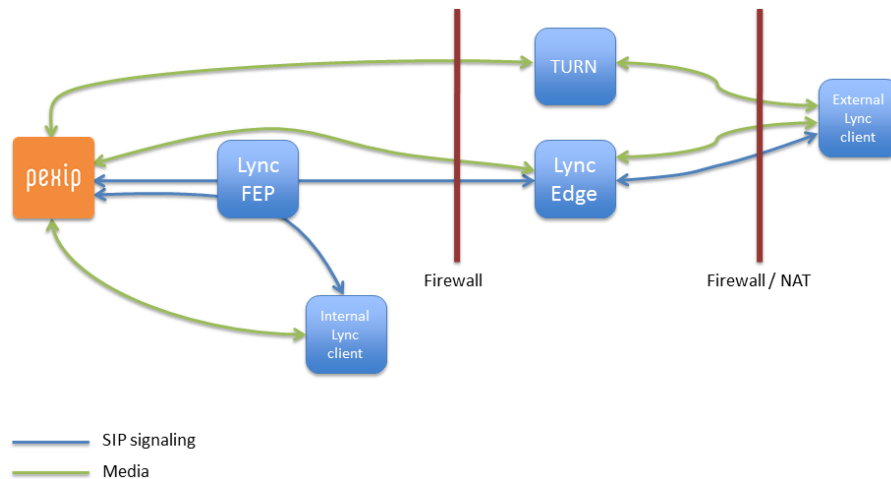
The goal with our integration is to set up a static SIP domain route for the SIP domain **vc.example.com** from the Front End pool towards a trusted application pool of local Conferencing Nodes. This provides a redundant integration environment between Lync/SfB and Pexip Infinity.

The Pexip Infinity system location that contains the Conferencing Nodes will be configured with a Lync/SfB server. Outgoing calls from Pexip Infinity to Lync/SfB clients will dial out from an appropriate Conferencing Node in that location.

Incoming calls from remote and federated Lync/SfB users will arrive at the Edge server and be routed to the Pexip Infinity Conferencing Nodes via the static SIP route on the Front End pool, similar to native, federated Lync/SfB-to-Lync/SfB calls.

For ensuring media connectivity between the internal Pexip Infinity Conferencing Nodes and external/remote and federated Lync/SfB clients, Conferencing Nodes may relay media via TURN servers located outside the enterprise firewalls in each region. However, in some deployment scenarios where the TURN server is not located outside of the enterprise firewall, you may need to configure a separate STUN server so that each Conferencing Node can discover its public NAT address. In Lync / Skype for Business deployments it is essential that a Conferencing Node can discover its public NAT address.

The following diagram illustrates the typical signaling (SIP) and media (RTP) paths for various call scenarios involving Pexip Infinity and Lync/SfB clients. Since media negotiation between Pexip Infinity and Lync/SfB involves ICE (Interactive Connectivity Establishment), media paths depend on network architecture and the presence of firewalls and NATs (Network Address Translators). Note that the actual media paths in a real deployment may differ.



Example on-prem deployment signaling and media paths

Pexip Infinity configuration for an on-prem Lync / Skype for Business environment

This section describes the configuration required on the Pexip platform to integrate Pexip Infinity with an on-prem Lync / Skype for Business environment.

As the Pexip Infinity Conferencing Nodes typically will reside on a private IP network for this type of Lync/SfB integration, the Conferencing Nodes will require access to a TURN server to ensure that RTP media (audio/video/presentation) can be exchanged with remote/external and federated Lync/SfB clients across firewalls/NAT. This TURN server is typically deployed outside the enterprise firewall or in a public DMZ.

Pexip Infinity is compatible with standards-based (RFC 5766) TURN servers such as Cisco VCS Expressway. TURN services are also offered by various commercial vendors, most of which will be compatible with Pexip Infinity. The Pexip Reverse Proxy and TURN Server features a built-in TURN server which can be used for this purpose. For more information, see [Pexip Reverse Proxy and TURN Server Deployment Guide](#).

Prerequisites

The deployment process assumes that the Management Node and the Conferencing Nodes have already been configured with basic settings, such as an IP address and NTP server, and that the Conferencing Nodes have already been configured with one or more Virtual Meeting Room aliases for the SIP domain to be used, such as `meet@vc.example.com`.

Providing all of the Conferencing Nodes in the application pool are all deployed in the same system location e.g. Europe, no additional clustering configuration is required on the Pexip platform.

Configuration summary

The Pexip Infinity configuration consists of the following steps, each described in more detail in the following sections:

1. [Assigning a server certificate](#) to the Conferencing Nodes.
2. [Configuring a Lync / Skype for Business server](#) per location.
3. [Configuring DNS records and DNS servers](#).
4. [Configuring the SIP TLS FQDN setting](#) for the Conferencing Nodes.
5. [Configuring the Pexip Infinity domain](#).
6. [Configuring a TURN server](#) per location (optional, but required for supporting external/federated Lync/SfB clients).
7. [Configuring a STUN server](#) per location (optional, but required if the TURN server is not located outside of the enterprise firewall).

After completing the Pexip Infinity configuration, you must also perform the [Lync / Skype for Business server configuration for an on-prem deployment](#).

Assigning a server certificate to the Pexip Infinity Conferencing Nodes

When integrating Pexip Infinity with an on-prem Lync/SfB environment, every Conferencing Node must be configured with a TLS server certificate which matches their respective FQDNs (Fully Qualified Domain Name), and the Lync/SfB servers must trust this certificate. Server certificates are typically issued by a Certificate Authority (CA) within the Lync/SfB environment itself (normally this will be the CA which was used to provide the Lync/SfB servers themselves with server certificates).

For more information about creating certificate signing requests, see [Certificate creation and requirements](#).

Certificate requirements

In our example deployment, any of the Conferencing Nodes may communicate with the Lync/SfB environment. Calls from Lync/SfB to Pexip Infinity are routed from the FEP to any of the Conferencing Nodes in the application pool, and outbound calls from Pexip Infinity to Lync/SfB may be initiated by any Conferencing Node. To ensure that the Lync/SfB environment trusts these Conferencing Nodes, a certificate that is trusted by the Lync/SfB servers must be assigned to every node.

We recommend that you generate and use a single SAN certificate that encompasses all of the Conferencing Nodes in the application pool.

In the certificate:

- the Subject name (commonName attribute) must be the Trusted Application Pool FQDN
- Subject Alternative Name (altNames attribute) entries must be included for every node in the pool, plus the common application pool FQDN.

Therefore, in our example, the Subject name (commonName) and SAN (altNames) sections for the certificate to be installed on every Conferencing Node would be configured as:

```
commonName = eu-px.example.com
altNames = eu-px01.example.com, eu-px02.example.com, eu-px03.example.com, eu-px.example.com
```

Assigning the certificate to Conferencing Nodes

To assign a server certificate and private key to one or more Conferencing Nodes:

1. From the Management Node, go to **Platform Configuration > TLS Certificates** and select **Add TLS certificate**.
2. Copy-paste the **TLS certificate** and its associated **Private key** into the relevant text boxes, or alternatively use the **select the file** links to upload the certificate and private key files.
3. In the **Nodes** section, from the **Available Nodes** list, select every Conferencing Node in the application pool (**eu-px01.example.com**, **eu-px02.example.com** and **eu-px03.example.com** in our example), and move them into the **Chosen Nodes** list.
4. Select **Save**. The certificate and private key will be pushed automatically to the selected Conferencing Nodes.

Uploading trusted CA certificates

- i** If the server certificate has been issued by one or more intermediate CAs (Certificate Authorities), these intermediate certificates must be uploaded. You can upload them as a single-file bundle by going to **Platform Configuration > Trusted CA Certificates** and selecting **Import**.

See [Certificates issued by intermediate CAs](#) for more information.

Configuring a Lync / Skype for Business server per location



To allow internal Conferencing Nodes to call out to Lync/SfB clients you must define the target Lync/SfB servers. In our example deployment, a Lync/SfB Front End pool has been deployed in Europe with the pool address **eu-lyncpool.example.com**.

To instruct the Conferencing Nodes in the Europe system location to use the Europe-based Lync/SfB Front End pool, you must first define the Lync/SfB Front End pool on the Management Node, and then link it to the **Europe** location, as follows:

1. Go to **Call Control > Lync / Skype For Business Servers** and select **Add Lync / Skype for Business server**:

Name	<input type="text" value="eu-lyncpool"/> *
The name used to refer to this Lync / Skype for Business server. Maximum length: 250 characters.	
Description	<input type="text" value="European Lync FEP"/>
A description of the Lync / Skype for Business server. Maximum length: 250 characters.	
Address	<input type="text" value="eu-lyncpool.example.com"/> *
The IP address or FQDN of the Lync / Skype for Business server to be used for outbound MS-SIP calls. This can be a Front End Server or Director; it cannot be an Edge Server. Maximum length: 255 characters.	
Port	<input type="text" value="5061"/>
The IP port of the Lync / Skype for Business server. Range: 1 to 65535. Default: 5061.	
Transport	<input type="text" value="TLS"/> *
The IP transport used to connect to the Lync / Skype for Business server.	

2. Complete the fields and select **Save**.
In the example above, the Europe Lync/SfB server has been defined by its pool name FQDN **eu-lyncpool.example.com**.
Note that the Lync/SfB server can be a Front End Server/Processor or a Director; it cannot be an Edge Server.
3. To assign the new Lync/SfB server to the appropriate location, go to **Platform Configuration > Locations** and select the **Europe** location.
4. In the **Lync / Skype for Business server** field, select the Europe Lync/SfB server from the drop-down list, and then select **Save**.

Lync / Skype for Business server	<input type="text" value="eu-lyncpool"/>  
The Lync / Skype for Business server to be used for outbound calls from this location. For more information, see About Lync / Skype for Business servers .	

Configuring DNS records and DNS servers

DNS A-records

In DNS, ensure that the following records are configured:

- An A-record for each Conferencing Node. In our example this would be 3 records with host names of **eu-px01**, **eu-px02** and **eu-px03**, and that they each point to individual IP address of the node.

- Another A-record per Conferencing Node. This time the host name of every record should be **eu-px.example.com** (the application pool name of the Conferencing Nodes), and again associate it with the IP address of each Conferencing Node. This step allows Lync/SfB to spread the traffic across all of the Conferencing Nodes.

Pexip Infinity DNS server configuration

Ensure that Pexip Infinity is configured to use DNS servers on the inside of the network (**System Configuration > DNS Servers**, and then assigned to each location via **Platform Configuration > Locations**). This ensures that Pexip Infinity can resolve internal hostnames, which is mandatory for communicating with Lync/SfB on-prem.

- i** If you omit this step and use an external DNS server instead, calls might drop after a few minutes when Pexip Infinity verifies that the remote side is still responding properly. This is because an external DNS server cannot resolve the internal hostname of the Lync/SfB FEPs.

Configuring the SIP TLS FQDN setting for every Conferencing Node

The SIP TLS FQDN setting for each Conferencing Node must be configured to reflect its DNS FQDN.

This is done on the Management Node, by going to **Platform Configuration > Conferencing Nodes**, choosing each node in turn and populating the **SIP TLS FQDN** field.

SIP TLS FQDN	<input type="text" value="eu-px01.example.com"/>
<small>(Required for Conferencing Nodes that are involved in signalling of calls to and from Lync / Skype for Business servers.) An identity for this Conferencing Node, used in signaling SIP TLS Contact addresses. For more information, see SIP TLS FQDN. Maximum length: 255 characters.</small>	

The example above shows the **SIP TLS FQDN** for the eu-px01 Conferencing Node, which is set to **eu-px01.example.com**.

For any Pexip Infinity and Lync/SfB integration, you must ensure that each Conferencing Node is configured with its respective DNS hostname as the **SIP TLS FQDN**. Pexip Infinity will present this as being the server name, and it must match the name on the certificate installed on the node. Each Conferencing Node must have a unique **SIP TLS FQDN**.

Configuring the Pexip Infinity domain

You must specify the name of the SIP domain that is routed from Lync/SfB to Pexip Infinity for this deployment. This domain is inserted into the From header in outbound calls from Pexip Infinity to Lync/SfB, and ensures that Lync/SfB can route messages back to Pexip Infinity when, for example, initiating content sharing.

You specify this by going to **Platform Configuration > Global Settings** and configuring the **Pexip Infinity domain (for Lync / Skype for Business integration)** setting:

Pexip Infinity domain (for Lync / Skype for Business integration)	<input type="text" value="vc.example.com"/>
<small>The name of the SIP domain that is routed from Microsoft Lync / Skype for Business to Pexip Infinity, either as a static route or via federation. You can also configure a per-location override. Maximum length: 255 characters.</small>	

- i** This must be set to the same SIP domain as used by the static route from Lync/SfB to Pexip Infinity, which is **vc.example.com** in our example (see [Creating a static SIP domain route and associating this route with a trusted application](#)).

Configuring a TURN server per location (optional)

This configuration is optional, but required for supporting external/federated Lync/SfB clients.

To allow internal Conferencing Nodes to establish two-way media connectivity with remote/external and federated Lync/SfB clients across firewalls/NAT, media may be relayed via a TURN server. In our example, the TURN server has the IP address **203.0.113.5**.



To instruct the Conferencing Nodes to use the TURN server, we must first define the TURN server on the Management Node, and then link it to the **Europe** location, as follows:

1. Go to **Call Control > TURN Servers** and select **Add TURN server**:

Add TURN server

Name	<input type="text" value="turn-europe"/> *
	<small>The name used to refer to this TURN server. Length: 250 characters.</small>
Description	<input type="text" value="TURN server for Europe conference node:"/>
	<small>A description of the TURN server. Length: 250 characters.</small>
IP address	<input type="text" value="203.0.113.5"/> *
	<small>The IP address of the TURN server.</small>
Port	<input type="text" value="3478"/> *
	<small>The IP port on the TURN server to which the Conferencing Node will connect. Range: 1 to 65535. Default: 3478.</small>
Username	<input type="text" value="turnuser"/>
	<small>The username of a valid account on the TURN server. Length: 100 characters.</small>
Password	<input type="password" value="....."/> *
	<small>The password of a valid account on the TURN server. Length: 100 characters.</small>

2. Complete the fields and select **Save**.
In the example above, the TURN server has been defined by its **IP address** and **Port**, in addition to the **Username** and **Password** for our TURN user (which has already been created on the TURN server).
3. Assign this TURN server to the appropriate location: go to **Platform Configuration > Locations** and select the **Europe** location.
4. In the **TURN server** field, select the Europe TURN server from the drop-down list, and then select **Save**.

TURN server	<input type="text" value="turn-europe"/>  
	<small>The TURN server to be used when ICE clients (including Lync clients and Infinity Connect WebRTC clients) located outside the firewall connect to a Conferencing Node in this location. For more information, see About TURN servers.</small>

Configuring a STUN server per location

This configuration is optional, but required if you need to relay media via a TURN server with external and federated Lync/SfB clients, but the TURN server is not located outside of the enterprise firewall. In this case, you will also need to configure separate STUN servers per location. This allows a Conferencing Node to discover its public NAT address, which is essential in Lync/SfB deployments.

Configuring STUN server addresses

To add, edit or delete STUN server connection details, go to **Call Control > STUN Servers**.

Note that Pexip Infinity ships with one STUN server address already configured by default: **stun.l.google.com**

Associating STUN server addresses with Conferencing Nodes

To associate a STUN server address with a Conferencing Node, you must configure the node's system location:

1. Go to **Platform Configuration > Locations**.
2. Select the Conferencing Node's location.
3. Select a **STUN server** and select **Save**.

All Conferencing Nodes in that location will use the nominated STUN server for conference calls.

STUN server

stun.l.google.com ▼  

The STUN server to be used by Conferencing Nodes in this location to determine the public IP address to signal to ICE clients (including Lync clients and Infinity Connect WebRTC clients) located outside the firewall.

Lync / Skype for Business server configuration for an on-prem deployment

This section describes the commands that need to be issued on the Lync/SfB server to set up a redundant integration where the on-prem Lync/SfB environment talks to all Pexip Infinity Conferencing Nodes as a pool of resources.

The Lync/SfB server configuration consists of the following steps (each is described in full in the sections that follow):

1. [Creating a trusted application pool](#) for the Conferencing Nodes.
2. [Adding the other Conferencing Nodes](#) to the trusted application pool.
3. [Creating a trusted application](#) for the pool of Conferencing Nodes.
4. [Creating a static SIP domain route](#) and associating this route with a trusted application.
5. [Enabling the new topology](#).

Using the Lync/SfB management shell

The above operations are performed using the Lync/SfB Management shell, which is normally available on the Lync/SfB Front End Servers in the Lync/SfB server environment.

The command syntax described in the following section is based on the devices described in the [example deployment for the on-prem Lync/SfB integration](#). Where applicable, you must replace these example parameters with parameters appropriate for your actual deployed environment.

Commands that are entered in the management shell are shown as follows:

this is the command to enter; parameters to be replaced for your actual deployment are **emphasized**

For a comprehensive overview of the Lync/SfB management shell commands used in this deployment guide, see <http://technet.microsoft.com/en-us/library/gg398867.aspx>. Additional general application activation information can be found at <https://msdn.microsoft.com/EN-US/library/office/dn466115.aspx>.

Creating a trusted application pool for the Conferencing Nodes

This command adds a trusted application pool for the Front End pool **eu-lyncpool.example.com** to trust traffic coming from Pexip Infinity (and to be able to send traffic back), as well as adding the first node (**eu-px01.example.com**) as a computer in the application pool.

```
New-CsTrustedApplicationPool -Identity eu-px.example.com -ComputerFqdn eu-px01.example.com -Registrar eu-lyncpool.example.com -Site 1 -RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true
```

Syntax explained

-Identity defines the DNS FQDN of the group of Conferencing Nodes that belong to this trusted application pool. In this example, it is **eu-px.example.com**, which must also be [configured in DNS](#).

-ComputerFqdn defines the DNS FQDN of the first node in the trusted application pool.

-Registrar defines the FQDN of the Front End pool to which this trusted application pool belongs.

-Site defines the Site ID to which this trusted application pool belongs. The Lync/SfB management shell command **Get-CsSite** can be used to retrieve the SiteID of a given Front End pool.

-RequiresReplication defines whether replication is required for this application pool. In our case this is not required.

-ThrottleAsServer defines how connections to this trusted application are throttled. In our case we use the default value of **True**.

-TreatAsAuthenticated defines whether this trusted application pool is considered authenticated, or if authentication is required. Here, we use the default value of **True**, meaning that the server with this hostname/certificate is considered to be authenticated.

i When creating a trusted application pool (and a trusted application computer in the next step) in this way, Lync/SfB will issue a warning stating:

"WARNING: Machine eu-px01.example.com from the topology you are publishing was not found in Active Directory and will result in errors during Enable-CsTopology as it tries to prepare Active Directory entries for the topology machines."

This warning can be safely ignored as the Pexip nodes are not domain joined, and you should answer Yes to this warning.

Adding the other Conferencing Nodes to the trusted application pool

You must now add the remaining two nodes, **eu-px02** and **eu-px03** in our example, as computers to the newly added trusted application pool as this is a load-balanced setup with 3 Conferencing Nodes.

Note that Lync Server 2013 Standard Edition (as opposed to Enterprise Edition) does not support adding trusted application computers to a trusted application pool. For Standard Edition Lync servers, a separate trusted application pool must be created for each Conferencing Node (in addition to the **eu-px.example.com** trusted application pool).

To add trusted application computers to the trusted application pool:

```
New-CsTrustedApplicationComputer -Identity eu-px02.example.com -Pool eu-px.example.com
New-CsTrustedApplicationComputer -Identity eu-px03.example.com -Pool eu-px.example.com
```

Creating a trusted application for the pool of Conferencing Nodes

This command creates a trusted application for the pool of Conferencing Nodes:

```
New-CsTrustedApplication -Applicationid eu-px -TrustedApplicationPoolFqdn eu-px.example.com -Port 5061
```

Syntax explained

`-ApplicationId` is a friendly identifier for the trusted application.

`-TrustedApplicationPoolFqdn` defines which trusted application pool that this trusted application belongs to.

`-Port` defines which port the trusted application (the Conferencing Nodes) will be sending SIP traffic from. In our case this is 5061 (SIP TLS).

Creating a static SIP domain route and associating this route with a trusted application

In Lync/SfB, static SIP routes can either be associated with the global routing table, or with a specific Lync/SfB registrar or registrar pool. In our case, we want to have one static SIP route per location (i.e. per registrar), so that we can route SIP and media traffic from a Front End pool to a pool of Conferencing Nodes.

This example creates a static route from the Europe Front End pool (**eu-lyncpool.example.com**) to the **eu-px.example.com** nodes for the domain **vc.example.com**:

First, you need to check if there is any existing routing configuration for the registrar. To do this, run the command:

```
Get-CsStaticRoutingConfiguration
```

On a new system this may report only:

```
Identity : Global
Route : {}
```

or if there is existing routing configuration the output will contain additional routes, for example:

```
Identity : Global
Route : {}
```

```
Identity : Service:Registrar:eu-lyncpool.example.com
Route :
{MatchUri=something.example.com;MatchOnlyPhoneUri=False;Enabled=True;ReplaceHostInRequestUri=False...}
```

You need to check if the **Identity** in any of the routes matches your registrar. The example output above does have a match for our registrar (**eu-lyncpool.example.com**).

If there is not an existing **Identity** that matches your registrar, then you need to use the following command to create a new static routing configuration for your registrar:

```
New-CsStaticRoutingConfiguration -Identity "Service:Registrar:eu-lyncpool.example.com"
```

Now you can apply your required static route to your registrars' static routing configuration by using the following commands:

```
$route = New-CsStaticRoute -TLSSRoute -Destination "eu-px.example.com" -Port 5061 -MatchUri "vc.example.com" -
UseDefaultCertificate $true

Set-CsStaticRoutingConfiguration -Identity "Service:Registrar:eu-lyncpool.example.com" -Route @{$Add=$route}
```

If static routes for additional domains are required, this can be achieved by re-running the 2 commands above, substituting the `-MatchUri` parameter with the desired domain name. If the specified domain is the primary SIP domain used for this Lync/SfB environment, Lync/SfB will only send SIP requests which are not destined to actual Lync/SfB users for that domain towards the Conferencing Nodes.

Pexip Infinity supports both same domain, and subdomain or different domain integrations. If your Lync/SfB environment consists of thousands of Lync/SfB users, consult your Pexip support representative to discuss the recommended design and dial plan.

Syntax explained

`Get-CsStaticRoutingConfiguration` returns information about the current static routing configuration.

`New-CsStaticRoutingConfiguration` creates a new static routing configuration for a given registrar (unless it already exists).

`-Identity` defines the registrar for which we want to create this new static routing configuration.

`$route` defines a variable to hold the static route object that we are creating.

`-TLSSRoute` defines that the route we are creating will use SIP TLS for signaling transport.

`-Destination` defines the DNS FQDN where Lync/SfB should send SIP requests matching the domain specified in `-MatchUri`.

`-Port` defines the TCP port to which the SIP requests should be sent, in our case 5061 for SIP TLS.

`-MatchUri` defines the SIP domain to statically route towards the Conferencing Nodes.

`-UseDefaultCertificate $true` defines that the route uses the default certificate for authentication purposes.

`Set-CsStaticRoutingConfiguration` applies a given static route object to a static routing configuration.

`-Identity` defines the registrar on which we want to apply the static route object. In our case this is the Europe Front End pool.

`-Route @{$Add=$route}` defines the static route object that we want to apply. Note that the variable name, in our case `$route`, is case sensitive.

Enabling the new topology

The new topology can now be enabled using the following command:

```
Enable-CsTopology
```

After this command has been run, it should be possible to place calls from Lync/SfB clients to **meet@vc.example.com** and similar aliases within a few minutes. Lync/SfB clients which are already logged in may have to log out and back in again before being able to place calls towards the Pexip Infinity Conferencing Nodes.

If the calls fail, check the Pexip Administrator log, or the Support log to see if your call is reaching Pexip Infinity.

Reverting configuration

If you need to undo the changes to your Lync/SfB deployment that have been made by following this guide, you must:

- Remove static SIP domain routes.
- Remove trusted application pools. Removing the trusted application pool will automatically remove all trusted applications within that pool.
- Re-enable the topology.

The commands below show how to achieve this using our example deployment.

Removing the static routing configuration

```
$route=New-CsStaticRoute -TLSSRoute -Destination "eu-px.example.com" -MatchUri "vc.example.com" -Port 5061 -
UseDefaultCertificate $true

Set-CsStaticRoutingConfiguration -Identity "service:Registrar:eu-lyncpool.example.com" -Route @{$Remove=$route}
```

Removing the trusted application pools

```
Remove-CsTrustedApplicationPool -Identity "eu-px.example.com"
```

Re-enabling the topology

```
Enable-CsTopology
```

Adding more nodes or locations to an existing on-prem Lync / Skype for Business deployment

This section explains the steps involved if you need to add additional Conferencing Nodes, or new Lync / Skype for Business servers and Conferencing Nodes in a new geographic location, to an existing on-prem Lync/SfB environment.

Adding a new Conferencing Node to an existing location

Within Pexip Infinity

Using the names of the example environment described in this guide, you need to:

- Assign a hostname to the Conferencing Node, e.g. in the format **eu-pxNN.example.com**.
- Assign a DNS A record for this Conferencing Node, registered as **eu-pxNN.example.com**.
- Add a DNS A record to the pool domain **eu-px.example.com** so that Lync/SfB will also load balance over this new node.
- Generate a new single certificate for all of the Conferencing Nodes in the application pool. This new certificate should contain the same name information as the existing certificate, with the addition of the FQDN of the new node as another SAN (Subject Alternative Name).

The new certificate must be uploaded to all of the Conferencing Nodes in the application pool.

For example, before adding the new node, the certificate name information in our example would be:

```
CN=eu-px.example.com, SAN=eu-px.example.com, px-cn1.example.com, px-cn2.example.com
```

The name information in the new certificate would be (assuming the new hostname is **px-cn3.example.com**):

```
CN=eu-px.example.com, SAN=eu-px.example.com, px-cn1.example.com, px-cn2.example.com, px-cn3.example.com
```

Within Lync/SfB

You need to add the identity of the new Conferencing Node to the existing Trusted Application Pool, in our example **eu-px.example.com**:

```
New-CsTrustedApplicationComputer -Identity eu-pxNN.example.com -Pool eu-px.example.com
```

and then enable topology:

```
Enable-CsTopology
```

Adding new Front End pools (FEPs), locations and Conferencing Nodes

If you have Lync/SfB servers and Conferencing Nodes in other geographic locations, then you should apply the same configuration model for these other locations as described for the [Europe location configuration](#).

For example, if you had the following devices located in the USA:

- 2 Lync/SfB Front End Servers **us-lynccfe01** and **us-lynccfe02** in a pool **us-lynccpool.example.com**
- 2 Conferencing Nodes **us-px01** and **us-px02** in **System location US** and to be placed in an application pool **us-px.example.com**

Within Pexip Infinity

1. Generate and assign a server certificate to the US Conferencing Nodes:
commonName = **us-px.example.com**
altNames = **us-px01.example.com, us-px02.example.com, us-px.example.com**

2. Configure the US system location to use:
 - the **us-lyncpool.example.com** Front End pool
 - DNS servers on the inside of the network
 - a TURN server
 - a STUN server.
3. Configure DNS records for the US Conferencing Nodes:
 - A-records for each Conferencing Node **us-px01** and **us-px02**
 - another A-record per Conferencing Node with the host name **us-px.example.com** (the application pool name of the Conferencing Nodes).
4. Configure the SIP TLS FQDN setting for each US Conferencing Node to reflect its DNS FQDN e.g. **us-px01.example.com** and **us-px02.example.com**.

Within Lync/SfB

1. Create a trusted application pool for the Conferencing Nodes.
 This command adds a trusted application pool for the Front End pool **us-lyncpool.example.com** and adds the first node (**us-px01.example.com**) as a computer in the application pool:

```
New-CsTrustedApplicationPool -Identity us-px.example.com -ComputerFqdn us-px01.example.com -Registrar us-lyncpool1.example.com -Site 1 -RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true
```
2. Add the other Conferencing Nodes in that location to the trusted application pool.
 This command adds **us-px02** to the new trusted application pool:

```
New-CsTrustedApplicationComputer -Identity us-px02.example.com -Pool us-px.example.com
```
3. Create a trusted application for the pool of Conferencing Nodes.
 This command creates a trusted application for the **us-px.example.com** pool:

```
New-CsTrustedApplication -Applicationid us-px -TrustedApplicationPoolFqdn us-px.example.com -Port 5061
```
4. Create a static SIP domain route and associate it with the trusted application.
 This example creates a static route from the US Front End pool (**us-lyncpool.example.com**) to the **us-px.example.com** nodes for the domain **vc.example.com**:

```
$newroute = New-CsStaticRoute -TLSSRoute -Destination "us-px.example.com" -Port 5061 -MatchUri "vc.example.com" -UseDefaultCertificate $true
Set-CsStaticRoutingConfiguration -Identity "Service:Registrar:us-lyncpool.example.com" -Route @{Add=$newroute}
```

Note that if there is no existing routing configuration for this registrar, this can be created via:

```
New-CsStaticRoutingConfiguration -Identity "Service:Registrar:us-lyncpool.example.com"
```
5. Enable the new topology using the following command:

```
Enable-CsTopology
```

Example public DMZ deployment

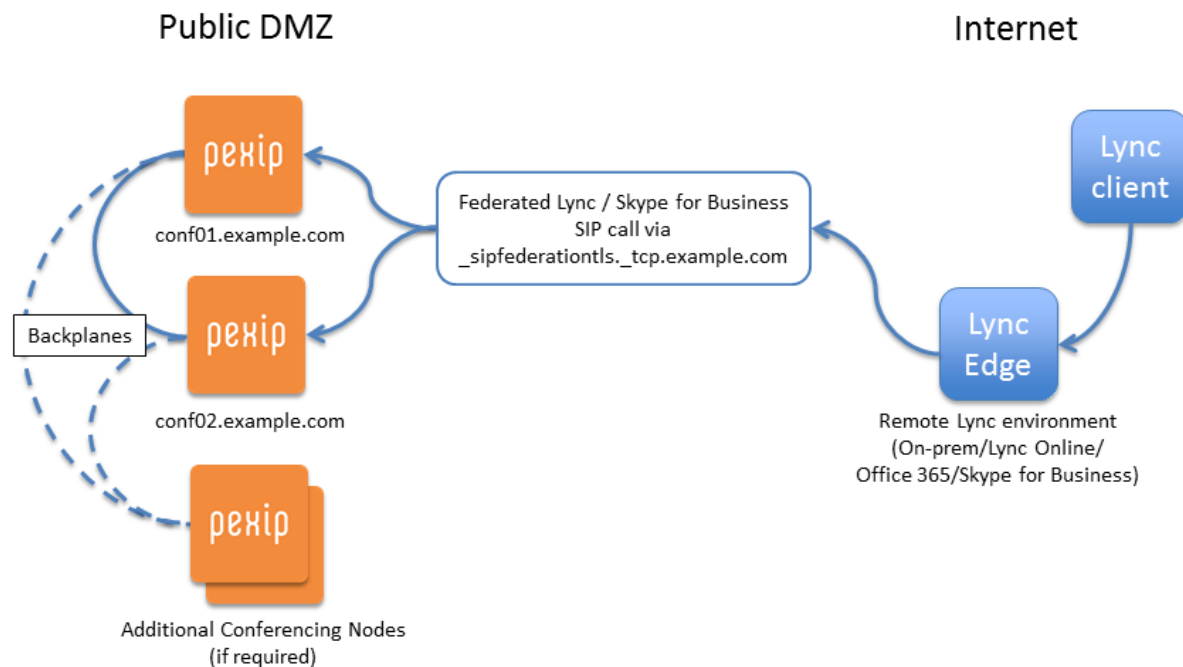
This section explains how to deploy Pexip Infinity in a public DMZ for enabling direct federation with remote Lync / Skype for Business environments such as Office 365 and Lync / Skype for Business Online as well as traditional enterprise Lync / Skype for Business environments. If you want to integrate Pexip Infinity with an existing, on-prem Lync/SfB environment, see [Example on-prem deployment](#) instead.

For integrating Pexip directly with remote Lync/SfB environments, the following requirements have to be satisfied:

- The Conferencing Nodes in the Pexip environment must be deployed in a public DMZ network, meaning all Conferencing Nodes must be assigned publicly-reachable IP addresses, either directly or they can be deployed behind static NAT.
- For inbound call support, at least one Conferencing Node must be configured with a public TLS server certificate (provided by an official CA provider such as Verisign, Comodo, GlobalSign and similar). For outbound call support, all Conferencing Nodes in the public DMZ must be configured with a public TLS server certificate.

Note that RDP content sharing from Pexip Infinity towards a Lync/SfB client is considered an outbound call, even if the Lync/SfB client had dialed in to the conference, as RDP is a separately initiated SIP session.

- The Lync/SfB federation DNS SRV record for the video domain in use must resolve to the Conferencing Node(s) that will receive incoming calls.



Example public DMZ deployment used in this guide

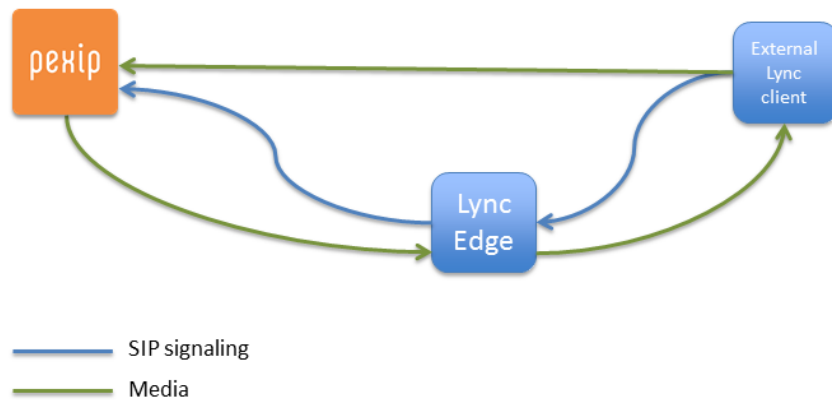
The diagram above shows the example deployment which forms the basis of the public DMZ deployment in this guide. In this scenario, all Conferencing Nodes are deployed in a public DMZ network. Two Conferencing Nodes are configured to receive incoming calls (handle the SIP signaling). Additional Conferencing Nodes can optionally be deployed to increase the media capacity. Media processing is dynamically distributed among all the Conferencing Nodes.

The Management Node will typically also be located in the same public DMZ, but this is not a requirement. The Management Node can be located on an internal network behind the public DMZ, as long as:

- there is no NAT (Network Address Translation) taking place between Pexip Infinity nodes on the internal network and nodes on the public DMZ, and
- any firewalls between the two networks are configured to pass IPsec traffic in both directions between the Management Node and all Conferencing Nodes in the Pexip environment.

The following diagram illustrates the typical signaling (SIP) and media (RTP) paths for various call scenarios involving Pexip Infinity and Lync/SfB clients. Since media negotiation between Pexip Infinity and Lync/SfB involves ICE (Interactive Connectivity

Establishment), media paths depend on network architecture and the presence of firewalls and NATs (Network Address Translators). Note that the actual media paths in a real deployment may differ.



Example public DMZ deployment signaling and media paths

Pexip Infinity configuration for public DMZ deployments

In this example, two Pexip Infinity Conferencing Nodes have been deployed in a public DMZ alongside the Management Node, as follows:

- conf01.example.com (Conferencing Node 1)
- conf02.example.com (Conferencing Node 2)

These Conferencing Nodes will handle the SIP signaling for the incoming calls. In general, for redundancy or load balancing we recommend a maximum of 2 or 3 Conferencing Nodes for handling incoming calls, which ideally are hosted on different physical servers for extra resiliency. Optionally, additional media processing nodes (conf03.example.com, conf04.example.com etc.) may also be deployed if required.

The deployment process assumes that the Management Node and the Conferencing Nodes have already been configured with basic settings, such as an IP address and a DNS server, and that the Conferencing Nodes have already been configured with one or more Virtual Meeting Room aliases for the SIP domain to be used.

To allow remote Lync/SfB environments to communicate with our public DMZ Pexip environment through federated connections, we must complete the following steps:

1. [Plan DNS names](#) for your environment.
2. [Assign publicly-issued TLS server certificates](#) to the Conferencing Nodes.
3. [Configure the SIP TLS FQDN setting](#) for the Conferencing Nodes.
4. [Configure the Pexip Infinity domain](#) to, in this case, **example.com**.
5. [Create a Lync/SfB federation DNS SRV record and its associated A-records](#) for the SIP domain **example.com** (which will use the **sip.example.com** hostname and round-robin DNS to refer to the 2 Conferencing Nodes).
6. [Ensure that Lync/SfB servers are not associated with a location](#) so that each Conferencing Node uses DNS to locate an appropriate system via which to route outbound calls to Lync/SfB clients.

Optional configuration:

- [Adding additional Conferencing Nodes](#) for extra media capacity.
- [Appendix 1: Public DMZ deployment with multiple SIP domains](#) if you need to support multiple subdomains or top-level domains.
- [Appendix 2: Configuring Pexip Infinity nodes to work behind a NAT device](#) if you want to deploy your Conferencing Nodes behind static NAT.

Planning DNS names for your environment

In this example environment, the domain **example.com** is used as the SIP domain and is used in all of the configuration examples below. Use this as a model for your deployment, using your own domain and hostnames as appropriate.

Note that if you already have your domain name such as **example.com** in use by Office365, you will already have **sip.example.com** associated with that environment. If you intend to use the same main domain for your Pexip deployment, then — to avoid any conflicts — you must use a subdomain for your Pexip environment i.e. **<subdomain>.example.com**. You will therefore need to adapt the naming patterns used in these examples when applying them to your own environment. For example, for a subdomain of **vc.example.com**, your DNS A record hostname that refers to your DMZ Conferencing Nodes would be **sip.vc.example.com**, your **_sipfederationtls._tcp** SRV record would need to be **_sipfederationtls._tcp.vc.example.com**. and your individual Conferencing Node hostnames would be **conf01.vc.example.com**, **conf02.vc.example.com** etc.

Assigning publicly-issued TLS server certificates to Conferencing Nodes

To enable a Pexip Infinity public DMZ deployment to receive incoming Lync/SfB calls from federated peers, one or more of the Conferencing Nodes (**conf01.example.com** and **conf02.example.com** in our example) in the public DMZ must be configured with a publicly-issued TLS server certificate. This ensures that remote Lync/SfB environment Edge servers will trust the Conferencing Node.

If only inbound call support is required, a certificate needs to be installed only on the Conferencing Node (or nodes, as in our example) referenced by the **_sipfederationtls._tcp** SRV record. These referenced nodes will handle the SIP signaling; media processing will be dynamically distributed among all the Conferencing Nodes assigned to the same location.

However, if outbound Pexip Infinity to Lync/SfB call support is required, **all** of the Conferencing Nodes within the public DMZ must have publicly-issued certificates installed. This is because outbound calls from Pexip Infinity to Lync/SfB may be initiated by any Conferencing Node.

In deployments where inbound and outbound call support is required, we recommend that you generate and use a single SAN certificate that encompasses all of the Conferencing Nodes in the public DMZ.

In the certificate:


- the Subject name (commonName attribute) should be set to the hostname referenced by the **_sipfederationtls._tcp** SRV record
- Subject Alternative Name (altNames attribute) entries must be included for every individual node in the public DMZ (including the hostname referenced in the Subject name).

Therefore, in our example, the Subject name (commonName) and SAN (altNames) sections for the certificate to be installed on every Conferencing Node would be configured as:

```
commonName = sip.example.com
altNames = sip.example.com, conf01.example.com, conf02.example.com
```

For more information about creating certificate signing requests, see [Certificate creation and requirements](#).

To assign a server certificate and private key to one or more Conferencing Nodes:

1. From the Management Node, go to **Platform Configuration > TLS Certificates** and select **Add TLS certificate**.
 2. Copy-paste the **TLS certificate** and its associated **Private key** into the relevant text boxes, or alternatively use the **select the file** links to upload the certificate and private key files.
 3. In the **Nodes** section, from the **Available Nodes** list, select every Conferencing Node referenced by the **_sipfederationtls._tcp** SRV record (e.g. **conf01.example.com** and **conf02.example.com** in our example), or every node within the public DMZ if outbound calling support is required, and move them into the **Chosen Nodes** list.
 4. Select **Save**. The certificate and private key will be pushed automatically to the selected Conferencing Nodes.
-  If the server certificate has been issued by one or more intermediate CAs (Certificate Authorities), these intermediate certificates must be uploaded. You can upload them as a single-file bundle by going to **Platform Configuration > Trusted CA Certificates** and selecting **Import**.

Configuring the SIP TLS FQDN setting for the Conferencing Nodes

After the certificates have been uploaded to the Conferencing Nodes, the SIP TLS FQDN setting for each node should be configured to reflect its unique DNS FQDN. This is done on the Management Node, by going to **Platform Configuration > Conferencing Nodes**, choosing each Conferencing Node in turn and populating the **SIP TLS FQDN** field:

SIP TLS FQDN	<input type="text" value="conf01.example.com"/>
<small>(Required for Conferencing Nodes that are involved in signalling of calls to and from Lync / Skype for Business servers.) An identity for this Conferencing Node, used in signaling SIP TLS Contact addresses. For more information, see SIP TLS FQDN. Maximum length: 255 characters.</small>	

The example above shows that the **SIP TLS FQDN** for the **conf01.example.com** Conferencing Node has been set to **conf01.example.com**. This FQDN has to match one of the Subject Alternative Names in the certificate installed on the Conferencing Node. You must do this for each Conferencing Node that supports inbound calling (those that are referenced by the sip.example.com round-robin DNS A-records, which in our example also includes the **conf02.example.com** Conferencing Node).

If outbound calling support is required, you must do this for every Conferencing Node within the public DMZ.

Configuring the Pexip Infinity domain

You must specify the name of the SIP domain that is routed from Lync/SfB to Pexip Infinity for this deployment. This domain is inserted into the From header in outbound calls from Pexip Infinity to Lync/SfB, and ensures that Lync/SfB can route messages back to Pexip Infinity when, for example, initiating content sharing.

You specify this by going to **Platform Configuration > Global Settings** and configuring the **Pexip Infinity domain (for Lync / Skype for Business integration)** setting:

Pexip Infinity domain (for Lync / Skype for Business integration)	<input type="text" value="example.com"/>
<small>The name of the SIP domain that is routed from Microsoft Lync / Skype for Business to Pexip Infinity, either as a static route or via federation. You can also configure a per-location override. Maximum length: 255 characters.</small>	

Typically this will be set to the same SIP domain as used elsewhere in the deployment, which is **example.com** in this case. Note that if you are using the same main domain as Office365 for your Pexip deployment, and therefore [using a subdomain for your Pexip environment](#), this should be the subdomain, e.g. **vc.example.com**.

Creating a Lync / Skype for Business federation DNS SRV record for your domain and its associated A-records

To ensure that calls from remote Lync/SfB environments towards the domain **example.com** are routed to our Conferencing Node, the following DNS SRV record must be created:

_sipfederationtls._tcp.<domain> where **<domain>** in our case is **example.com**, resulting in the DNS SRV record **_sipfederationtls._tcp.example.com**.

The DNS SRV record should:

- point to the DNS A-records that refer to our Conferencing Nodes (in our case using the hostname **sip.example.com**)
- have the port set to **5061** (required value)
- have a priority of **1** (recommended value)
- have a weight of **100** (recommended value)

Note that the domain name used in the SRV record has to match the domain in the corresponding A-record. This is required due to the trust model for Lync/SfB federation. Using our example:

- **_sipfederationtls._tcp.example.com** must use the same domain as **sip.example.com**
- you cannot, for example, configure the **_sipfederationtls._tcp.example.com** SRV record to point to **sip.video.example.com** or **conf01.otherdomain.com**.

The following illustration show how the SRV record would look in Microsoft DNS Manager. (This is for illustration purposes only – the actual video DNS domain may be managed through other DNS providers.)

DNS A-records

DNS A-records must exist for the hostname specified in the _sipfederationtls._tcp SRV record (which is **sip.example.com** in our case).

This could be a single record, or as in our example, where for resiliency and capacity purposes we have 2 Conferencing Nodes configured to receive incoming Lync/SfB calls from federated peers, we have 2 round-robin DNS A-records for the sip.example.com hostname:

Hostname	Host IP address
sip.example.com.	198.51.100.40
sip.example.com.	198.51.100.41

Even if you only intend initially to use a single Conferencing Node to receive incoming Lync/SfB calls, this approach allows you to easily add more nodes in the future. (In your actual deployment, both the **Hostname** and **Host IP address** should be changed to use the real name of your domain i.e. sip.<your_domain> and the IP addresses of your Conferencing Nodes.)

Note that these A-records specified above for sip.example.com are required in addition to the "standard" A-records that will exist for each Conferencing Node based on their individual hostnames and resolve to the same IP addresses, for example:

Hostname	Host IP address
conf01.example.com.	198.51.100.40
conf02.example.com.	198.51.100.41

(Again, the **Hostname** and **Host IP address** should reflect the real names and addresses of your Conferencing Nodes.)

The IP address must be the public address of the Conferencing Node if it is located behind a NAT.

With the DNS SRV record and A-records created correctly, calls from remote Lync/SfB environments towards the **example.com** domain will now be routed to **sip.example.com** and resolve to your Conferencing Nodes, allowing any remote Lync/SfB environment to call into the Pexip Infinity environment.

The Pexip Infinity environment is now ready to accept incoming calls from any remote Lync/SfB environment.

Note that:

- The remote Lync/SfB environment must be configured to allow Lync/SfB federation towards the **example.com** domain.
- To make an outbound call to another Lync/SfB user in a remote Lync/SfB environment, a **_sipfederationtls._tcp.<remote_domain>** record for that remote domain must exist. Even though you (as the administrator for your own domain) will not have any authority over the DNS records for that <remote_domain> — and are not responsible for creating them — you should check that such records exist when troubleshooting any outbound calling issues.

Ensuring that Lync / Skype for Business servers are not associated with a location

To ensure that each Conferencing Node uses DNS to locate an appropriate Lync/SfB system via which to route outbound calls, you must ensure that each Pexip Infinity location is not configured to route calls to a specific Lync/SfB server.

1. Go to **Platform Configuration > Locations**.
2. Select each location in turn and ensure that nothing is selected in the **Lync / Skype for Business server** field.


It should now be possible to send and receive calls between Pexip Infinity Conferencing Nodes and federated Lync/SfB clients.

Adding additional Conferencing Nodes for extra media capacity

If you add an extra Conferencing Node in the public DMZ to provide extra media capacity, you must:

- Update the single SAN certificate used on every existing Conferencing Node, as well as the new node, to include in the altNames section the hostname of the new node e.g. conf03.example.com.
- Configure the new Conferencing Node's **SIP TLS FQDN** setting to reflect its DNS FQDN e.g. conf03.example.com.
- Add a DNS A-record for the new hostname e.g.

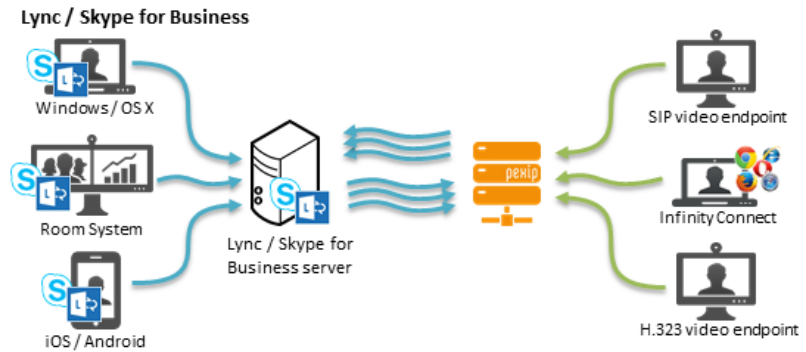
```
conf03.example.com.      86400 IN A 198.51.100.42
```

-  It is not necessary to create a new sip.<domain> round robin DNS A-record for every new Conferencing Node. Only do this if you want the new Conferencing Node to handle incoming call signaling. In general we recommend a maximum of 2 or 3 Conferencing Nodes to handle the incoming signaling.

Configuring Pexip Infinity as a Lync / Skype for Business gateway

Pexip Infinity can act as a gateway between Lync / Skype for Business and standards-based endpoints. This enables Lync/SfB clients to:

- invite H.323/SIP endpoints and registered Infinity Connect clients into a Lync meeting
- use the Pexip Distributed Gateway service to route incoming calls directly into an ad hoc or scheduled Lync meeting
- when dialed into a Pexip VMR conference, invite other Lync/SfB or external contacts into that same Pexip VMR (this creates a new Lync meeting which is merged with the existing Pexip VMR)
- receive and initiate person-to-person calls with standards-based devices.



Using the Pexip Distributed Gateway service

The Pexip Distributed Gateway is configured as a series of Call Routing Rules that specify which calls should be interworked and to where.

Incoming calls received by Pexip Infinity are routed as follows:

1. Pexip Infinity receives an incoming call via one of its Conferencing Nodes.
2. It checks whether the destination alias belongs to a Pexip Infinity Virtual Meeting Room, Virtual Auditorium, Virtual Reception or Test Call Service; if so, it directs the call to that service.
3. If the alias does not belong to any of the above services, Pexip Infinity checks the Call Routing Rules to see if the alias matches any rules specified there for incoming calls. If so, it places an outgoing call to the destination alias according to the rule's call target settings (which protocol and call control system to use, whether to route to registered devices only, etc).

This means that if an alias matches both a Virtual Meeting Room and a Call Routing Rule, the former will always take precedence and the call will be routed to the Virtual Meeting Room. You must therefore ensure that any regular expressions used in a Call Routing Rule do not unintentionally overlap with any aliases used by Virtual Meeting Rooms, Virtual Auditoriums, Virtual Receptions or Test Call Services.

If you configure your Pexip Distributed Gateway to support all of the Lync/SfB scenarios described here, you will have Call Routing Rules similar to those shown below:

Select Call Routing Rule to change

Action: 0 of 3 selected

Priority	Name	Description	Incoming	Outgoing	Call location	Registered only	Connect	SIP	Lync/SfB	H.323	Destination alias match	Replace string	Call target	Out location	Protocol	Enabled
40	Route calls from Lync / Skype for Business		✓	✗	Any Location	✗	✗	✗	✓	✗	.*@vc.example.com		Registered device or external system	Automatic	SIP	True
50	Route calls to Lync meeting		✓	✗	Any Location	✗	✓	✓	✗	✗	88\d(5,6)@example.com	\1	Lync/SfB meeting direct (not via Virtual Reception)	Automatic	Lync/SfB (MS-SIP)	True
60	Route to Lync / Skype for Business clients		✓	✗	Any Location	✗	✓	✓	✗	✗	.*@example.com		Lync/SfB clients or meetings, via a Virtual Reception	Automatic	Lync/SfB (MS-SIP)	True

Example routing rules

Configuring rules to allow Lync / Skype for Business to dial out to other devices via the gateway

You can configure a Call Routing Rule that enables Lync/SfB clients to initiate point-to-point calls with standards-based devices, and to invite other endpoints into a Lync meeting.

To configure the rule:

1. Go to **Service Configuration > Call Routing** and select **Add Call Routing Rule**.
2. Configure the following fields (leave all other fields with default values or as required for your specific deployment):


Option	Description
Name	The name you will use to refer to this rule.
Priority	Assign the priority for this rule.
Incoming gateway calls	Ensure this option is selected.
Outgoing calls from a conference	Leave unselected.
Match Infinity Connect (WebRTC / RTMP)	Select Match Lync / Skype for Business (MS-SIP) and leave the other protocols unselected. (This rule is only handling call requests received from the Lync/SfB environment.)
Match SIP	
Match Lync / Skype for Business (MS-SIP)	
Match H.323	
Match against full alias URI	Leave unselected.
Destination alias regex match	Enter a regular expression that will match the calls received from the Lync/SfB environment. For example, to match any alias in the vc.example.com domain: <code>.*@vc.example.com</code>
Destination alias regex replace string	If required, enter the regular expression string to transform the originally dialed (matched) alias into the alias to use to place the outbound call. If you do not need to change the alias, leave this field blank.
Call target	Select either <i>Registered device or external system</i> or <i>Registered devices only</i> , depending upon your requirements.
Protocol	The protocol used to place the outgoing call. This will be either <i>SIP</i> or <i>H.323</i> . If you want to place the call over both <i>SIP</i> and <i>H.323</i> , you will need to create 2 rules, one per protocol. Note that if the call is being placed to a registered device, such as an Infinity Connect desktop client, Pexip Infinity will always use the protocol that the device used to make the registration.
SIP Proxy	You can optionally specify the SIP Proxy to use to place an outgoing SIP call.
H.323 Gatekeeper	You can optionally specify the H.323 Gatekeeper to use to place an outgoing H.323 call.

3. Select **Save**.

Add Call Routing Rule

Name	<input type="text" value="Route calls from Lync / Skype for Business"/> *
The name used to refer to this Call Routing Rule. Maximum length: 250 characters.	
Service tag	<input type="text"/>
A unique identifier used to track usage of this Call Routing Rule. For more information, see Tracking usage with a service tag . Maximum length: 250 characters.	
Description	<input type="text"/>
A description of the Call Routing Rule. Maximum length: 250 characters.	
Priority	<input type="text" value="40"/> *
The priority of this rule. Rules are checked in ascending priority order until the first matching rule is found, and it is then applied. Range: 1 to 200.	

Use this rule for...

Incoming gateway calls	<input checked="" type="checkbox"/>	Applies this rule to incoming calls that have not been routed to a Virtual Meeting Room or Virtual Reception, and should be routed via the Pexip Distributed Gateway service .
Outgoing calls from a conference	<input type="checkbox"/>	Applies this rule to outgoing calls placed from a conference service (e.g. when adding a participant to a Virtual Meeting Room) where Automatic routing has been selected. For more information see Configuring Call Routing Rules .
Calls being handled in location	<input type="text" value="Any Location"/> 	Applies the rule only if the incoming call is being handled by a Conferencing Node in the selected location or the outgoing call is being initiated from the selected location. To apply the rule regardless of the location, select Any Location .

When matching Incoming Gateway calls...

Match incoming calls from registered devices only	<input type="checkbox"/>	Only apply this rule to incoming calls from devices, videoconferencing endpoints, soft clients or Infinity Connect clients that are registered to Pexip Infinity. Note that the call must also match one of the selected protocols below. Calls placed from non-registered clients or devices, or from the Infinity Connect Web App will not be routed by this rule if it is enabled.
Match Infinity Connect (WebRTC / RTMP)	<input type="checkbox"/>	Select whether this rule should apply to incoming calls from Infinity Connect clients (WebRTC / RTMP).
Match SIP	<input type="checkbox"/>	Select whether this rule should apply to incoming SIP calls.
Match Lync / Skype for Business (MS-SIP)	<input checked="" type="checkbox"/>	Select whether this rule should apply to incoming Lync / Skype for Business (MS-SIP) calls.
Match H.323	<input type="checkbox"/>	Select whether this rule should apply to incoming H.323 calls.

Alias match and transform

Match against full alias URI	<input type="checkbox"/>	This setting is for advanced use cases and will not normally be required. By default, Pexip Infinity matches against a parsed version of the destination alias, i.e. it ignores the URI scheme, any other parameters, and any host IP addresses. So, if the original alias is "sip:alice@example.com;transport=tls" for example, then by default the rule will match against "alice@example.com". Select this option to match against the full, unparsed alias instead.
Destination alias regex match	<input type="text" value=".*@vc.example.com"/> *	The regular expression that the destination alias (the alias that was dialed) is checked against to see if this rule applies to this call. For help with using regexes, see Regular expression reference . Maximum length: 250 characters.
Destination alias regex replace string	<input type="text"/>	The regular expression string used to transform the originally dialed alias (if a match was found). Leave blank to leave the originally dialed alias unchanged. Maximum length: 250 characters.

Call media settings	
Maximum inbound call bandwidth (kbps)	<input type="text"/> This optional field allows you to limit the bandwidth of media being received by Pexip Infinity from each individual participant dialed in via this Call Routing Rule. For more information see Restricting call bandwidth . Range: 128 to 4096.
Maximum outbound call bandwidth (kbps)	<input type="text"/> This optional field allows you to limit the bandwidth of media being sent by Pexip Infinity to each individual participant dialed out from this Call Routing Rule. For more information see Restricting call bandwidth . Range: 128 to 4096.
Call capability	<div> <input type="text" value="Main video + presentation"/> * </div> Maximum media content of the call. The participant being called will not be able to escalate beyond the selected capability. For more information see Controlling media capability .
Theme	<div> <input type="text" value="<use Default theme>"/> </div> The theme for use with this service. If no theme is selected here, files from the theme that has been selected as the default (Platform configuration > Global settings > Default theme) will be applied. For more information, see Customizing video and voice prompts using themes .

Outgoing call placement	
Call target	<div> <input type="text" value="Registered device or external system"/> * </div> The device or system to which the call is routed. The options are: Registered device or external system: routes the call to a matching registered device if it is currently registered, otherwise attempts to route the call via an external system such as a SIP proxy, Lync / Skype for Business server, H.323 gatekeeper or other gateway/ITSP. Registered devices only: routes the call to a matching registered device only (providing it is currently registered). Lync / Skype for Business meeting direct (not via Virtual Reception): routes the call via a Lync / Skype for Business server to a Lync / Skype for Business meeting. Note that the destination alias must be transformed into a Lync / Skype for Business Conference ID. Lync / Skype for Business clients, or meetings via a Virtual Reception: routes the call via a Lync / Skype for Business server either to a Lync / Skype for Business client, or - for calls that have come via a Virtual Reception - to a Lync / Skype for Business meeting. For Lync / Skype for Business meetings via Virtual Reception routing, ensure that Match against full alias URI is selected and that the Destination alias regex match ends with .*
Outgoing location	<div> <input type="text" value="Automatic"/> </div> When calling an external system, this forces the outgoing call to be handled by a Conferencing Node in a specific location. When calling a Lync / Skype for Business meeting, a Conferencing Node in this location will handle the outgoing call, and - for Lync / Skype for Business meeting direct targets - perform the Conference ID lookup on the Lync / Skype for Business server. Select Automatic to allow Pexip Infinity to automatically select which Conferencing Node to use.
Protocol	<div> <input type="text" value="SIP"/> * </div> When calling an external system, this is the protocol to use when placing the outbound call. Note that if the call is to a registered device, Pexip Infinity will instead use the protocol that the device used to make the registration.
SIP proxy	<div> <input type="text" value="Use DNS"/> </div> When calling an external system, this is the SIP proxy to use for outbound SIP calls. For more information, see About H.323 gatekeepers and SIP proxies . Select Use DNS to try to use normal SIP resolution procedures to route the call.

Rule state	
Enable this rule	<input checked="" type="checkbox"/> Determines if the rule is enabled or not. Any disabled rules still appear in the rules list but are ignored. Use this setting to test configuration changes, or to temporarily disable specific rules.

Configuring rules to allow devices to call Lync / Skype for Business clients via the gateway

You can configure a Call Routing Rule that enables non-Lync/SfB devices, such as SIP and H.323 endpoints or Infinity Connect clients, to make point-to-point calls to Lync/SfB clients.

To configure the rule:

1. Go to **Service Configuration > Call Routing** and select **Add Call Routing Rule**.
2. Configure the following fields (leave all other fields with default values or as required for your specific deployment):


Option	Description
Name	The name you will use to refer to this rule.
Priority	Assign the priority for this rule.
Incoming gateway calls	Ensure this option is selected.
Outgoing calls from a conference	Leave unselected.
Match Infinity Connect (WebRTC / RTMP)	Select one or more of Match Infinity Connect (WebRTC / RTMP) , Match SIP and Match H.323 as appropriate.
Match SIP	(Do not select Match Lync / Skype for Business (MS-SIP) as this rule is only handling call requests received from outside the Lync/SfB environment.)
Match Lync (MS-SIP)	
Match H.323	
Match against full alias URI	Leave unselected.
Destination alias regex match	Enter a regular expression that will match the calls to be sent to the Lync/SfB environment. For example, to match any alias in the example.com domain: . + @example.com
Destination alias regex replace string	If required, enter the regular expression string to transform the originally dialed (matched) alias into the alias to use to place the Lync/SfB call. If you do not need to change the alias, leave this field blank.
Call target	Select Lync / Skype for Business clients, or meetings via a Virtual Reception (we want to route the calls to Lync/SfB clients via an external Lync/SfB server).
Outgoing location	If required, you can ensure that the outgoing call to Lync/SfB is handled by a Conferencing Node in a specific location. If an outgoing location is not specified, the call is placed from a Conferencing Node in the ingress location (the same location as the Conferencing Node that is handling the incoming call).
Lync / Skype for Business server	Select the Lync/SfB server that you want to use to handle the call, for example eu-lyncpool .

3. Select **Save**.

Add Call Routing Rule

Name	<input type="text" value="Route to Lync / Skype for Business clients"/> *
The name used to refer to this Call Routing Rule. Maximum length: 250 characters.	
Service tag	<input type="text"/>
A unique identifier used to track usage of this Call Routing Rule. For more information, see Tracking usage with a service tag . Maximum length: 250 characters.	
Description	<input type="text"/>
A description of the Call Routing Rule. Maximum length: 250 characters.	
Priority	<input type="text" value="60"/> *
The priority of this rule. Rules are checked in ascending priority order until the first matching rule is found, and it is then applied. Range: 1 to 200.	

Use this rule for...

Incoming gateway calls	<input checked="" type="checkbox"/>	Applies this rule to incoming calls that have not been routed to a Virtual Meeting Room or Virtual Reception, and should be routed via the Pexip Distributed Gateway service .
Outgoing calls from a conference	<input type="checkbox"/>	Applies this rule to outgoing calls placed from a conference service (e.g. when adding a participant to a Virtual Meeting Room) where Automatic routing has been selected. For more information see Configuring Call Routing Rules .
Calls being handled in location	<input type="text" value="Any Location"/> 	Applies the rule only if the incoming call is being handled by a Conferencing Node in the selected location or the outgoing call is being initiated from the selected location. To apply the rule regardless of the location, select Any Location .

When matching incoming Gateway calls...

Match incoming calls from registered devices only	<input type="checkbox"/>	Only apply this rule to incoming calls from devices, videoconferencing endpoints, soft clients or Infinity Connect clients that are registered to Pexip Infinity. Note that the call must also match one of the selected protocols below. Calls placed from non-registered clients or devices, or from the Infinity Connect Web App will not be routed by this rule if it is enabled.
Match Infinity Connect (WebRTC / RTMP)	<input checked="" type="checkbox"/>	Select whether this rule should apply to incoming calls from Infinity Connect clients (WebRTC / RTMP).
Match SIP	<input checked="" type="checkbox"/>	Select whether this rule should apply to incoming SIP calls.
Match Lync / Skype for Business (MS-SIP)	<input type="checkbox"/>	Select whether this rule should apply to incoming Lync / Skype for Business (MS-SIP) calls.
Match H.323	<input checked="" type="checkbox"/>	Select whether this rule should apply to incoming H.323 calls.

Alias match and transform

Match against full alias URI	<input type="checkbox"/>	This setting is for advanced use cases and will not normally be required. By default, Pexip Infinity matches against a parsed version of the destination alias, i.e. it ignores the URI scheme, any other parameters, and any host IP addresses. So, if the original alias is "sip:alice@example.com;transport=tls" for example, then by default the rule will match against "alice@example.com". Select this option to match against the full, unparsed alias instead.
Destination alias regex match	<input type="text" value=".*@example.com"/> *	The regular expression that the destination alias (the alias that was dialed) is checked against to see if this rule applies to this call. For help with using regexes, see Regular expression reference . Maximum length: 250 characters.
Destination alias regex replace string	<input type="text"/>	The regular expression string used to transform the originally dialed alias (if a match was found). Leave blank to leave the originally dialed alias unchanged. Maximum length: 250 characters.

Call media settings	
Maximum inbound call bandwidth (kbps)	<input type="text"/> <p>This optional field allows you to limit the bandwidth of media being received by Pexip Infinity from each individual participant dialed in via this Call Routing Rule. For more information see Restricting call bandwidth. Range: 128 to 4096.</p>
Maximum outbound call bandwidth (kbps)	<input type="text"/> <p>This optional field allows you to limit the bandwidth of media being sent by Pexip Infinity to each individual participant dialed out from this Call Routing Rule. For more information see Restricting call bandwidth. Range: 128 to 4096.</p>
Call capability	<div> Main video + presentation ▼ * </div> <p>Maximum media content of the call. The participant being called will not be able to escalate beyond the selected capability. For more information see Controlling media capability.</p>
Theme	<div> <use Default theme> ▼ ✎ + </div> <p>The theme for use with this service. If no theme is selected here, files from the theme that has been selected as the default (Platform configuration > Global settings > Default theme) will be applied. For more information, see Customizing video and voice prompts using themes.</p>

Outgoing call placement	
Call target	<div> Lync / Skype for Business clients, or meetings via a Virtual Reception ▼ * </div> <p>The device or system to which the call is routed. The options are: Registered device or external system: routes the call to a matching registered device if it is currently registered, otherwise attempts to route the call via an external system such as a SIP proxy, Lync / Skype for Business server, H.323 gatekeeper or other gateway/ITSP. Registered devices only: routes the call to a matching registered device only (providing it is currently registered). Lync / Skype for Business meeting direct (not via Virtual Reception): routes the call via a Lync / Skype for Business server to a Lync / Skype for Business meeting. Note that the destination alias must be transformed into a Lync / Skype for Business Conference ID. Lync / Skype for Business clients, or meetings via a Virtual Reception: routes the call via a Lync / Skype for Business server either to a Lync / Skype for Business client, or - for calls that have come via a Virtual Reception - to a Lync / Skype for Business meeting. For Lync / Skype for Business meetings via Virtual Reception routing, ensure that Match against full alias URI is selected and that the Destination alias regex match ends with .*</p>
Outgoing location	<div> Automatic ▼ ✎ + </div> <p>When calling an external system, this forces the outgoing call to be handled by a Conferencing Node in a specific location. When calling a Lync / Skype for Business meeting, a Conferencing Node in this location will handle the outgoing call, and - for Lync / Skype for Business meeting direct targets - perform the Conference ID lookup on the Lync / Skype for Business server. Select Automatic to allow Pexip Infinity to automatically select which Conferencing Node to use.</p>
Lync / Skype for Business server	<div> eu-lyncpool ▼ ✎ + </div> <p>When calling an external system, this is the Lync / Skype for Business server to use for outbound Lync / Skype for Business (MS-SIP) calls. Select Use DNS to try to use normal Lync / Skype for Business (MS-SIP) resolution procedures to route the call. When calling a Lync / Skype for Business meeting, this is the Lync / Skype for Business server to use for the Conference ID lookup and to place the call. For more information, see About Lync / Skype for Business servers.</p>
TURN server	<div> ----- ▼ ✎ + </div> <p>The TURN server to be used for outbound Lync / Skype for Business (MS-SIP) calls (where applicable). For more information, see About TURN servers.</p>
STUN server	<div> ----- ▼ ✎ + </div> <p>The STUN server to be used for outbound Lync / Skype for Business (MS-SIP) calls (where applicable).</p>

Rule state	
Enable this rule	<input checked="" type="checkbox"/> <p>Determines if the rule is enabled or not. Any disabled rules still appear in the rules list but are ignored. Use this setting to test configuration changes, or to temporarily disable specific rules.</p>

Configuring rules to use Pexip Infinity as a Lync/SfB gateway into Lync meetings

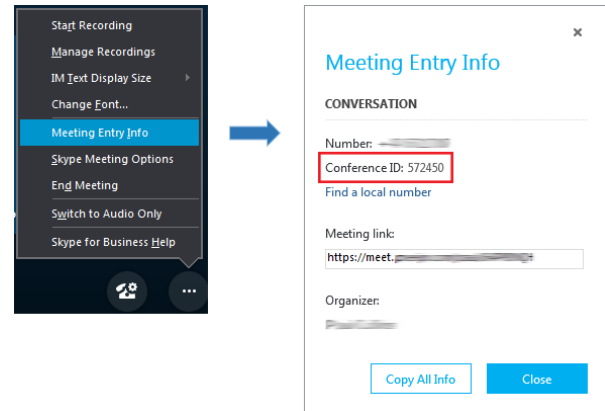
In addition to Pexip Infinity acting as a point-to-point gateway between non-Lync/SfB devices, such as SIP and H.323 endpoints or Infinity Connect clients, and Lync/SfB clients, you can also configure the Pexip Distributed Gateway such that it can route calls from those external devices directly into ad hoc or scheduled Lync meetings.

All calls are routed into the Lync meetings by means of the Lync/SfB Conference ID that is associated with the Lync meeting. The Lync/SfB Conference ID is typically a 5 or 6 digit number. For scheduled meetings it will normally be included in the meeting invitation.

For ad hoc conferences, existing Lync/SfB participants in the conference can find the Conference ID by selecting the **Meeting Entry Info** option (see picture).

There are two ways you can configure these gateway calls within Pexip Infinity:

- **Routing indirectly via a Virtual Reception:** here you configure Pexip Infinity to act as a Lync/SfB IVR gateway or "lobby" by configuring a Virtual Reception to capture the Conference ID of the required conference, and then use a Call Routing Rule to route the call into the Lync meeting.
- **Routing directly via the Pexip Distributed Gateway:** here you use a single Call Routing Rule to route incoming calls for specific alias patterns — that will typically include the Conference ID — directly into the relevant Lync meetings.



You can use either or both of these two methods, depending upon your requirements. The configuration required for these methods is explained below (see [Routing indirectly via a Virtual Reception \(IVR gateway\)](#) and [Routing directly via the Pexip Distributed Gateway](#)). Also included are some guidelines for [Lync/SfB configuration to use Pexip Infinity as a Lync/SfB gateway](#).

Note that:

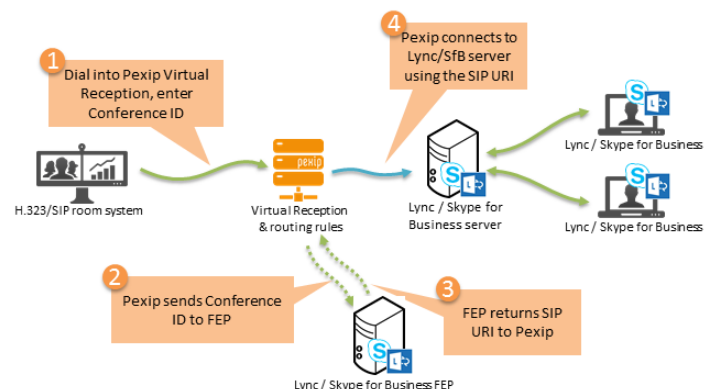
- The Lync/SfB gateway features are only supported within on-prem Lync/SfB deployments, as the Conferencing Nodes must be trusted applications within the Lync/SfB environment.
- Non-Lync/SfB video callers will see a holding screen until a Lync/SfB client joins the conference with video.

Routing indirectly via a Virtual Reception (IVR gateway)

To route calls to Lync meetings via a Virtual Reception (IVR gateway) you need:

- A Virtual Reception configured specifically to handle Lync meetings.
- A Call Routing Rule to route the calls handled by the Virtual Reception into the relevant Lync meeting (typically you will adapt your existing rule configured above that routes point-to-point calls to Lync/SfB clients).

The Virtual Reception requests the caller to enter the Lync/SfB Conference ID (typically a 5 or 6 digit number) which it then uses to retrieve the full conference URI from the Lync/SfB server. The Pexip Distributed Gateway then matches this conference URI and routes the caller to the appropriate Lync meeting.





To configure the Virtual Reception:

1. Go to **Service Configuration > Virtual Receptions** and select **Add Virtual Reception**.
2. Configure the following fields (leave all other fields with default values or as required for your specific deployment):

Option	Description
Name	The name you will use to refer to this Virtual Reception, for example "Lync IVR gateway".
Theme	Optionally, you may want to assign a specific theme to this Virtual Reception to brand it as the gateway to Lync/SfB conferences, for example by customizing the voice prompts.
Lync / Skype for Business server (in the Advanced options)	Select the Lync/SfB server that you want to use to resolve the Lync/SfB Conference ID, for example <i>eu-lyncpool</i> .
Lync / Skype for Business meeting lookup location	You can optionally specify the system location that will perform the Lync/SfB Conference ID lookup on the Lync/SfB server. If a location is not selected, the IVR ingress node will perform the lookup. This can assist in scenarios where an external device connects to a Virtual Reception via a Conferencing Node in the DMZ and that node is not trusted by the Lync/SfB FEP. This allows you to nominate the location (in which the Conferencing Nodes are trusted by Lync/SfB) to perform the lookup.
Alias	Enter the alias that users will dial to use this Lync/SfB gateway Virtual Reception, for example <i>lync.lobby@example.com</i> .

3. Select **Save**.

Add Virtual Reception

Name	<input type="text" value="Lync/Skype for Business IVR gateway"/> *
The name used to refer to this Virtual Reception. Maximum length: 250 characters.	
Description	<input type="text"/>
A description of the Virtual Reception. Maximum length: 250 characters.	
Theme	<input type="text" value="<use Default theme>"/>  
The theme for use with this service. If no theme is selected here, files from the theme that has been selected as the default (Platform configuration > Global settings > Default theme) will be applied. For more information, see Customizing video and voice prompts using themes .	

Advanced options (Hide)	
Destination alias regex match	<input type="text"/>
An optional regular expression used to match against the alias entered by the caller into the Virtual Reception. If the entered alias does not match the expression, the Virtual Reception will not route the call. If this field is left blank, any entered alias is permitted. For more information, see Restricting or transforming the aliases entered into a Virtual Reception . Maximum length: 250 characters.	
Destination alias regex replace string	<input type="text"/>
An optional regular expression used to transform the alias entered by the caller into the Virtual Reception. (Only applies if a regex match string is also configured and the entered alias matches that regex.) Leave this field blank if you do not want to change the alias entered by the caller. Maximum length: 250 characters.	
Maximum inbound call bandwidth (kbps)	<input type="text"/>
This optional field allows you to limit the bandwidth of media being received by Pexip Infinity from each individual participant dialed in to this Virtual Reception. For more information see Restricting call bandwidth . Range: 128 to 4096.	
Maximum outbound call bandwidth (kbps)	<input type="text"/>
This optional field allows you to limit the bandwidth of media being sent by Pexip Infinity to each individual participant dialed in to this Virtual Reception. For more information see Restricting call bandwidth . Range: 128 to 4096.	

Conference capabilities	<div> Main video + presentation </div> <p>Maximum media content of the conference. Participants will not be able to escalate beyond the selected capability. For more information see Controlling media capability.</p>
Service tag	<div> </div> <p>A unique identifier used to track usage of this Virtual Reception. For more information, see Tracking usage with a service tag. Maximum length: 250 characters.</p>
Lync / Skype for Business server	<div> eu-lyncpool </div> <p>Select a Lync / Skype for Business server only if this Virtual Reception is to act as an IVR gateway to scheduled and ad hoc Lync / Skype for Business meetings. You must then ensure that your Call Routing Rule that routes calls to your Lync / Skype for Business environment has Match against full alias URI selected and a Destination alias regex match in the style <code>*@example.com.*</code> For more information, see Pexip Infinity and Microsoft Lync / Skype for Business Deployment Guide.</p>
Lync / Skype for Business meeting lookup location	<div> </div> <p>If selected, a Conferencing Node in this system location will perform the Lync / Skype for Business Conference ID lookup on the Lync / Skype for Business server. If a location is not selected, the IVR ingress node will perform the lookup.</p>

Aliases

Alias: #1	
Alias:	<div> lync.lobby@example.com </div> <p>The dial string used to join this service, in the form that it will be received by Pexip Infinity. This alias must include any domain that is automatically added by the participant's endpoint or call control system, or dialed by the participant. For more information, see About aliases. Maximum length: 250 characters.</p>
Description:	<div> </div> <p>An optional description of the alias. Maximum length: 250 characters.</p>
Add another Alias	
<div> <div>Save</div> <div>Save and add another</div> <div>?</div> </div>	

To configure the Call Routing Rule:

- Go to **Service Configuration > Call Routing**.
- Select the existing Call Routing Rule that currently routes calls to your Lync/SfB clients (as configured in [Configuring rules to allow devices to call Lync / Skype for Business clients via the gateway](#) above).
- Modify the following fields (leave all other fields unchanged):

Option	Description
Match against full alias URI	Select this option. (The alias of the Lync/SfB conference contains various parameters that must not be stripped away.)
Destination alias regex match	Amend the regular expression to also match against aliases that contain parameters after the domain portion, for example: <code>*@example.com.*</code>

Note that this rule will still continue to support the routing of point-to-point calls to Lync/SfB clients. This modification just enhances the scope of the rule to also include routing to Lync/SfB Lync meetings.

- Select **Save**.

Match against full alias URI	<input checked="" type="checkbox"/> <p>This setting is for advanced use cases and will not normally be required. By default, Pexip Infinity matches against a parsed version of the destination alias, i.e. it ignores the URI scheme, any other parameters, and any host IP addresses. So, if the original alias is "sip:alice@example.com;transport=tls" for example, then by default the rule will match against "alice@example.com". Select this option to match against the full, unparsed alias instead.</p>
Destination alias regex match	<div> .*@example.com.* </div> <p>The regular expression that the destination alias (the alias that was dialed) is checked against to see if this rule applies to this call. Maximum length: 250 characters.</p>

Using the Lync/SfB IVR gateway service

After the Virtual Reception and Call Routing Rule have been configured, non-Lync/SfB users can now dial the alias of the Virtual Reception (e.g. `lync.lobby@example.com`) and then, when prompted by the IVR service, enter the Lync/SfB Conference ID of the conference they want to join.

The Pexip Distributed Gateway will then route the call into the appropriate Lync/SfB conference.

Note that:

- SIP and H.323 endpoints can bypass having to enter the destination alias via DTMF tones. They would do this by including the Lync/SfB Conference ID in their dial string when dialing the Virtual Reception. The dial string should be in the format: `<reception_alias>*<conference_id>@<domain>`.

For example, if the alias of the Virtual Reception is `lync.lobby@example.com` and the Lync/SfB Conference ID is `572450`, then the endpoint can dial `lync.lobby**572450@example.com` to be transferred directly into the Lync/SfB conference.

- Infinity Connect Web App users can also be provided with a preconfigured link URL that, when clicked, will automatically provide the Lync/SfB Conference ID to the Virtual Reception and take the user directly into the Lync/SfB conference. The URL needs to be in the format:

`https://<address>/webapp/?conference=<reception_alias>&name=<name>&join=1&extension=<Conference ID>`

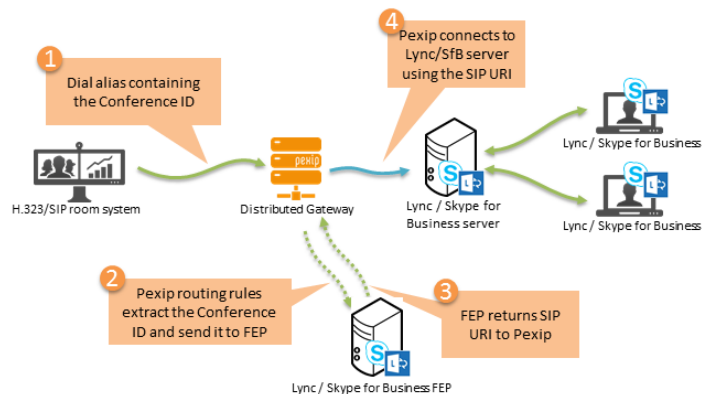
for example

`https://node.example.com/webapp/?conference=lync.lobby@example.com&name=Alice&join=1&extension=572450`

Routing directly via the Pexip Distributed Gateway

To route calls to Lync meetings directly via the Pexip Distributed Gateway you need:

- To decide on an alias pattern that participants will dial to access the Lync meetings. The alias pattern will typically include the Lync/SfB Conference ID, for example the pattern could be: `88<ConferenceID>@example.com` i.e. a prefix of 88 followed by the Conference ID, and thus the participant would dial `8812345@example.com` to access a Lync meeting with a Conference ID of 12345.
- A Call Routing Rule that matches that alias pattern and transforms it such that it contains just the Lync/SfB Conference ID which it can then pass on to the target Lync/SfB server.



To configure the rule:



- Go to **Service Configuration > Call Routing** and select **Add Call Routing Rule**.
- Configure the following fields (leave all other fields with default values or as required for your specific deployment):

Option	Description
Name	The name you will use to refer to this rule.
Priority	Assign the priority for this rule.
Incoming gateway calls	Ensure this option is selected.
Outgoing calls from a conference	Leave unselected.

Option	Description
Match Infinity Connect (WebRTC / RTMP) Match SIP Match Lync / Skype for Business (MS-SIP) Match H.323	Select one or more of Match Infinity Connect (WebRTC / RTMP) , Match SIP and Match H.323 as appropriate. (Do not select Match Lync / Skype for Business (MS-SIP) as this rule is only handling call requests received from outside the Lync/SfB environment.)
Match against full alias URI	Leave unselected.
Destination alias regex match	Enter a regular expression that matches the calls to be sent to the Lync meeting. For example, to match any alias in the style of 88<ConferenceID>@example.com you could use: 88(\d{5,6})@example\.com Note that \d{5,6} which matches the numeric 5-6 digit Conference ID, is enclosed in a () group.
Destination alias regex replace string	This must transform the dialed alias so that it only contains the Conference ID. In our example, to extract the Conference ID from the dialed alias we would use: \1 which replaces the originally dialed alias with just the Conference ID group from the regex match field.
Call target	Select Lync / Skype for Business meeting direct (not via Virtual Reception) . This type of call target is specifically designed to take the Conference ID (that we extracted via the regex strings) and send it to the nominated Lync/SfB server so that the call can be routed into the Lync/SfB meeting.
Outgoing location	If required, you can ensure that the outgoing call to Lync/SfB is handled by a Conferencing Node in a specific location. If an outgoing location is not specified, the call is placed from a Conferencing Node in the ingress location (the same location as the Conferencing Node that is handling the incoming call).
Lync / Skype for Business server	Select the Lync/SfB server that you want to use to perform the Conference ID lookup and to handle the call, for example <i>eu-lyncpool</i> .

Add Call Routing Rule

Name	<input type="text" value="Route calls to Lync meeting"/> *
The name used to refer to this Call Routing Rule. Maximum length: 250 characters.	
Service tag	<input type="text"/>
A unique identifier used to track usage of this Call Routing Rule. For more information, see Tracking usage with a service tag . Maximum length: 250 characters.	
Description	<input type="text"/>
A description of the Call Routing Rule. Maximum length: 250 characters.	
Priority	<input type="text" value="50"/> *
The priority of this rule. Rules are checked in ascending priority order until the first matching rule is found, and it is then applied. Range: 1 to 200.	

Use this rule for...	
Incoming gateway calls	<input checked="" type="checkbox"/> Applies this rule to incoming calls that have not been routed to a Virtual Meeting Room or Virtual Reception, and should be routed via the Pexip Distributed Gateway service .
Outgoing calls from a conference	<input type="checkbox"/> Applies this rule to outgoing calls placed from a conference service (e.g. when adding a participant to a Virtual Meeting Room) where Automatic routing has been selected. For more information see Configuring Call Routing Rules .
Calls being handled in location	<input type="text" value="Any Location"/>   Applies the rule only if the incoming call is being handled by a Conferencing Node in the selected location or the outgoing call is being initiated from the selected location. To apply the rule regardless of the location, select Any Location .

When matching incoming Gateway calls...	
Match incoming calls from registered devices only	<input type="checkbox"/> Only apply this rule to incoming calls from devices, videoconferencing endpoints, soft clients or Infinity Connect clients that are registered to Pexip Infinity. Note that the call must also match one of the selected protocols below. Calls placed from non-registered clients or devices, or from the Infinity Connect Web App will not be routed by this rule if it is enabled.
Match Infinity Connect (WebRTC / RTMP)	<input checked="" type="checkbox"/> Select whether this rule should apply to incoming calls from Infinity Connect clients (WebRTC / RTMP).
Match SIP	<input checked="" type="checkbox"/> Select whether this rule should apply to incoming SIP calls.
Match Lync / Skype for Business (MS-SIP)	<input type="checkbox"/> Select whether this rule should apply to incoming Lync / Skype for Business (MS-SIP) calls.
Match H.323	<input checked="" type="checkbox"/> Select whether this rule should apply to incoming H.323 calls.

Alias match and transform	
Match against full alias URI	<input type="checkbox"/> This setting is for advanced use cases and will not normally be required. By default, Pexip Infinity matches against a parsed version of the destination alias, i.e. it ignores the URI scheme, any other parameters, and any host IP addresses. So, if the original alias is "sip:alice@example.com;transport=tls" for example, then by default the rule will match against "alice@example.com". Select this option to match against the full, unparsed alias instead.
Destination alias regex match	<input type="text" value="88(\d{5,6})@example\,com"/> * The regular expression that the destination alias (the alias that was dialed) is checked against to see if this rule applies to this call. For help with using regexes, see Regular expression reference . Maximum length: 250 characters.
Destination alias regex replace string	<input type="text" value="\1"/> The regular expression string used to transform the originally dialed alias (if a match was found). Leave blank to leave the originally dialed alias unchanged. Maximum length: 250 characters.

Call media settings	
Maximum inbound call bandwidth (kbps)	<input type="text"/> <p>This optional field allows you to limit the bandwidth of media being received by Pexip Infinity from each individual participant dialed in via this Call Routing Rule. For more information see Restricting call bandwidth. Range: 128 to 4096.</p>
Maximum outbound call bandwidth (kbps)	<input type="text"/> <p>This optional field allows you to limit the bandwidth of media being sent by Pexip Infinity to each individual participant dialed out from this Call Routing Rule. For more information see Restricting call bandwidth. Range: 128 to 4096.</p>
Call capability	<div> Main video + presentation ▼ * </div> <p>Maximum media content of the call. The participant being called will not be able to escalate beyond the selected capability. For more information see Controlling media capability.</p>
Theme	<div> <use Default theme> ▼ ✎ + </div> <p>The theme for use with this service. If no theme is selected here, files from the theme that has been selected as the default (Platform configuration > Global settings > Default theme) will be applied. For more information, see Customizing video and voice prompts using themes.</p>

Outgoing call placement	
Call target	<div> Lync / Skype for Business meeting direct (not via Virtual Reception) ▼ * </div> <p>The device or system to which the call is routed. The options are: Registered device or external system: routes the call to a matching registered device if it is currently registered, otherwise attempts to route the call via an external system such as a SIP proxy, Lync / Skype for Business server, H.323 gatekeeper or other gateway/ITSP. Registered devices only: routes the call to a matching registered device only (providing it is currently registered). Lync / Skype for Business meeting direct (not via Virtual Reception): routes the call via a Lync / Skype for Business server to a Lync / Skype for Business meeting. Note that the destination alias must be transformed into a Lync / Skype for Business Conference ID. Lync / Skype for Business clients, or meetings via a Virtual Reception: routes the call via a Lync / Skype for Business server either to a Lync / Skype for Business client, or - for calls that have come via a Virtual Reception - to a Lync / Skype for Business meeting. For Lync / Skype for Business meetings via Virtual Reception routing, ensure that Match against full alias URI is selected and that the Destination alias regex match ends with .*</p>
Outgoing location	<div> Automatic ▼ ✎ + </div> <p>When calling an external system, this forces the outgoing call to be handled by a Conferencing Node in a specific location. When calling a Lync / Skype for Business meeting, a Conferencing Node in this location will handle the outgoing call, and - for Lync / Skype for Business meeting direct targets - perform the Conference ID lookup on the Lync / Skype for Business server. Select Automatic to allow Pexip Infinity to automatically select which Conferencing Node to use.</p>
Lync / Skype for Business server	<div> eu-lyncpool ▼ ✎ + </div> <p>When calling an external system, this is the Lync / Skype for Business server to use for outbound Lync / Skype for Business (MS-SIP) calls. Select Use DNS to try to use normal Lync / Skype for Business (MS-SIP) resolution procedures to route the call. When calling a Lync / Skype for Business meeting, this is the Lync / Skype for Business server to use for the Conference ID lookup and to place the call. For more information, see About Lync / Skype for Business servers.</p>
TURN server	<div> ----- ▼ ✎ + </div> <p>The TURN server to be used for outbound Lync / Skype for Business (MS-SIP) calls (where applicable). For more information, see About TURN servers.</p>
STUN server	<div> ----- ▼ ✎ + </div> <p>The STUN server to be used for outbound Lync / Skype for Business (MS-SIP) calls (where applicable).</p>

Rule state	
Enable this rule	<input checked="" type="checkbox"/> <p>Determines if the rule is enabled or not. Any disabled rules still appear in the rules list but are ignored. Use this setting to test configuration changes, or to temporarily disable specific rules.</p>

Using the direct Lync/SfB gateway service

After the Call Routing Rule has been configured, non-Lync/SfB users can now dial an alias that matches your specified pattern (e.g. **8812345@example.com**) to be routed directly into the appropriate Lync meeting (in this example the Lync meeting with a Conference ID of 12345).

Lync/SfB configuration to use Pexip Infinity as a Lync/SfB gateway

Ensuring that Lync/SfB is configured with a dial-in access number

To ensure that a numeric Lync/SfB Conference ID is generated, your Lync/SfB environment must be configured with a conferencing dial-in access number.

For information about configuring this via Lync's administrative tools in Lync Server 2013, see <https://technet.microsoft.com/en-us/library/gg398126%28v=ocs.15%29.aspx>.

Waiting in Lync/SfB's meeting lobby

Participants joining the Lync meeting may also be held in a Lync / Skype for Business meeting lobby.

In Lync, you can select the **PSTN callers bypass lobby** option to allow phone participants to bypass the lobby. For information about configuring this setting in Lync Server 2013, see [https://technet.microsoft.com/en-us/library/jj721889\(v=ocs.15\).aspx](https://technet.microsoft.com/en-us/library/jj721889(v=ocs.15).aspx).

Custom footer for meeting invites

You may also want to add a custom footer to the meeting invites that are sent out for scheduled conferences, so that it includes the alias details for the Pexip Infinity Virtual Reception that users will need to call (and from where they will enter the Conference ID).

For more information about configuring meeting invitations in Lync Server 2013, see <https://technet.microsoft.com/en-us/library/gg398638.aspx>.

Trusting Conferencing Nodes

When calling into a Lync meeting, by default, the Lync/SfB Conference ID lookup is invoked from the ingress node (the same Conferencing Node that is handling the incoming call) and the call to Lync/SfB is placed from the ingress location (the same location as the Conferencing Node that is handling the incoming call). In both cases you can override the default behavior by specifying the location that will perform the Conference ID lookup and the location that will place the outbound call.

The nodes that perform the lookup and place the call must be trusted by the Front End Pool to ensure call success.

Ensuring each Conferencing Node's TLS FQDN is set (all gateway scenarios)

For any Pexip Infinity and Lync/SfB integration, you must ensure that each Conferencing Node is configured with its respective DNS hostname as the **SIP TLS FQDN**. Pexip Infinity will present this as being the server name, and it must match the name on the certificate installed on the node. Each Conferencing Node must have a unique **SIP TLS FQDN**.

This is done on the Management Node, by going to **Platform Configuration > Conferencing Nodes**, choosing each node in turn and populating the **SIP TLS FQDN** field.

SIP TLS FQDN	<input type="text" value="eu-px01.example.com"/>
<small>(Required for Conferencing Nodes that are involved in signalling of calls to and from Lync / Skype for Business servers.) An identity for this Conferencing Node, used in signaling SIP TLS Contact addresses. For more information, see SIP TLS FQDN. Maximum length: 255 characters.</small>	

The example above shows the **SIP TLS FQDN** for the eu-px01 Conferencing Node, which is set to **eu-px01.example.com**.

The SIP TLS FQDN must be set even if you are using a TCP connection to Lync/SfB.

Certificate creation and requirements


Pexip Infinity supports the use of Base64-encoded X.509 SSL/TLS certificates. Such certificates are used when integrating Pexip Infinity with Microsoft Lync and Skype for Business, either as part of an on-prem deployment or when deploying Pexip in a public DMZ for enabling direct federation with remote Lync/SfB environments.

For an on-prem integration between Lync/SfB and Pexip Infinity, it is common to use an internal/enterprise Certificate Authority (CA) for requesting and creating certificates. However, for a public DMZ deployment of Pexip Infinity, a certificate from a public TLS/SSL certificate vendor/CA such as for instance Verisign, Comodo or GlobalSign is required.

Creating a certificate signing request (CSR)

The on-prem and public DMZ Lync/SfB integration guidelines both recommend that the same single certificate is installed on all Conferencing Nodes. This provides support for redundant Conferencing Node deployments and multiple SIP domains for Lync/SfB federation. Therefore, the certificate created for the Conferencing Nodes will typically need to contain multiple SANs (Subject Alternative Names). This type of certificate is also known as a UC certificate.

While this means that this single certificate will potentially contain a relatively high number of names, the administrator only has to manage a single SAN certificate across all Conferencing Node (unless [multiple domain/subdomain](#) support is required).

 Wildcard TLS certificates are not supported in SIP or Microsoft Lync / Skype for Business environments (as per RFC 5922). If you are using SIP or Lync / Skype for Business, your Conferencing Nodes must not use wildcard TLS certificates.

You can use Pexip Infinity's inbuilt [Certificate Signing Request \(CSR\) generator](#) to assist in acquiring a server certificate from a Certificate Authority.

Public DMZ environment requirements

When requesting certificates for Conferencing Nodes for public DMZ deployments:

- the Subject name (commonName attribute) should be set to the hostname referenced by the _sipfederationtls._tcp SRV record
- Subject Alternative Name (altNames attribute) entries must be included for every individual node in the public DMZ (including the hostname referenced in the Subject name).

See [Assigning publicly-issued TLS server certificates to Conferencing Nodes](#) for more information and examples for a public DMZ deployment.

On-prem environment requirements

When requesting certificates for Conferencing Nodes for on-prem deployments:

- the Subject name (commonName attribute) must be the Trusted Application Pool FQDN
- Subject Alternative Name (altNames attribute) entries must be included for every node in the pool, plus the common application pool FQDN.

See [Assigning a server certificate to the Pexip Infinity Conferencing Nodes](#) for more information and examples for an on-prem deployment.

Comparison of public DMZ and on-prem examples

When using Pexip Infinity's inbuilt [CSR generator](#) the examples below show the entries that would be required to match our example public DMZ deployment, and our example on-premises deployment (for the Europe-located pool of Pexip nodes):

Field	Public DMZ environment	On-prem environment (Europe)
Subject name	<i>User-provided custom Common Name</i>	<i>User-provided custom Common Name</i>
Custom subject name	sip.example.com	eu-px.example.com

Field	Public DMZ environment	On-prem environment (Europe)
Subject alternative names	conf01.example.com, conf02.example.com (and sip.example.com will also be included automatically)	eu-px01.example.com, eu-px02.example.com, eu-px03.example.com (and eu-px.example.com will also be included automatically)

Adding additional nodes in the future

These SAN/UC certificates can normally be updated at any time (although usually for an additional fee) from most certificate vendors.

Thus, if for instance you need to add two additional nodes, you can create a new CSR containing the original altNames and the two additional altNames, submit the CSR to the certificate vendor, pay the additional fee (which is usually per SAN entry), get an updated SAN/UC certificate and then upload this new certificate to all nodes (the original certificate will be revoked and become unusable).

Assigning a certificate to a Conferencing Node

In Pexip Infinity, certificates are managed from the Pexip Infinity Administrator interface under **Platform Configuration > TLS Certificates**. You apply a certificate to a Conferencing Node by uploading the server certificate and associated private key and then assigning it to the Conferencing Nodes in question. The certificate should be in Base64-encoded X.509 (PEM) format.

The result of uploading and assigning our example public DMZ certificate and private key would look similar to this:

TLS Certificates

All certificates Certificates by Node							
Action:	-----	Go	0 of 9 selected	Enter search here	Search		
<input type="checkbox"/>	Subject name	Issuer name	Subject alternative names	Nodes	End date	Status	
<input type="checkbox"/>	pexip-manager.example.com	COMODO RSA		1	2016-10-05 00:59:59 (BST)	Good	
<input type="checkbox"/>	sip.example.com	COMODO RSA	DNS:sip.example.com, DNS:conf01.example.com, DNS:conf02.example.com	2	2036-09-07 01:49:31 (BST)	Good	

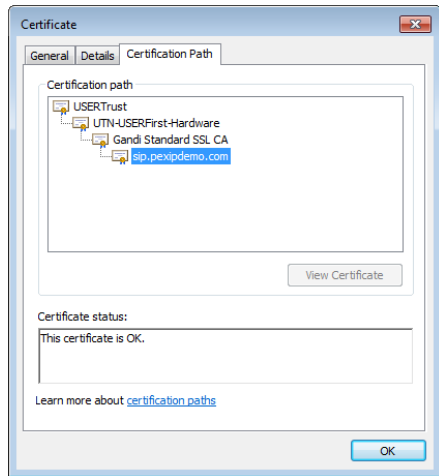
Certificates issued by intermediate CAs

In most cases, server certificates are issued by intermediate Certificate Authorities (as opposed to Root CAs). When this is the case, the chain of intermediate CA certificates must be installed on the Management Node to ensure that the certificate chain of trust is properly established when clients connect to a Conferencing Node over SIP TLS.

The intermediate CA certificates can be bundled/concatenated in a single text file and uploaded to the Management Node by going to **Platform Configuration > Trusted CA Certificates** and selecting **Import**. Whenever a Certificate Authority provides a server certificate issued through one or more intermediate CAs, the provider normally also provides this bundle of intermediate CA certificates as part of the process.

To identify whether or not a certificate has been issued by an intermediate CA, ensure that the certificate has a **.cer** file extension and open the certificate file on a Windows PC. Navigating to the **Certification Path** pane will display the CA structure of the certificate.

In the example below, the certificate for **sip.pexipdemo.com** has been issued by the intermediate CA **Gandi Standard SSL CA**, which is a subordinate CA for **UTN-USERFirst-Hardware**, which in turn is a subordinate CA for **USERTrust**, which is the root CA in this case:



In this particular case, **UTN-USERFirst-Hardware** and **Gandi Standard SSL CA** are the intermediate Certificate Authorities for the **sip.pexipdemo.com** certificate. This means that we would have to bundle together these two CA certificates in a text file and upload it using the **Import** trusted CAs facility on the Management Node in order to ensure proper certificate chain trust for the server certificates we install on the Conferencing Nodes.

Configuring the SIP TLS FQDN for a Conferencing Node

When assigning a server certificate to a Conferencing Node, you must configure the SIP TLS FQDN for this Conferencing Node to an FQDN matching that of the certificate. The **SIP TLS FQDN** setting is configurable for each Conferencing Node, by going to **Platform Configuration > Conferencing Nodes** and selecting the Conferencing Node in question.

The **SIP TLS FQDN** setting allows the administrator to set the DNS FQDN that a Conferencing Node will use when presenting its identity to connecting clients (by controlling which value the Conferencing Node will insert in its SIP contact header). Each Conferencing Node must have a unique **SIP TLS FQDN**.

Using our public DMZ example, when assigning a Conferencing Node a common certificate issued to **sip.example.com** but where that certificate contains each Conferencing Node's FQDN as one of the certificate's altNames, you would then normally also configure the node's hostname (**conf01.example.com** in this example) as the **SIP TLS FQDN** for this Conferencing Node (and **conf01.example.com** would also be the DNS A-record pointing to the publicly-reachable IP address of the Conferencing Node in question):

SIP TLS FQDN	<input type="text" value="conf01.example.com"/>
<small>(Required for Conferencing Nodes that are involved in signalling of calls to and from Lync / Skype for Business servers.) An identity for this Conferencing Node, used in signaling SIP TLS Contact addresses. For more information, see SIP TLS FQDN. Maximum length: 255 characters.</small>	

In our on-premises example, the node with a hostname of **eu-px01.example.com** would have its **SIP TLS FQDN** also set to **eu-px01.example.com**, and so on for the other Conferencing Nodes.

Certificate signing requests (CSRs)

To acquire a server certificate from a Certificate Authority (CA), a certificate signing request (CSR) has to be created and submitted to the CA. You can generate a CSR from within Pexip Infinity, and then upload the returned certificate associated with that request.

CSRs generated via Pexip Infinity always request client certificate and server certificate capabilities.

Creating a certificate signing request

To generate a CSR within Pexip Infinity:

1. Go to **Utilities > Certificate Signing Requests**.
2. Select **Add Certificate signing request**.
3. Complete the following fields:

Subject name	Select the name to be specified as the Common Name field of the requested certificate's subject. This is typically set to the FQDN of the node on which the certificate is to be installed. The available options are prepopulated with the FQDNs (hostname plus domain) of the Management Node and each currently deployed Conferencing Node. The list also includes any SIP TLS FQDN names of your Conferencing Nodes, if such names have been configured and are different from the node's FQDN. If you want to specify a custom Common Name instead, select <i>User-provided custom Common Name</i> .
Custom subject name	Enter the name that you want to use as the Common Name field of the requested certificate's subject, if you have selected <i>User-provided custom Common Name</i> above.
Private key type	Select the type of private key to generate, or select <i>Upload user-provided private key</i> if you want to provide your own private key. Default: RSA (2048bit)
Private key	Only applies if you have selected <i>Upload user-provided private key</i> above. Enter the PEM formatted RSA or ECC private key to use when generating your CSR. You can either paste the key into the input field or upload the private key file from your local file system.
Subject alternative names	Select the subject alternative names to be included in the CSR. This allows the certificate to be used to secure a server with multiple names (such as a different DNS name), or to secure multiple servers using the same certificate. You can choose from the same list of names presented in the Subject name field (the name you have already chosen as the Common Name is by default automatically included in the Subject alternative names list). In some deployments it may be more practical to generate single CSR in which all of your Conferencing Node FQDNs are included in the list of subject alternative names. This means that the same single server certificate returned by the CA can then be assigned to every Conferencing Node. When integrating with Microsoft Lync / Skype for Business, subject alternative name entries must be included for every individual Conferencing Node in the public DMZ (public DMZ deployments) or in the trusted application pool (on-prem deployments). See Certificate creation and requirements more information.
Additional subject alternative names	Optionally, enter a comma-separated list of additional subject alternative names to include in the CSR. For example, when integrating with on-prem Lync / Skype for Business deployments you would typically need to add the trusted application pool FQDN.
Additional subject fields (if required you can enter the following additional CSR attributes; these are all blank by default)	
Organization name	The name of your organization.
Department	The department within your organization.
City	The city where your organization is located.

State or Province	The state or province where your organization is located.
Country	The 2 letter code of the country where your organization is located.
Advanced (in most scenarios you should leave the advanced options to their default settings)	
Include Microsoft certificate template extension	Select this option to specify a (Microsoft-specific) certificate template in the CSR. This is needed when using the Certification Authority MMC snap-in to request a certificate from an enterprise CA. Selecting this option causes the 'WebServer' certificate template to be specified. Default: disabled.
Include Common Name in Subject Alternative Names	Specifies whether to include the requested subject Common Name in the Subject Alternative Name field of the CSR. Default: enabled.

4. Select **Save**.

You are returned to the list of certificate signing requests.

5. Select the CSR you have just created.

You are shown the decoded certificate data.

6. Scroll to the bottom of the page and select **Download**.

This downloads the CSR to your local file system, with a filename in the format `<subject-name>.csr`.

Note that the private key is not downloaded, or included within the CSR.

7. You can now submit this CSR file to your chosen CA for signing.

The CA will then send you a signed certificate which you can upload into Pexip Infinity (see below).

Uploading the signed certificate associated with a certificate signing request

When the Certificate Authority sends you a signed certificate in response to your CSR, you can upload that certificate into Pexip Infinity and assign it to one or more of your nodes. Make sure that you upload it via the **Certificate Signing Requests** page as this ensures that it is linked with the private key associated with your original CSR.

To upload the signed certificate:

1. Go to **Utilities > Certificate Signing Requests**.

2. Select the original CSR that is associated with the signed certificate.

You are shown the decoded certificate data.

3. Scroll down the page and in the **Certificate** field either paste the PEM-formatted certificate into the input field or upload the certificate file from your local file system.

The certificate file that you have obtained from the Certificate Authority typically has a .CRT or .PEM extension. Do not upload your certificate signing request (.CSR file).

4. Select **Complete**.

Providing it is a valid certificate and is based on the original CSR:

- the certificate is uploaded and automatically linked with the private key associated with your original CSR
- the original CSR is deleted
- you are taken to the **Change TLS Certificate** page.

5. You can now assign that certificate to the Management Node or one of more Conferencing Nodes as required:

- a. From within the **Change TLS Certificate** page go to the **Nodes** field and from the **Available Nodes** list, select the nodes to which you want to assign the certificate and move them into the **Chosen Nodes** list.
- b. Go to the bottom of the page and select **Save**.

Troubleshooting

If you receive an error message "Certificate and private key do not appear to be part of the same key pair" when attempting to upload a signed certificate, this most likely means that you have tried to upload the certificate against the wrong CSR.

Modifying a CSR

After a CSR has been created it cannot be modified — the only available actions are to download it (for sending to a CA), or to apply the returned, signed certificate that is associated with that request.

If you need to change the content of a CSR, you should delete the original CSR and create a new CSR with the correct content.

Note that a CSR is automatically deleted when the resulting signed certificate is uploaded.

Presence and contact lists

Publishing presence information

Pexip Infinity automatically publishes basic presence information in Microsoft Lync and Skype for Business environments for Pexip services (Virtual Meeting Rooms, Virtual Auditoriums and contacts reached via the Pexip Distributed Gateway). The contact will indicate that it is 'Available' when a Lync/SfB client subscribes to it.

Note that a Pexip Distributed Gateway contact publishes an 'Available' presence if the contact alias matches any Call Routing Rule. This does not necessarily mean that the destination alias that is associated with the rule is online and available.

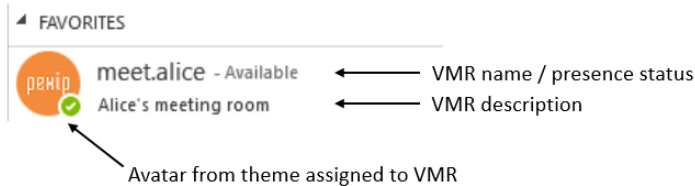
The Call Routing Rule that allows Lync/SfB to dial out to other devices should be configured with a **Destination alias regex match** that matches your dial plan as precisely as possible. For example, if all of your endpoints have a dial plan in the format **<city>-roomXXX@vc.example.com** where XXX is a number (e.g. london-room003@vc.example.com), then you should use a regex like **[a-z]+-room\d\d\d@vc\.example\.com** instead of just **.*@vc.example.com**. This will help identify invalid contact addresses in the Lync/SfB client contact list as they would not match the rule, have no presence, and hopefully alert the Lync/SfB user to a possible typing mistake.

Customizing the contact list avatar

You can customize the avatar that is displayed in Lync/SfB users' contact lists to represent the Pexip service.

The avatar that is displayed in the Lync/SfB user's contact list is the content of the **presence_avatar_image.jpg** file contained in the theme associated with the VMR. If no theme has been associated with the VMR, or it is a Pexip Distributed Gateway contact, then the avatar from the default theme is used. Note that this feature only works in environments where the Conferencing Nodes are directly reachable from the Lync/SfB client.

The contact list also displays the VMR name, its presence status and the VMR description.



For more information about how to customize a theme, see 'Customizing video and voice prompts using themes' in the [Pexip Infinity Administrator Guide](#).

Appendix 1: Public DMZ deployment with multiple SIP domains

For some environments, such as those required by service providers, it may be desirable to support (host) multiple SIP domains for Lync / Skype for Business federation in a Pexip Infinity public DMZ deployment.

In our [example public DMZ deployment](#), federation support for the SIP domain `example.com` was implemented. This comprised:

- two Conferencing Nodes: `conf01.example.com` and `conf02.example.com`
- a global Pexip Infinity domain of `example.com`
- a `_sipfederationtls._tcp.example.com` DNS SRV record pointing to `sip.example.com`
- the same SAN certificate installed on every Conferencing Node, configured as:
`commonName = sip.example.com`
`altNames = sip.example.com, conf01.example.com, conf02.example.com`

This section describes the considerations and steps that must be taken to add an additional [subdomain](#) e.g. `abc.example.com` or an additional [top-level domain](#) e.g. `customer-xyz.com` to this existing deployment.

Adding an additional subdomain

To add an additional subdomain e.g. `abc.example.com` to an existing deployment:

1. Add a new system location.
You must add a new Pexip Infinity system location (**Platform Configuration > Locations**) to support each additional subdomain. For example, add a new system location `abc` to support the subdomain `abc.example.com`.
2. Configure the Pexip Infinity domain for the new system location.
In our example deployment, the **Pexip Infinity domain (for Lync / Skype for Business integration)** global setting (**Platform Configuration > Global Settings**) has been set to `example.com`.
You must override this global setting for each new location. Go to **Platform Configuration > Locations** and configure the **Pexip Infinity domain (for Lync / Skype for Business integration)** setting as appropriate for each new location.
For example, for location `abc`, set the **Pexip Infinity domain (for Lync / Skype for Business integration)** to `abc.example.com`.
3. Deploy new Conferencing Nodes.
You must deploy new Conferencing Nodes to support each additional subdomain, and they should be assigned to the new system location.
For example, add nodes `conf01.abc.example.com` and `conf02.abc.example.com` and assign them to location `abc`.
4. Configure additional DNS A records and DNS SRV records for the new Conferencing Nodes.
For example, for the nodes supporting subdomain `abc.example.com`, you would create:
 - A-record: `conf01.abc.example.com`, pointing to the publicly-reachable IP address of `conf01.abc.example.com`
 - A-record: `conf02.abc.example.com`, pointing to the publicly-reachable IP address of `conf02.abc.example.com`
 - SRV-record: `_sipfederationtls._tcp.abc.example.com`, pointing to `conf01.abc.example.com` on port **5061**Note that the domain name used in the SRV-record has to match the domain in the corresponding A-record (e.g. `_sipfederationtls._tcp.abc.example.com` must use the same domain as `conf01.abc.example.com`; you cannot, for example, configure the `_sipfederationtls._tcp.abc.example.com` SRV-record to point to `conf01.example.com`). This is required due to the trust model for Lync/SfB federation.
5. Obtain and install a SAN certificate for the new Conferencing Nodes.
All of the new Conferencing Nodes in the new location should use the same SAN certificate. The certificate Common Name should be set to the FQDN of the node referenced by the `_sipfederationtls._tcp` SRV record, and the SANs should include the FQDNs of all of the nodes in the location.
For example, the certificate for our new nodes would have:

```
commonName = conf01.abc.example.com
altNames = conf01.abc.example.com, conf02.abc.example.com
```

See [Certificate creation and requirements](#) for more information on generating certificate signing requests.

6. Configure each Conferencing Node's **SIP TLS FQDN**.

The SIP TLS FQDN setting for each node should be configured to reflect its unique DNS FQDN. Go to **Platform Configuration > Conferencing Nodes**, choose each Conferencing Node in turn and configure the **SIP TLS FQDN** field accordingly.

7. To provide additional media capacity, you can optionally configure the new **abc** location to have a **Primary overflow location** set to the system location used by the original Conferencing Nodes that are supporting the **example.com** domain (signaling will still be handled by the new nodes in the new location).

Adding an additional top-level domain

To add an additional top-level domain e.g. **customer-xyz.com** to an existing deployment:

1. Add a new system location.

You must add a new Pexip Infinity system location (**Platform Configuration > Locations**) to support each additional domain.

For example, add a new system location **xyz** to support the domain **customer-xyz.com**.

2. Configure the Pexip Infinity domain for the new system location.

In our example deployment, the **Pexip Infinity domain (for Lync / Skype for Business integration)** global setting (**Platform Configuration > Global Settings**) has been set to **example.com**.

You must override this global setting for each new location. Go to **Platform Configuration > Locations** and configure the **Pexip Infinity domain (for Lync / Skype for Business integration)** setting as appropriate for each new location.

For example, for location **xyz**, set the **Pexip Infinity domain (for Lync / Skype for Business integration)** to **customer-xyz.com**.

3. Deploy new Conferencing Nodes.

You must deploy new Conferencing Nodes to support each additional domain, and they should be assigned to the new system location.

For example, add nodes **conf01.customer-xyz.com** and **conf02.customer-xyz.com** and assign them to location **xyz**.

4. Configure additional DNS A records and DNS SRV records for the new Conferencing Nodes.

For example, for the nodes supporting domain **customer-xyz.com**, you would create:

- A-record: **conf01.customer-xyz.com**, pointing to the publicly-reachable IP address of **conf01.customer-xyz.com**
- A-record: **conf02.customer-xyz.com**, pointing to the publicly-reachable IP address of **conf02.customer-xyz.com**
- SRV-record: **_sipfederationtls._tcp.customer-xyz.com**, pointing to **conf01.customer-xyz.com** on port **5061**


Note that the domain name used in the SRV-record has to match the domain in the corresponding A-record (e.g. **_sipfederationtls._tcp.customer-xyz.com** must use the same domain as **conf01.customer-xyz.com**). This is required due to the trust model for Lync/SfB federation.

5. Obtain and install a SAN certificate for the new Conferencing Nodes.

All of the new Conferencing Nodes in the new location should use the same SAN certificate. The certificate Common Name should be set to the FQDN of the node referenced by the **_sipfederationtls._tcp** SRV record, and the SANs should include the FQDNs of all of the nodes in the location.

For example, the certificate for our new nodes would have:

```
commonName = conf01.customer-xyz.com
altNames = conf01.customer-xyz.com, conf02.customer-xyz.com
```

 When hosting an additional top-level domain (**customer-xyz.com** in our example), the owner of that domain will have to provide the certificate. Typically, in a service provider environment, the domain owner will be the customer itself and not the service provider. The customer would have to obtain the certificate and give it to the service provider.

6. Configure each Conferencing Node's **SIP TLS FQDN**.

The SIP TLS FQDN setting for each node should be configured to reflect its DNS FQDN. Go to **Platform Configuration > Conferencing Nodes**, choose each Conferencing Node in turn and configure the **SIP TLS FQDN** field accordingly.

7. To provide additional media capacity, you can optionally configure the new **xyz** location to have a **Primary overflow location** set to the system location used by the original Conferencing Nodes that are supporting the **example.com** domain (signaling will still be handled by the new nodes in the new location).

Appendix 2: Configuring Pexip Infinity nodes to work behind a NAT device

To configure your Pexip Infinity deployment to work behind a static NAT device (from the perspective of clients located on the Internet or in a dedicated video zone) you must:

1. Configure the NAT device / firewall with the static, publicly-reachable IP address of each Conferencing Node that you want to be accessible from devices in the internet / video zone, and then map the public address to the node's corresponding internal IP address. Note that it must be a 1:1 NAT.
2. Configure each publicly-reachable Conferencing Node with its **IPv4 static NAT address (Platform Configuration > Conferencing Nodes)** i.e. the public address of the node that you have configured on the NAT device.

Note that:

- Any Conferencing Nodes that are configured with a static NAT address must not be configured with the same **System location** as nodes that do not have static NAT enabled. This is to ensure that load balancing is not performed across nodes servicing external clients and nodes that can only service private IP addresses.
- Static NAT must be on the secondary interface if the Conferencing Node has dual network interfaces.
- Any internal systems such as Cisco VCSs or endpoints that will send signaling and media traffic to Pexip Infinity nodes that are enabled for static NAT should send that traffic to the public address of those nodes. You must ensure that your local network allows this.
- We do not recommend that you allow the Management Node to be accessible from devices in the public internet. However, if you want to do this, you must assign and configure the Management Node with its static NAT address. You should also configure your firewall to only allow access to the Management Node from the specific IP addresses from where you want to allow management tasks to be performed.
- There cannot be a NAT device between any Pexip Infinity nodes.

Appendix 3: Firewall ports

When integrating Pexip Infinity with Microsoft Lync and Skype for Business, the following ports have to be allowed through any firewalls which carry traffic for the involved devices:

Direction	Purpose	Protocol	Source	Destination
Between the Lync/SfB FEP and the Conferencing Node (bidirectional)	SIP signaling	TCP	<any>	5061
From Lync/SfB clients towards the Conferencing Nodes	RTP/RTCP media	UDP	<any>	40000–49999
From Lync/SfB clients towards the Conferencing Nodes	HTTP conference avatar	TCP	<any>	80
From the Conferencing Nodes towards a Lync/SfB Edge server (AV Edge Interface)	RTP/RTCP/RDP media	UDP / TCP	40000–49999	50000–59999
From the Lync/SfB Edge server (AV Edge Interface) towards Conferencing Nodes	RTP/RTCP/RDP media	UDP / TCP	50000–59999	40000–49999
From the Conferencing Nodes towards Lync/SfB clients or Lync/SfB servers	RTP/RTCP/RDP media	UDP / TCP	40000–49999	<any>
From the Conferencing Nodes towards the TURN server	RTP/RTCP media	UDP	40000–49999	3478
From the Conferencing Nodes towards the Lync/SfB Web Conferencing service	PSOM (PowerPoint presentation from Lync/SfB)	TCP (TLS)	55000–65535	443 / 8057 †
From the Conferencing Nodes towards the Lync/SfB Front End server or Edge server	HTTPS (PowerPoint presentation from Lync/SfB)	TCP (TLS)	55000–65535	443

† typically 443 for Web Conferencing Edge and 8057 for a Lync/SfB Front End server / FEP

For a complete list of Pexip Infinity Conferencing Node port usage, see [Pexip Infinity port usage](#).

Appendix 4: Troubleshooting and limitations

Lync/SfB client does not connect to Pexip Infinity conference

Checklist

- Verify that a Virtual Meeting Room with the alias being dialed exists on the Management Node.
- Verify that the Conferencing Node receives the SIP INVITE request from the Lync/SfB client (via the FEP):
 - Management Node support log (Status > Support Log)
 - Lync/SfB FEP logging tool

Detail

If the Lync/SfB client fails to connect to the conference altogether, we need to verify that the alias exists on the Management Node. After that has been verified, check if the Conferencing Node receives the SIP INVITE request from the Lync/SfB client. This can be done both on the Conferencing Node (with the support log) and on the FEP serving the Lync/SfB client (using the Lync/SfB debugging tools).

A normal SIP call flow between a Lync/SfB client and the Pexip Infinity Conferencing Node should be:

Lync/SfB client	Pexip Infinity
	INVITE (with SDP) --->
	<--- 100 TRYING
	<--- 180 RINGING
	<--- 200 OK (with SDP)
	ACK --->

After ICE negotiation has completed between the Lync/SfB client and the Conferencing Node, the Lync/SfB client should send a second INVITE to signal the ICE negotiation completion. If this second INVITE is not seen, this is a strong indication of a media connectivity issue between the two peers.

Lync/SfB client can successfully connect to the Pexip Infinity conference, but audio and/or video is not working in one or both directions

Checklist

- Verify that the Lync/SfB client is correctly configured with an audio and video device.
- Verify that the call from the Lync/SfB client is placed as a video call rather than a Lync/SfB (audio-only) call.
- Verify (with SIP logs) that the SIP call setup behaves as expected:
 - INVITE from Lync/SfB client should contain m=audio and m=video lines in SDP
 - 200 OK response from Pexip Infinity should contain m=audio and m=video lines in SDP.
- Verify that firewall configuration permits relevant media traffic.
- Verify that Lync/SfB client receives RTP media from Pexip Infinity (using for instance Wireshark).
- Verify that Pexip Infinity Conferencing Node receives RTP media from Lync/SfB client (using for instance tcpdump).

Collecting SIP logs using the Lync/SfB Server Logging Tool

The Microsoft Debugging Tools can be downloaded from:

- Lync Server 2013: <http://www.microsoft.com/en-us/download/details.aspx?id=35453>
- Skype for Business Server 2015: <https://www.microsoft.com/en-us/download/details.aspx?id=47263>

The default location for installation of the logging tool is:

- Lync 2013: **C:\Program Files\Microsoft Lync Server 2013\Debugging Tools\OCSLogger.exe;**
- Lync 2010: **C:\Program Files\Common Files\Microsoft Lync Server 2010\Tracing\OCSLogger.exe**
- Skype for Business Server 2015: **C:\Program Files\Skype for Business Server 2015\Debugging Tools\CLSLogger.exe**

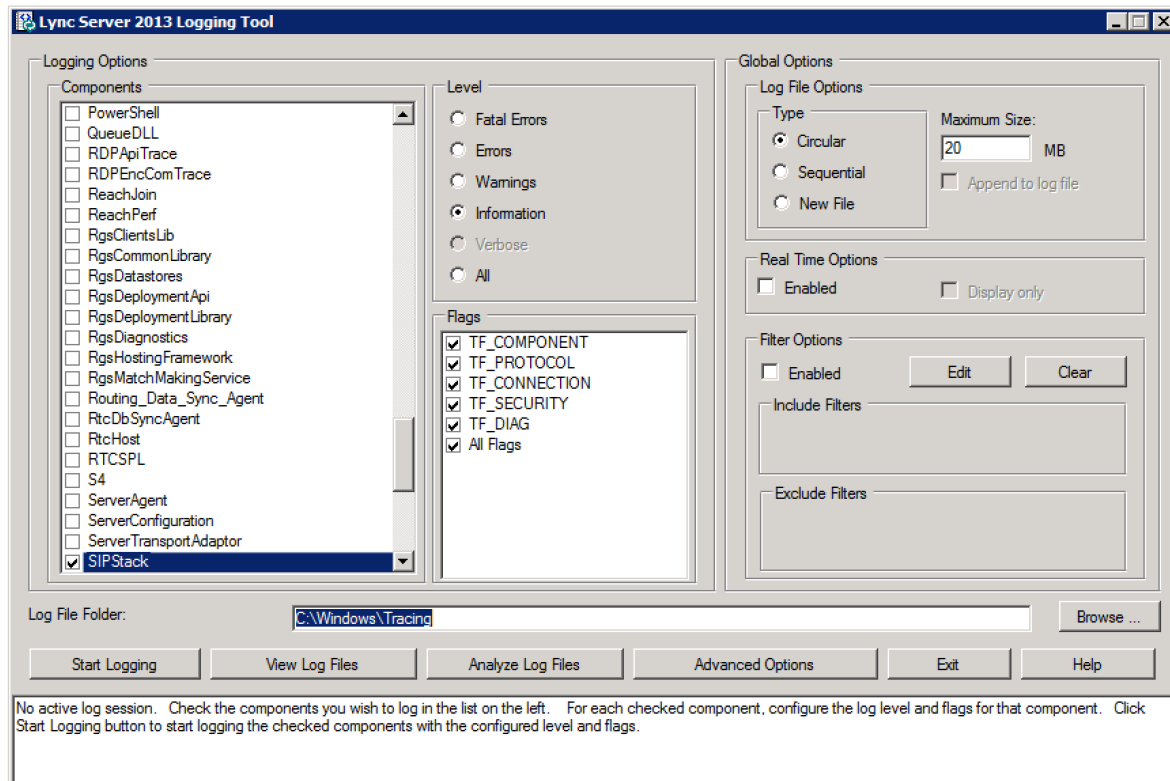
Note however that a different location may have been chosen at the time of installation.

After opening the logging tool, the following selection is normally suitable for initial troubleshooting of failing calls between Lync/SfB and the Pexip Infinity Conferencing Node:

- Components: SIPStack, InboundRouting and OutboundRouting
(Note that the InboundRouting and OutboundRouting components are only available on a FEP)
- Level: Information
- Flags: All Flags

To use the Lync Server logging tool:

1. Select **Start Logging** and place a new call from the Lync/SfB client towards the Pexip Infinity conference alias.
2. After the call has failed, select **Stop Logging**.
3. Select **View Log Files**.
4. Select **View** in the dialog which appears, and save the resulting text file in a suitable location.



Conference status shows backplanes to a merged Lync meeting with no participants

After a Pexip VMR has been merged with a Lync meeting, when viewing the conference status information for the VMR you may see one or more backplanes to the Lync/SfB server where there are no participants connected to that Lync/SfB node. One way in which this can occur is if a Lync/SfB client dials into a Pexip VMR, invites other Lync/SfB contacts into the meeting and then all of those participants disconnect.

Whenever a Lync/SfB client that is dialed into a Pexip VMR adds a contact into the meeting, an adhoc Lync meeting is created and it is merged with the Pexip VMR. A backplane is established between the Lync meeting and the Pexip VMR. That backplane will continue to exist even if all of the participants in the Lync meeting disconnect. The backplane is only taken down when the Pexip VMR conference ends.

Therefore if the Lync/SfB client and any other Lync/SfB contacts that had been in the adhoc Lync meeting all disconnect, you will continue to see the merged Lync meeting as a remote media node but with no participants connected to it.

Note that the remote media node of a merged Lync meeting is identified by the address of the Lync/SfB client that initiated the Lync meeting.

Poor image quality and delays when sharing content from Lync/SfB

This can occur when the maximum inbound or outbound call bandwidth is too low.

Ensure that the **Maximum inbound call bandwidth** and **Maximum outbound call bandwidth** advanced configuration settings for the Virtual Meeting Room or Virtual Auditorium is at least 1024 kbps.

Received content can be slow to update

Updates to content being received by a Lync client via Pexip Infinity can in some cases be slow to load when viewed in "fit to window" mode. When the same content is viewed in "actual size" mode, the images are updated as expected. This occurs when content is being sent via RDP; content sent via Video-based Screen Sharing (VbSS) is not affected. To resolve this issue, ensure that VbSS is enabled on the Lync / Skype for Business server, and on Pexip Infinity (**Platform Configuration > Global Settings > Connectivity > Enable Lync / Skype For Business Video-based Screen Sharing (VbSS)**).

DNS resolution failures

The following error messages indicate that DNS is not resolving addresses correctly:

- **Transaction failed UPDATE** appears as the disconnect reason when viewing participant status
- **RFC3263 lookup failure** appears in a **support.dns** log entry in the support log

Sending messages from a Lync/SfB client to a locked conference

If a Lync/SfB client initiates an IM session with a locked Pexip Infinity conference and attempts to send a message, it will appear to the Lync/SfB client as though the message has been successfully sent.

However, other participants in the Pexip Infinity conference will not see the message. The Lync/SfB client will temporarily appear in the conference participant list but cannot be allowed in to the locked conference (as they are not currently sending any audio or video).

Lync/SfB participants do not receive presentations / content sharing

Lync/SfB participants will not receive presentation content if Pexip Infinity is not configured to enable outbound calling to Lync/SfB clients.

You must configure Pexip Infinity to enable outbound calls to Lync/SfB clients. This includes ensuring that every Conferencing Node is configured with a TLS server certificate that is trusted by the Lync/SfB server environment, and that every node has its unique SIP TLS FQDN setting configured. See [Certificate creation and requirements](#) for more information.

Video calls from a Lync 2010 client for iOS only connect with audio

Outbound video calls made from the Lync 2010 client for iOS may only connect using audio rather than automatically escalating to video as expected. This is currently the expected behavior with this type of Lync client.

Lync/SfB presenter sees "Someone has joined and can't see what's being presented or shared" notification

If a Lync/SfB participant in a Lync meeting is presenting while another device joins the Lync meeting via the Pexip Distributed Gateway, the Lync/SfB presenter will see a "Someone has joined and can't see what's being presented or shared" notification.

However, the gateway participant will be able to see the presentation. The notification will disappear after approximately 15 seconds.

Lync/SfB users see low-resolution presentations in small scale

If a standards-based endpoint transmits a dual stream presentation at a very low resolution, the transcoded presentation will be sent in native resolution to any connected Lync/SfB clients.

This may create a sub-optimal experience depending on the PC screen resolution of the Lync/SfB end-user PC.

Can only make audio calls when using a Cisco VCS for call control

If a Cisco VCS is used as call control between a Conferencing Node and a Lync 2013 FEP, only audio calls are possible.

The FEP and the Conferencing Nodes should be neighbored directly and then audio and video calls will work as expected.

No video on Lync for Mac or Lync 2010 (PC) in Lync meetings

Video from Lync 2010 or Lync for Mac clients will not be seen on endpoints connected via Pexip into Lync meetings.

Pexip Infinity does not currently support sending an RTV video stream into AVMCU-hosted conferences. As a result, video from clients that only support RTV (such as Lync 2010 and Lync for Mac) will not be visible to those endpoints.

However, clients such as Lync for iPhone, Android, Lync 2013 PC, Windows phone, Skype for Business 2015 and so on, all support video when connected via Pexip into Lync meetings.

Poor sound quality

AVMCU calls support a maximum of G.722 (7 KHz audio), while Pexip Infinity supports up to AAC-LD (48 KHz audio). Under certain circumstances (for example, a meeting room with poor acoustics and many people speaking) there may be a perceptible difference in sound quality between an endpoint when using G.722 and the same endpoint when able to use a wider-band codec.

Problems connecting to Lync meetings via the Virtual Reception (IVR gateway)

The following table describes the typical problems and suggested resolutions for issues related to connecting to Lync meetings via the Virtual Reception (IVR gateway).

Symptom	Possible cause	Resolution
After entering the Conference ID, the call tries to connect to the user that scheduled the meeting.	The relevant Call Routing Rule does not have Match against full alias URI selected.	Ensure that Match against full alias URI is selected.
After entering the Conference ID, you get a "Call Failed: Conference extension not found" error.	The relevant Call Routing Rule does not have a trailing .* in the Destination alias regex match field.	Ensure that the Destination alias regex match field has a trailing .*

For more information, see [Routing indirectly via a Virtual Reception \(IVR gateway\)](#).

Audio-only calls when using a VCS for call control

If a Cisco VCS is used as call control between a Conferencing Node and a Lync 2013 FEP, only audio calls are possible.

Lync FEP and Conferencing Nodes should be neighbored directly then audio and video calls will work as expected.

Pexip VMR participants can't see shared PowerPoint files

If participants connected to the Pexip VMR in a Lync/SfB Fusion or gateway call can't see shared content when a Lync/SfB user presents PowerPoint files, the most likely reason is that **SIP TLS verification mode** is **On** (**Platform Configuration > Global Settings**) and that the Management Node does not trust the Lync/SfB Front End server / FEP or Web Conferencing Edge device (it is always the Web Conferencing Edge for federated connections). If the server is not trusted, Pexip participants will not see any content.

If this is the case you will see an **"unknown CA"** message similar to this in the Pexip Infinity support log:

```
Level="ERROR" Name="support.ms_data_conf.ms_data_conf" Message="PSOM connection attempt 1 failed"
Remote-address="lync-fep.example.local" Remote-port="8057" Error="SSL Alert" Reason-code="0x230" Alert-
type="fatal" Alert-description="unknown CA"
```

To resolve this, ensure that the trusted CA certificate of the relevant Lync Front End server / FEP or Web Conferencing Edge device is uploaded to the Management Node (**Platform Configuration > Trusted CA Certificates**).