# Pexip Infinity

# Microsoft Skype for Business / Lync Deployment Guide

**Software Version 29**

**Document Version 29.a**

**July 2022**

]pexip[

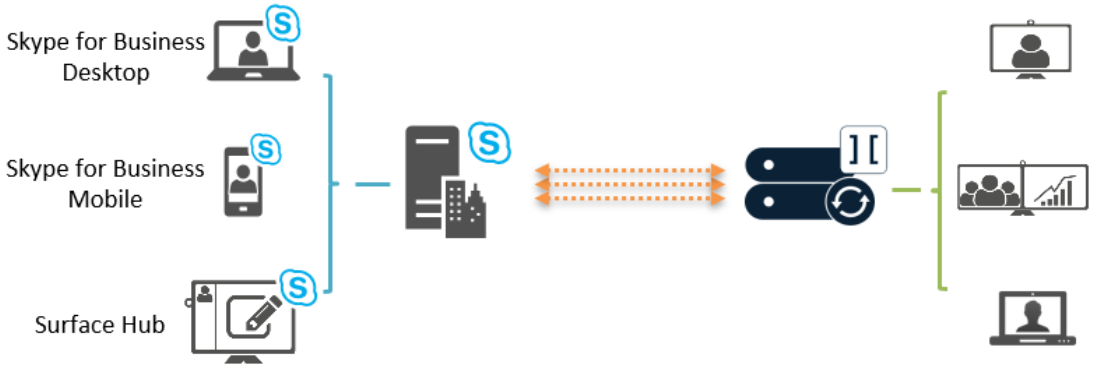
# Contents

# Introduction

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

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

It can be integrated with SfB/Lync as part of an existing, on-premises SfB/Lync environment inside an enterprise network, or as a standalone Pexip environment deployed in a public DMZ that enables direct federation with remote SfB/Lync environments, or as a hybrid deployment where SfB/Lync users may be homed either on-premises or in Office 365.




Pexip Infinity 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 SfB/Lync participants to join conferences hosted on Pexip Infinity, Pexip Infinity can act as a gateway between SfB/Lync and standards-based endpoints. This enables SfB/Lync 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 SfB/Lync meeting while retaining the native meeting experience on each device.

Version 29 of Pexip Infinity is interoperable with:

- Skype for Business
- Lync 2013 desktop clients for Windows
- Lync 2013 mobile clients for Apple iOS and Android devices.

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

## Architecture overview

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

- As part of an existing, on-premises SfB/Lync environment inside an enterprise network (referred to in this guide as **on-premises deployment**).
- As a standalone Pexip environment deployed in a public DMZ, leveraging direct federation with remote SfB/Lync environments (referred to in this guide as a **public DMZ deployment**).
- As a **hybrid deployment** which is a mix of on-premises and Office 365 deployments where users may be homed in either environment. A hybrid deployment has the same configuration requirements as a **public DMZ deployment**.

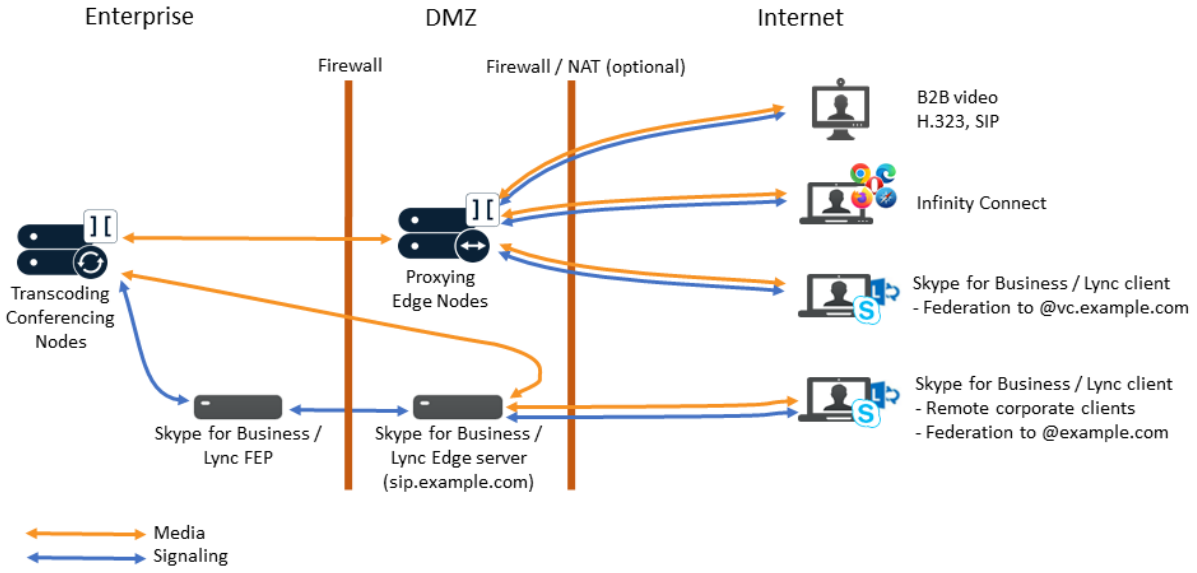
You will typically choose one of these methods, depending on requirements and preference. Each deployment method has a set of prerequisites and configuration steps which are covered in detail in the relevant sections of this guide.

## On-premises deployment

To integrate Pexip Infinity with an existing, on-premises SfB/Lync environment, one or more SIP domains are statically routed from the SfB/Lync environment towards one or more Pexip Infinity Conferencing Nodes. Then, when a SfB/Lync user dials a conference alias, such as meet.john@vc.example.com, or the alias of a standards-based endpoint, the user is placed into the appropriate Pexip-hosted conference. The SfB/Lync 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 SfB/Lync 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 SfB/Lync-enabled user in Active Directory. For example, if a user's SfB/Lync URI is **john@example.com** this could not be used as their VMR alias; however **meet.john@example.com** could be used.

An on-premises deployment can also provide access to Pexip Infinity services for clients located on the public internet. Here is an example deployment scenario for a separate VTC subdomain (vc.example.com) that provides B2B support for standards-based devices, federated B2B support for external SfB/Lync clients, and support for remote corporate SfB/Lync clients:




In this deployment scenario:

- Federated SfB calls to the Pexip Infinity video subdomain (e.g. @vc.example.com) are routed through Proxying Edge Nodes.
- Remote corporate SfB clients are routed through your SfB Edge server as normal, but they can also make gateway calls to the Pexip Infinity video subdomain (e.g. @vc.example.com) — in which case media is routed through the SfB Edge server providing the internal Transcoding Conferencing Node can route to the public facing interface of the SfB Edge server (otherwise a TURN server is required).
- Federated calls to your SfB domain (e.g. @example.com) are routed through your SfB Edge server as normal.
- Any external Infinity Connect clients (WebRTC and RTMP), SIP and H.323 endpoints and other forms of business-to-business video calls are routed through Proxying Edge Nodes. These calls can be gatewayed via Pexip Infinity to SfB/Lync clients or SfB/Lync meetings if required (see Using Pexip Infinity as a Skype for Business gateway for more information).

For full information on configuring Pexip Infinity with on-premises SfB/Lync, see Example on-premises deployment.

## Public DMZ / hybrid deployment

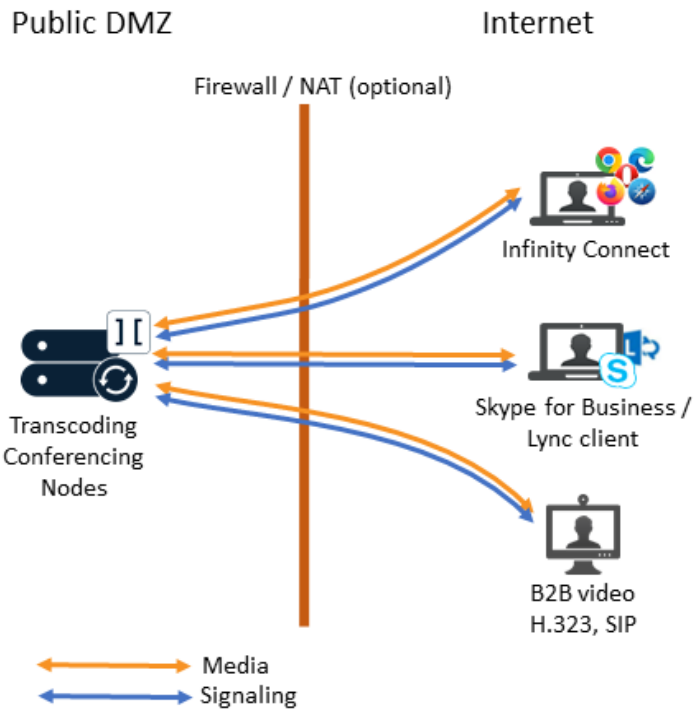
As Pexip Infinity supports SfB/Lync natively, it can be deployed to enable SfB/Lync interoperability without having any existing, on-premises SfB/Lync infrastructure. In such a deployment, Pexip Infinity can federate directly with remote SfB/Lync environments (on-premises environments as well as SfB/Lync Online/Office 365), without the need for a local SfB/Lync 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. The diagram (right) shows an example deployment scenario that also includes B2B support for standards-based devices.

When integrating with a **hybrid deployment** of SfB/Lync, where users may be homed either on-premises or in Office 365, you should follow the same configuration guidelines as for a **public DMZ deployment**.

For full information, see Example public DMZ / hybrid deployment.



# Integration features

Pexip Infinity enhances the feature set of Microsoft Skype for Business and Lync 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.

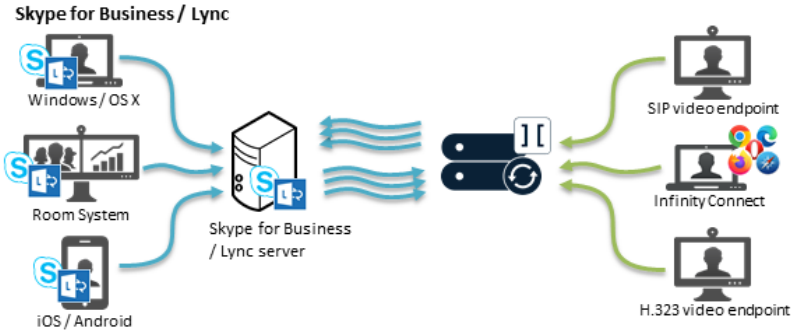
In addition, Pexip Infinity can be used as a direct gateway between any two users, regardless of device or technology. As a gateway, Pexip Infinity enables users to join from any system to a SfB/Lync meeting. This allows non-Microsoft users with anything from web browsers to traditional group videoconferencing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

Pexip's tight integration with SfB/Lync includes features such as simulcasting and multistreaming — see the full list of supported codecs, protocols, resilience and interoperability features.

## Pexip Infinity as a Skype for Business / Lync gateway

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

- invite H.323/SIP endpoints and registered Infinity Connect clients into a SfB/Lync meeting via manual dialout or drag and drop from the contacts list
- use the Infinity Gateway to route incoming calls directly into an ad hoc or scheduled SfB/Lync meeting
- when dialed into a Pexip VMR conference, invite other SfB/Lync or external contacts into that same Pexip VMR (this creates a new SfB/Lync meeting which is merged with the existing Pexip VMR)



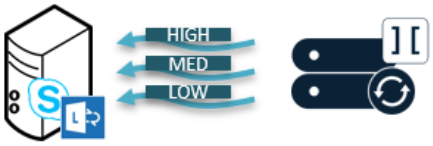

- receive and initiate person-to-person calls with standards-based devices, and then optionally add other participants (to escalate to a multipoint SfB meeting).

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

For information about to how configure the SfB/Lync gateway functionality, see Using Pexip Infinity as a Skype for Business gateway.

## Simulcast from Pexip Infinity to Skype for Business / Lync AVMCU

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




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

This optimizes the SfB/Lync user experience for all SfB/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**

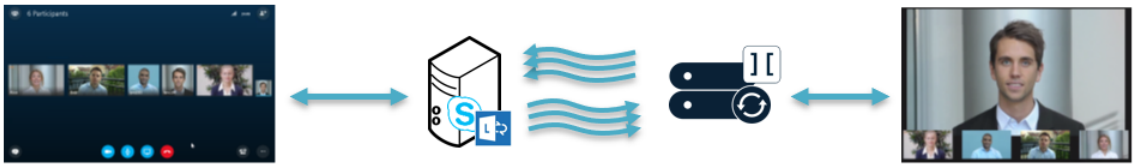
| Type | Start time | Tx codec | Tx bitrate (kbps) | Tx resolution | Tx framerate | Tx packets sent | Tx packets lost | Tx jitter (ms) | Rx codec | Rx bitrate (kbps) | Rx resolution | Rx framerate | Rx packets received | Rx packets lost | Rx jitter (ms) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Video | 2015-11-13 16:44:11 (GMT) | H.264 UC | 2500 | 1280x720 | 30.0 | 46926 | 0 | 0.02 | Off | 0 | | | 0 | 0 | -0.0 |
| Video | 2015-11-13 16:44:11 (GMT) | H.264 UC | 170 | 320x180 | 30.0 | 46240 | 0 | 0.0 | Off | 0 | | | 0 | 0 | -0.0 |
| Video | 2015-11-13 16:44:11 (GMT) | H.264 UC | 518 | 640x360 | 30.0 | 31009 | 0 | 0.0 | Off | 0 | | | 0 | 0 | -0.0 |

Simulcast to SfB/Lync AVMCU is automatically enabled and requires no administrator configuration.

# Multistreaming from Skype for Business / Lync 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 SfB/Lync meeting:

- Participants in a Pexip VMR that has been merged with a SfB/Lync meeting see a combined set of Pexip VMR and SfB/Lync meeting participants.
- Participants connected to a SfB/Lync meeting via the Infinity Gateway see a full combined set of both SfB/Lync 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:



Skype for Business user experience

Pexip gateway participant experience

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:

  Media streams

| Type | Start time | Tx codec | Tx bitrate (kbps) | Tx resolution | Tx framerate | Tx packets sent | Tx packets lost | Tx jitter (ms) | Rx codec | Rx bitrate (kbps) | Rx resolution | Rx framerate | 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 | 30.0 | 12137 | 0 | 4.73 |
| Video | 2015-11-13 16:44:11 (GMT) | Off | 0 | | | 0 | 0 | 0 | H.264 UC | 14 | 424x240 | 30.0 | 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 | 130 | 320x180 | 30.0 | 106312 | 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.
- If a SfB/Lync client pauses video or puts its call with the SfB/Lync meeting on hold, that participant is represented by a frozen image.
- 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.

SfB/Lync AVMCU multistreaming is automatically enabled and requires no administrator configuration.

# Supported codecs, protocols and resilience

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

- Video: H.264 UC and multistream H.264SVC (Lync 2013 and Skype for Business); Microsoft RTVideo support is deprecated from version 25.
- Audio: G.722.

Desktop/application window sharing, RDP and VbSS:

- Desktop and single application windows can be shared from Skype for Business / Lync for Windows, and Skype for Business / Lync for Mac.
- Pexip Infinity supports bi-directional RDP. Skype for Business / Lync users can send and receive dual streams.

- Pexip Infinity supports Video-based Screen Sharing (VbSS). Pexip Infinity supports sending and receiving content via VbSS to and from Skype for Business meetings, and to and from Skype for Business clients that are either calling another endpoint via the Infinity Gateway, or calling into a Virtual Meeting Room. For information about enabling VbSS on your Skype for Business infrastructure see https://technet.microsoft.com/en-us/library/mt756736.aspx.

Presenting PowerPoint files:

- Pexip Infinity supports the Persistent Shared Object Model (PSOM), and supports PowerPoint presentation from Windows desktop Lync 2013 and Windows Skype for Business clients.
- Participants that are connected to a Pexip VMR, or in a gateway call with a SfB/Lync client or SfB/Lync meeting, can see shared content if a SfB/Lync user presents PowerPoint files.
- Requires Office Web Apps (OWA) Server.
- Slide animation is not supported; Pexip participants will see a composite JPEG image. Also, annotations are not supported.
- Note that a SfB/Lync client's connection to a VMR or gateway participant is automatically escalated into a SfB/Lync meeting if the SfB/Lync client presents PowerPoint files.

Packet loss resiliency:

- Pexip Infinity supports send and receive video FEC (X-ULPFECUC) with Lync 2013 / Skype for Business clients and Skype for Business meetings.
- Pexip Infinity supports audio FEC (RED) for audio content sent to and received from Lync 2013 / Skype for Business clients and Skype for Business meetings.

Connectivity resilience:

- If the connection to a Skype for Business / Lync meeting is lost, Pexip Infinity attempts to re-establish the connection. Note that this does not apply to Pexip-hosted VMRs that have been merged into a SfB/Lync meeting.

## Limitations

The following are known limitations when integrating Pexip Infinity with Skype for Business / Lync:

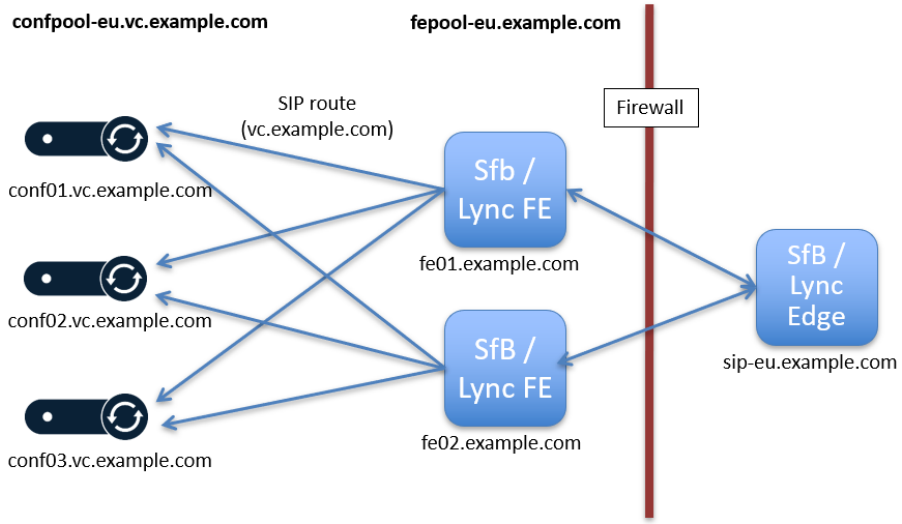
- Pexip Infinity does not support direct federation with consumer Skype; it does support federation with Skype for Business / Lync.
- For an on-prem Pexip Infinity deployment, if there are any firewalls in between the SfB/Lync server and the Conferencing Nodes, or between the internal SfB/Lync clients 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 SfB/Lync meetings with PIN-protected Pexip conferences:
  - When using drag and drop to merge a PIN-protected Pexip conference into a SfB/Lync meeting, you need to include the PIN in the SfB/Lync contact address using the format **<vmr_alias>**<PIN>@<domain>**. Note that this will make the PIN visible to other SfB/Lync meeting participants. You can only merge a locked Pexip conference into a SfB/Lync meeting if the Pexip conference is also PIN-protected.
  - If a SfB/Lync 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 SfB/Lync meeting (e.g. by drag-and-dropping other SfB/Lync participants into the call). Presentation and escalation is always possible if the SfB/Lync client initially dials the VMR with the PIN in the URI.
- When a SfB/Lync mobile client is in a gateway call to another device, it cannot invite other external contacts into that call unless the SfB/Lync mobile client is already in an existing SfB/Lync meeting.
- PowerPoint presentation from SfB on Mac clients is not supported.

For further information and troubleshooting, see Appendix 4: Troubleshooting and limitations .

# Example on-premises deployment

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

The following diagram shows the example deployment which forms the basis of the on-premises integration between SfB/Lync and Pexip Infinity:




***Example on-premises deployment used in this guide***

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 SfB/Lync infrastructure has two SfB/Lync Front End Servers in a Front End Pool (fepool-eu.example.com), and a SfB/Lync 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 (confpool-eu.vc.example.com) and integrated with SfB/Lync.

The example environment contains the following pools:

- SfB/Lync FEP **fepool-eu.example.com** containing:
  - fe01.example.com
  - fe02.example.com

  (Note that the SfB/Lync pool is assumed to be working already; this guide does not cover how to install SfB/Lync in general.)
- Pexip Conferencing Nodes **confpool-eu.vc.example.com** containing:
  - conf01.vc.example.com
  - conf02.vc.example.com
  - conf03.vc.example.com

The environment also contains a SfB/Lync Edge Server **sip-eu.example.com**.

Your actual Pexip Infinity environment may differ from the example, in which case you should make the relevant adjustments. This guide covers the specifics of one geographic location. Large enterprises with multiple SfB/Lync 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 example integration is to set up a static SIP domain route for the SIP domain **vc.example.com** (which in this example is a VTC subdomain of the main example.com SfB/Lync domain) from the Front End Pool towards a trusted application pool of local Conferencing Nodes. This provides a redundant integration environment between SfB/Lync and Pexip Infinity. This means that:

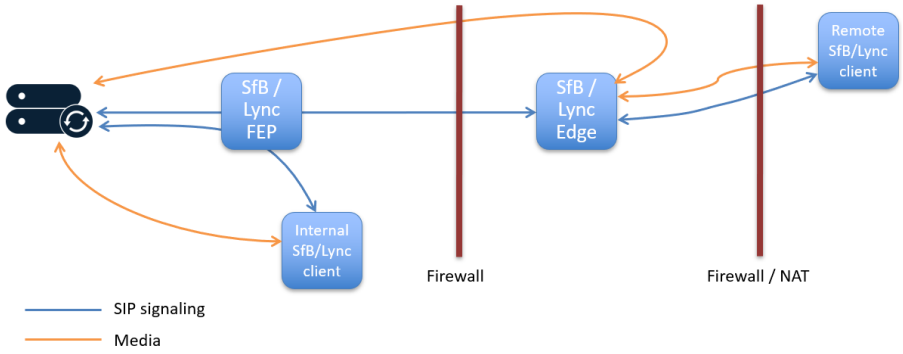
- Incoming calls from **remote corporate** SfB/Lync users to the VTC subdomain (vc.example.com) will arrive at the Edge Server and be routed to the Pexip Infinity Conferencing Nodes via the static SIP route on the Front End Pool. The configuration to support this routing is explained in this on-premises guide.
- Incoming native and federated SfB/Lync-to-SfB/Lync calls to the main example.com domain also arrive at the Edge Server and continue to be handled as normal.

In addition, you can also configure your Pexip Infinity system so that incoming calls from **external federated** SfB/Lync users to the VTC subdomain and any **B2B** calls are routed via Proxying Edge Nodes to the relevant services.

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

Conferencing Nodes do not need to use a TURN server for media routing to remote or federated SfB/Lync clients, providing they can reach the public-facing interface of the SfB/Lync Edge server. However, if the Conferencing Nodes are behind a NAT then they do need access to a STUN/TURN server so that each node can discover its NAT address. In Skype for Business / Lync deployments it is essential that a Conferencing Node can discover its NAT address.

The following diagram illustrates the typical signaling (SIP) and media (RTP) paths for various call scenarios involving Pexip Infinity and corporate SfB/Lync clients. Since media negotiation between Pexip Infinity and SfB/Lync 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-premises deployment signaling and media paths***

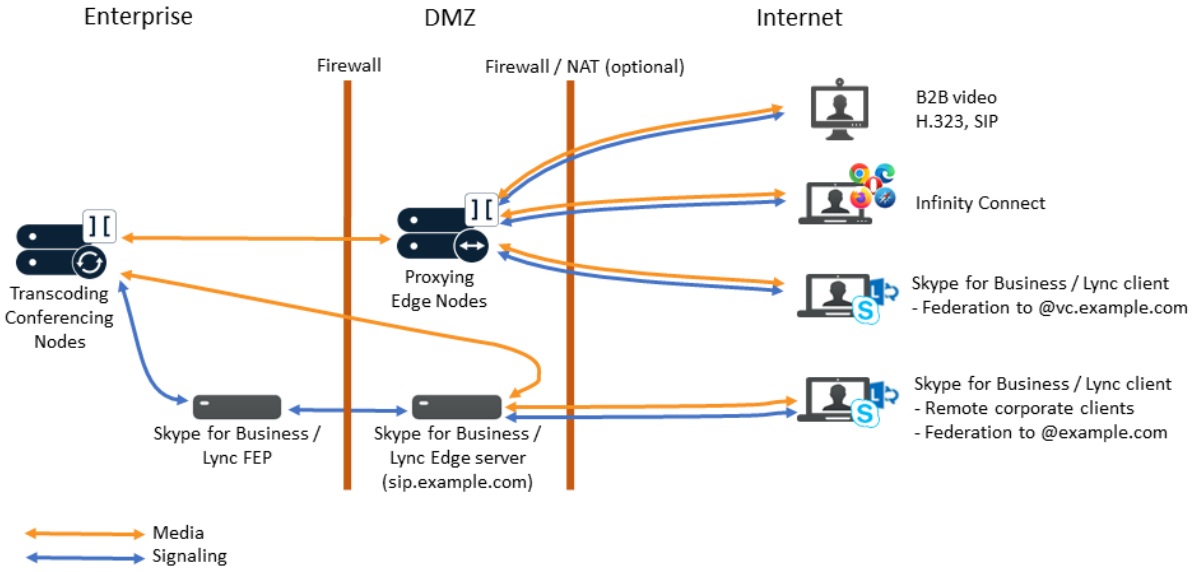
## Geographic distribution

With SfB/Lync environments that are geographically spread, for instance with SfB/Lync 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 SfB/Lync 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 SfB/Lync 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 Pexip-hosted conference to a SfB/Lync participant, SfB/Lync servers are configured for each location. This allows Pexip Infinity to dial out to the SfB/Lync server from a Conferencing Node at the most appropriate geographic location (see Adding new Front End Pools (FEPs), locations and Conferencing Nodes).

## Combining with support for other external clients

This integration between SfB/Lync and Pexip Infinity can fit into a broader deployment that also provides access to Pexip Infinity services for clients located on the public internet. Here is an example deployment scenario for a separate VTC subdomain (vc.example.com) that provides B2B support for standards-based devices, federated B2B support for external SfB/Lync clients, and support for remote corporate SfB/Lync clients:




# Pexip Infinity configuration for an on-premises Skype for Business environment

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

In this type of integration the Pexip Infinity Conferencing Nodes typically will reside on a private IP network. Conferencing Nodes do not need to use a TURN server for media routing to remote or federated SfB/Lync clients, providing they can reach the public-facing interface of the SfB/Lync Edge server. However, if the Conferencing Nodes are behind a NAT then they do need access to a STUN/TURN server so that each node can discover its NAT address. In Skype for Business / Lync deployments it is essential that a Conferencing Node can discover its NAT address.

## 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 Skype for Business / Lync 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 STUN/TURN server per location (optional, but required for supporting external/federated SfB/Lync clients).

After completing the Pexip Infinity configuration, you must also perform the Skype for Business server configuration for an on-premises deployment.

## Assigning a server certificate to the Pexip Infinity Conferencing Nodes

When integrating Pexip Infinity with an on-prem SfB/Lync environment, every Conferencing Node must be configured with a TLS server certificate which matches their respective FQDNs (Fully Qualified Domain Name), and the SfB/Lync servers must trust this certificate. Server certificates are typically issued by a Certificate Authority (CA) within the SfB/Lync environment itself (normally this will be the CA which was used to provide the SfB/Lync 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 SfB/Lync environment. Calls from SfB/Lync 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 SfB/Lync may be initiated by any Conferencing Node. To ensure that the SfB/Lync environment trusts these Conferencing Nodes, a certificate that is trusted by the SfB/Lync 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 (such as **confpool-eu.vc.example.com** in our examples).
- The Subject Alternative Name (altNames attribute) entries must include the Trusted Application Pool FQDN (i.e. a repeat of the Subject name), plus the FQDNs of all of the nodes in the pool that are involved in signaling.
- Assign the same certificate to all of the enterprise nodes that are involved in call signaling.

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 = confpool-eu.vc.example.com
altNames = conf01.vc.example.com, conf02.vc.example.com, conf03.vc.example.com, confpool-eu.vc.example.com
```

See Certificate and DNS examples for an on-premises integration for more information about synchronizing your DNS records and certificate names.

### 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 > 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 (**conf01.vc.example.com**, **conf02.vc.example.com** and **conf03.vc.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

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 > Trusted CA Certificates** and selecting **Import**.

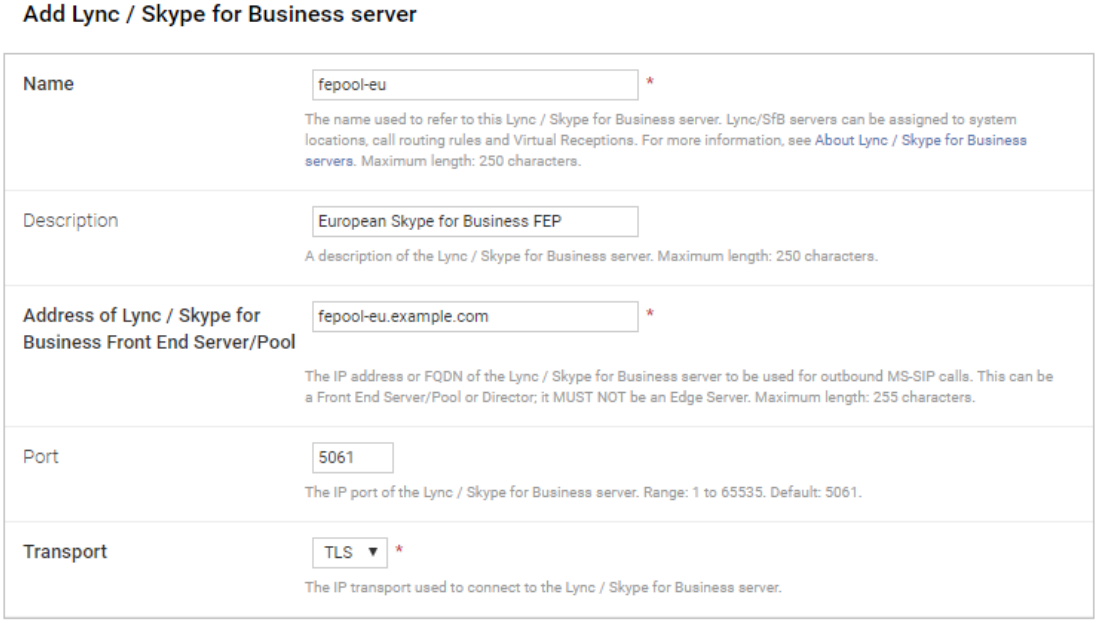
See Certificates issued by intermediate CAs for more information.

## Configuring a Skype for Business / Lync server per location

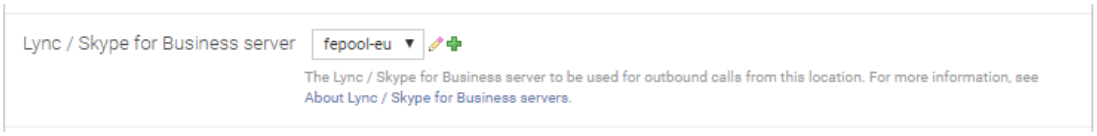
To allow internal Conferencing Nodes to call out to SfB/Lync clients you must define the target SfB/Lync servers. In our example deployment, a SfB/Lync Front End Pool has been deployed in Europe with the pool address **fepool-eu.example.com**.

To instruct the Conferencing Nodes in the Europe system location to use the Europe-based SfB/Lync Front End Pool, you must first define the SfB/Lync 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**:




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




## Configuring DNS records and DNS servers

You need to ensure the following DNS records for your Conferencing Nodes have been set up, and that Pexip Infinity is configured to use internal 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 is 3 records with host names of **conf01**, **conf02** and **conf03**, and they each point to the individual IP address of the node.
- Another A-record per Conferencing Node. This time the host name of every record should be **confpool-eu.vc.example.com** (the application pool name of the Conferencing Nodes), and again associate it with the IP address of each Conferencing Node. This step is not required for Skype for Business servers, but is necessary for Lync servers as it allows Lync to spread the traffic across all of the Conferencing Nodes.

For example (change the hostnames and IP addresses as appropriate for your actual deployment):

```
conf01.vc.example.com.          86400 IN A 10.44.0.10
conf02.vc.example.com.          86400 IN A 10.44.0.11
conf03.vc.example.com.          86400 IN A 10.44.0.12
confpool-eu.vc.example.com.     86400 IN A 10.44.0.10  (only required for Lync deployments)
confpool-eu.vc.example.com.     86400 IN A 10.44.0.11  (only required for Lync deployments)
confpool-eu.vc.example.com.     86400 IN A 10.44.0.12  (only required for Lync deployments)
```

See Certificate and DNS examples for an on-premises integration for more information about synchronizing your DNS records and certificate names.

### Pexip Infinity DNS server configuration

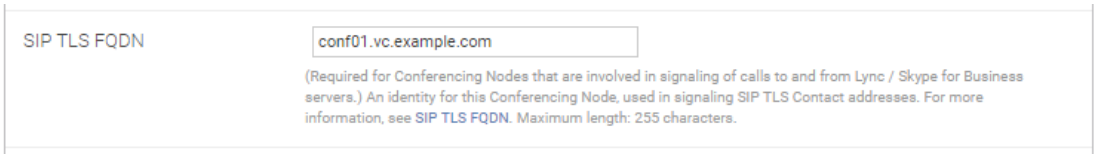
Ensure that Pexip Infinity is configured to use DNS servers on the inside of the network (**System > DNS Servers**, and then assigned to each location via **Platform > Locations**). This ensures that Pexip Infinity can resolve internal hostnames, which is mandatory for communicating with SfB/Lync on-premises.

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 SfB/Lync 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 > Conferencing Nodes**, choosing each node in turn and populating the **SIP TLS FQDN** field.



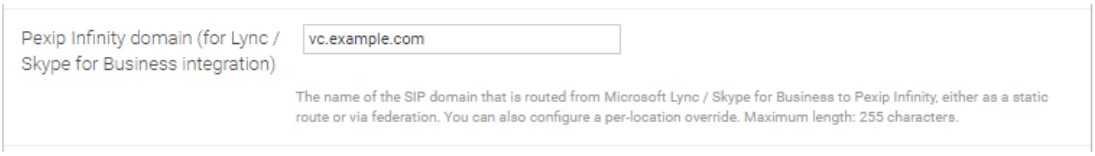

The example above shows the **SIP TLS FQDN** for the conf01 Conferencing Node, which is set to **conf01.vc.example.com**.

For any Pexip Infinity and SfB/Lync 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 SfB/Lync to Pexip Infinity for this deployment. This domain is inserted into the From header in outbound calls from Pexip Infinity to SfB/Lync, and ensures that SfB/Lync can route messages back to Pexip Infinity when, for example, initiating content sharing.

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




This must be set to the same SIP domain as used by the static route from SfB/Lync 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 STUN/TURN server per location (for supporting external/federated SfB/Lync clients)

Conferencing Nodes do not need to use a TURN server for media routing to remote or federated SfB/Lync clients, providing they can reach the public-facing interface of the SfB/Lync Edge server.

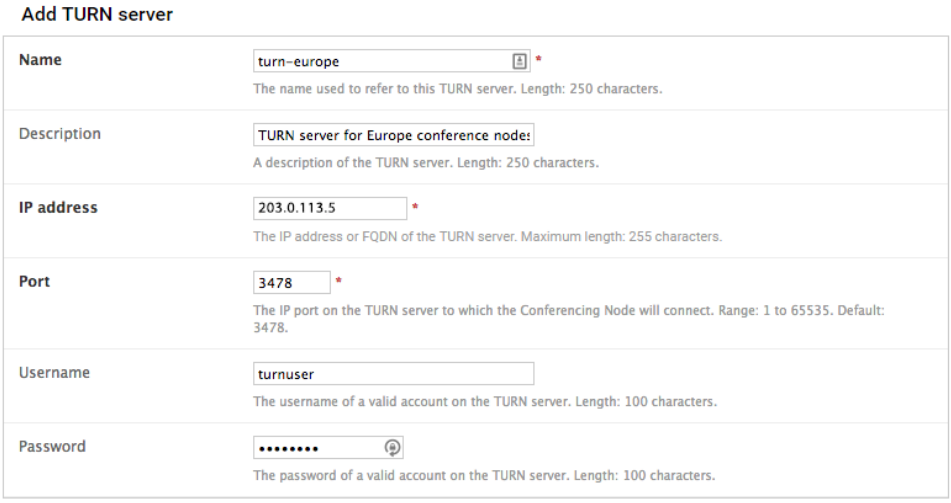
However, if there is NAT between the Conferencing Nodes and the public-facing interface of the SfB/Lync Edge server, those nodes need to use STUN so that they can discover and signal their public NAT address to the SfB/Lync client (so that it can create a TURN permission on the SfB/Lync Edge server for the node's reflexive address). When required, this STUN/TURN server is typically deployed outside of the enterprise firewall or in a public DMZ.

You can either configure Pexip Infinity with either the details of a TURN server (which can act as a STUN server) or with the details of a dedicated STUN server (which it will use instead of the TURN server).

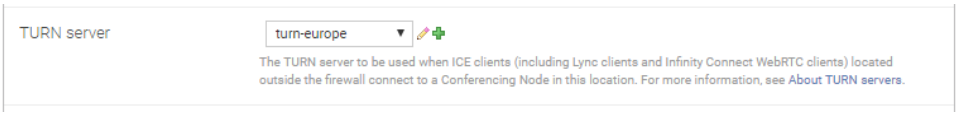
## Using a TURN server

To instruct the Conferencing Nodes to use a TURN server (which in our example has the IP address **203.0.113.5**), 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**:

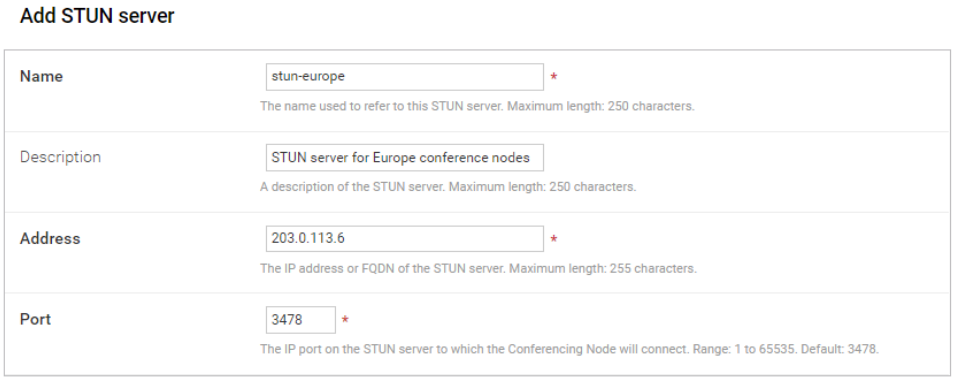



2. Complete the fields and select **Save**.
   In the example above, the TURN server has been defined by its **IP address** and **Port**, in addition to the **Username** and **Password** for our TURN user (which has already been created on the TURN server).
3. Assign this TURN server to the appropriate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



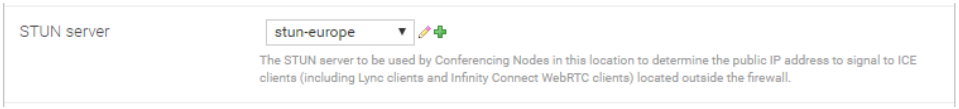

## Using a STUN server

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




2. Complete the fields and select **Save**.
3. Assign this STUN server to the appropriate location: go to **Platform > Locations** and select the **Europe** location.

4. In the **STUN server** field, select the Europe STUN server from the drop-down list, and then select **Save**.



# Skype for Business server configuration for an on-premises deployment

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

The SfB/Lync 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 SfB/Lync management shell**

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

The command syntax described in the following section is based on the devices described in the example deployment for the on-prem SfB/Lync 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 SfB/Lync management shell commands used in this deployment guide, see https://docs.microsoft.com/en-gb/powershell/module/skype/?view=skype-ps. 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 **fepool-eu.example.com** to trust traffic coming from Pexip Infinity (and to be able to send traffic back), as well as adding the first node (**conf01.vc.example.com**) as a computer in the application pool.

```
New-CsTrustedApplicationPool -Identity confpool-eu.vc.example.com -ComputerFqdn conf01.vc.example.com -Registrar fepool-eu.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 **confpool-eu.vc.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 SfB/Lync 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.

When creating a trusted application pool (and a trusted application computer in the next step) in this way, SfB/Lync will issue a warning stating:
**"WARNING: Machine conf01.vc.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, **conf02** and **conf03** 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 when creating a trusted application pool that will contain multiple computers, you **must** add the first trusted application computer when you initially create the trusted application pool.

To add more trusted application computers to the trusted application pool:

```
New-CsTrustedApplicationComputer -Identity conf02.vc.example.com -Pool confpool-eu.vc.example.com
New-CsTrustedApplicationComputer -Identity conf03.vc.example.com -Pool confpool-eu.vc.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 confpool-eu -TrustedApplicationPoolFqdn confpool-eu.vc.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 SfB/Lync, static SIP routes can either be associated with the global routing table, or with a specific SfB/Lync 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.

If you currently use global static routes for other integrations, these will become inoperable if you were to add routes per registrar.

This example creates a static route from the Europe Front End Pool (**fepool-eu.example.com**) to the **confpool-eu.vc.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:fepool-eu.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 (`fepool-eu.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:fepool-eu.example.com"
```

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

```
$route = New-CsStaticRoute -TLSRoute -Destination "confpool-eu.vc.example.com" -Port 5061 -MatchUri "vc.example.com" -
UseDefaultCertificate $true
Set-CsStaticRoutingConfiguration -Identity "Service:Registrar:fepool-eu.example.com" -Route @{Add=$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 SfB/Lync environment, SfB/Lync will only send SIP requests which are not destined to actual SfB/Lync users for that domain towards the Conferencing Nodes.

Pexip Infinity supports both same domain, and subdomain or different domain integrations. If your SfB/Lync environment consists of thousands of SfB/Lync 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.

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

`-Destination` defines the DNS FQDN where SfB/Lync 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 SfB/Lync clients to **meet@vc.example.com** and similar aliases within a few minutes. SfB/Lync 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 SfB/Lync 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 –TLSRoute –Destination "confpool-eu.vc.example.com" –MatchUri "vc.example.com" –Port 5061 –
UseDefaultCertificate $true
Set-CsStaticRoutingConfiguration –Identity "service:Registrar:fepool-eu.example.com" –Route @{Remove=$route}
```

### Removing the trusted application pools

```
Remove-CsTrustedApplicationPool –Identity "confpool-eu.vc.example.com"
```

### Re-enabling the topology

```
Enable-CsTopology
```

# Adding more nodes or locations to an existing on-premises Skype for Business deployment

This section explains the steps involved if you need to add additional Conferencing Nodes, or new Skype for Business / Lync servers and Conferencing Nodes in a new geographic location, to an existing on-premises SfB/Lync environment. It also describes a manual pool failover process.

## 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 **confNN.vc.example.com** and configure its SIP TLS FQDN setting to reflect its DNS FQDN.
- Assign DNS A records for this Conferencing Node:
  - A standard DNS A record, registered as its hostname e.g. **confNN.vc.example.com**.
  - Add a DNS A record to the pool domain **confpool-eu.vc.example.com** so that SfB/Lync will also load balance over this new node.

  For example (change the hostnames and IP addresses as appropriate for your actual deployment):

  ```
  conf04.vc.example.com.          86400 IN A 10.44.0.13
  confpool-eu.vc.example.com.     86400 IN A 10.44.0.13
  ```
- 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:

  ```
  commonName = confpool-eu.vc.example.com
  altNames = conf01.vc.example.com, conf02.vc.example.com, conf03.vc.example.com, confpool-eu.vc.example.com
  ```

  The name information in the new certificate would be (assuming the new hostname is **conf04.vc.example.com**):

  ```
  commonName = confpool-eu.vc.example.com
  altNames = conf01.vc.example.com, conf02.vc.example.com, conf03.vc.example.com, conf04.vc.example.com, confpool-
  eu.vc.example.com
  ```

**Within SfB/Lync**

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

```
New-CsTrustedApplicationComputer -Identity confNN.vc.example.com -Pool confpool-eu.vc.example.com
```

and then enable topology:

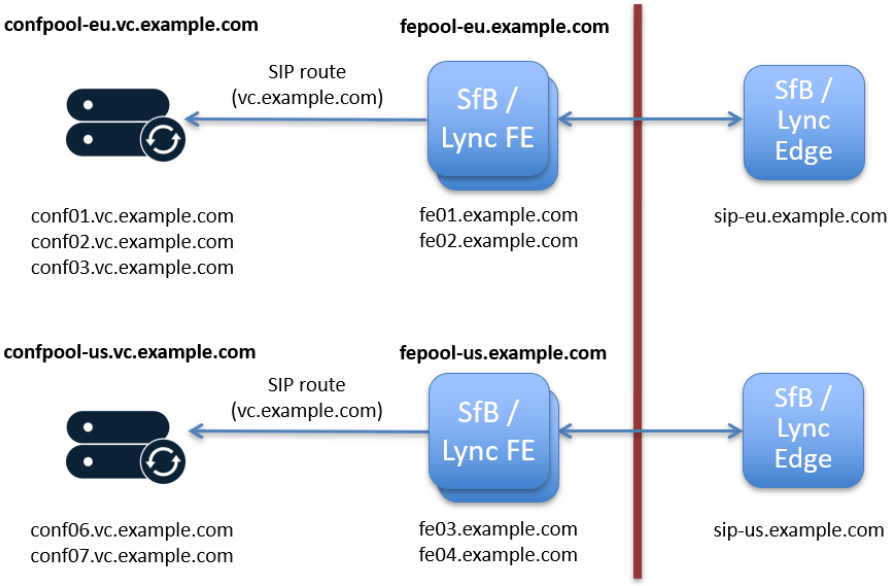
```
Enable-CsTopology
```

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

If you have SfB/Lync 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 (in addition to the existing Europe-located devices, as shown in the diagram, right):

- 2 SfB/Lync Front End Servers **fe03** and **fe04** in a pool **fepool-us.example.com**
- 2 Conferencing Nodes **conf06** and **conf07** in **System location *US*** and to be placed in an application pool **confpool-us.vc.example.com**




**Within Pexip Infinity**

1. Generate and assign a server certificate to the US Conferencing Nodes:

   commonName = **confpool-us.vc.example.com**
   altNames = **conf06.vc.example.com**, **conf07.vc.example.com**, **confpool-us.vc.example.com**
2. Configure the US system location to use:
   - the **fepool-us.example.com** Front End Pool
   - DNS servers on the inside of the network
   - a STUN/TURN server, if required.
3. Configure DNS records for the US Conferencing Nodes:
   - A-records for each Conferencing Node **conf06** and **conf07**
   - another A-record per Conferencing Node with the host name **confpool-us.vc.example.com** (the application pool name of the Conferencing Nodes).

   For example:

```
conf06.vc.example.com.          86400 IN A 10.44.0.15
conf07.vc.example.com.          86400 IN A 10.44.0.16
confpool-us.vc.example.com.     86400 IN A 10.44.0.15
confpool-us.vc.example.com.     86400 IN A 10.44.0.16
```

4. Configure the SIP TLS FQDN setting for each US Conferencing Node to reflect its DNS FQDN e.g. **conf06.vc.example.com** and **conf07.vc.example.com**.

**Within SfB/Lync**

1. Create a trusted application pool for the US Conferencing Nodes.

   This command adds a trusted application pool for the Front End Pool **fepool-us.example.com** and adds the first node (**conf06.vc.example.com**) as a computer in the application pool:

```
New-CsTrustedApplicationPool -Identity confpool-us.vc.example.com -ComputerFqdn conf06.vc.example.com -Registrar fepool-us.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 **conf07** to the new trusted application pool:

```
New-CsTrustedApplicationComputer -Identity conf07.vc.example.com -Pool confpool-us.vc.example.com
```

3. Create a trusted application for the pool of Conferencing Nodes.

   This command creates a trusted application for the **confpool-us.vc.example.com** pool:

```
New-CsTrustedApplication -Applicationid confpool-us -TrustedApplicationPoolFqdn confpool-us.vc.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 (**fepool-us.example.com**) to the **confpool-us.vc.example.com** nodes for the domain **vc.example.com**:

```
$newroute = New-CsStaticRoute -TLSRoute -Destination "confpool-us.vc.example.com" -Port 5061 -MatchUri "vc.example.com" -UseDefaultCertificate $true
```

```
Set-CsStaticRoutingConfiguration -Identity "Service:Registrar:fepool-us.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:fepool-us.example.com"
```

5. Enable the new topology using the following command:

```
Enable-CsTopology
```

## Pool failover (manual)

If a SfB/Lync Front End Pool becomes unavailable, you may need to reconfigure your Pexip Infinity system to use a different SfB/Lync pool/server.

To fail over to a secondary SfB/Lync pool/server within Pexip Infinity:

1. Ensure that the address of the alternative SfB/Lync Front End Pool is configured (**Call Control > Lync / Skype For Business ServerS**).
2. Assign the alternative SfB/Lync pool to the affected Pexip Infinity system locations: go to **Platform > Locations** and change the **Lync / Skype for Business server** in use for the relevant locations.
3. Assign the alternative SfB/Lync pool to any Call Routing Rules and Virtual Receptions that place calls to SfB/Lync from the affected locations: go to **Service Configuration > Call Routing** or **Virtual ReceptionS** and change the nominated **Lync / Skype for Business server** for the relevant rules / Virtual Receptions.

## Putting a Conferencing Node into maintenance mode

If a Conferencing Node in a trusted application pool is placed into maintenance mode, and a SfB/Lync server sends a call to that node, the node will respond with 503 Service Unavailable and the call will then fail (SfB/Lync will not try another node in the pool).

Therefore, if you need to place a Conferencing Node into maintenance mode, we recommend that you wait until all SfB/Lync calls on that node have completed, and then you should temporarily remove the node from the trusted application pool and then place it into maintenance mode. The node should then be returned to the trusted application pool after it has been taken back out of maintenance mode.

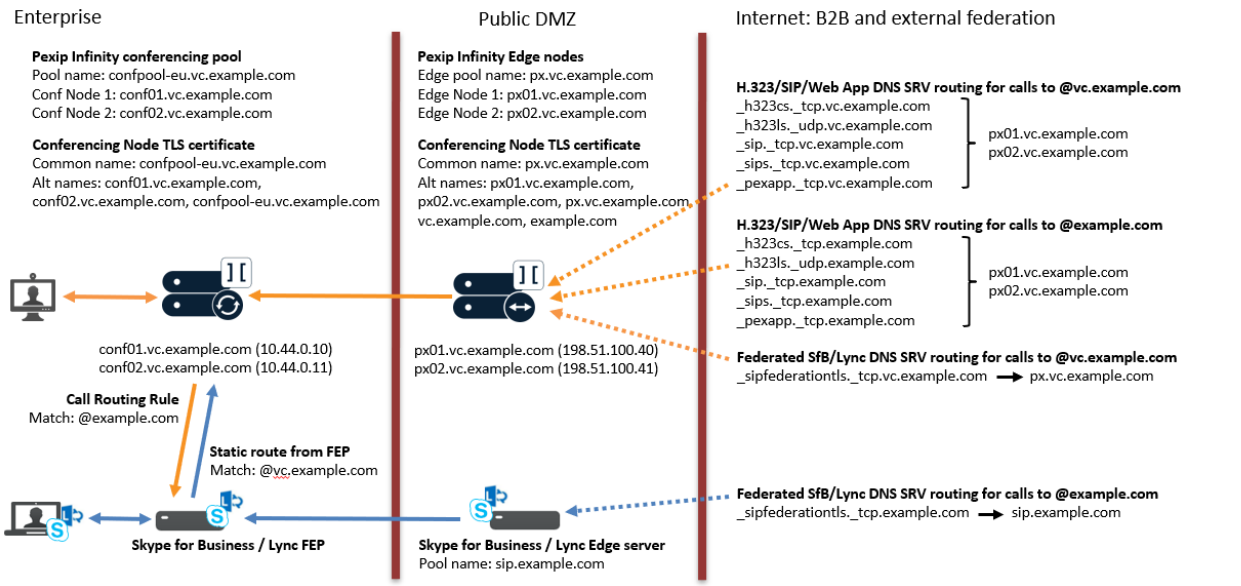
# Certificate and DNS examples for an on-premises integration

This topic contains example Conferencing Node naming patterns, certificate, and DNS requirements for an on-premises integration with Skype for Business / Lync. It also includes the DNS requirements for B2B federation with remote SfB/Lync and VTC systems.

You can use this example as the basis for your own integration, changing the example domain and DNS names as appropriate for your particular environment.

## Example deployment scenario

In this example, our on-premises SfB/Lync Front End Pool is configured with a trusted application pool of Conferencing Nodes, and that application pool has an identity/FQDN of confpool-eu.vc.example.com. The SfB/Lync Edge servers have a pool name of sip.example.com (sip.<domain> is the typical naming convention for the SfB/Lync Edge server pool name).




## Enterprise Conferencing Node configuration

For all of your enterprise-based Pexip Infinity Conferencing Nodes that are involved in call signaling with your on-premises SfB/Lync systems:

- The **SIP TLS FQDN** setting on each Conferencing Node **must** match the node's DNS FQDN and it must be unique per node. For example, if the node's DNS FQDN is **conf01.vc.example.com** then its **SIP TLS FQDN** setting must also be **conf01.vc.example.com**.
- The certificate on each Conferencing Node **must** refer to the Trusted Application Pool FQDN (as configured in SfB/Lync and used as the destination of the static route from SfB/Lync to Pexip) and it must also contain the Conferencing Node DNS FQDNs. We recommend that you generate and use a single SAN certificate that encompasses all of the Conferencing Nodes in the application pool:
  - The Subject name (commonName attribute) must be the Trusted Application Pool FQDN (such as **confpool-eu.vc.example.com** in our examples).
  - The Subject Alternative Name (altNames attribute) entries must include the Trusted Application Pool FQDN (i.e. a repeat of the Subject name), plus the FQDNs of all of the nodes in the pool that are involved in signaling.
  - Assign the same certificate to all of the enterprise nodes that are involved in call signaling.

## Public DMZ Conferencing Node configuration

For all of your public DMZ-based Pexip Infinity Conferencing Nodes that are involved in call signaling with your B2B and federated systems:

- The **SIP TLS FQDN** setting on each Conferencing Node **must** match the node's DNS FQDN and it must be unique per node. For example, if the node's DNS FQDN is **px01.vc.example.com** then its **SIP TLS FQDN** setting must also be **px01.vc.example.com**.
- The certificate on each Conferencing Node **must** include the hostname referenced by the _sipfederationtls._tcp SRV record that points to those nodes, plus the names of all of the Conferencing Nodes that are involved in call signaling:
  - The Subject name (commonName attribute) should be set to the target hostname referenced by the _sipfederationtls._tcp SRV record (the pool name of the Conferencing Nodes).

    In our examples, if the DNS SRV record is:

    ```
    _sipfederationtls._tcp.vc.example.com. 86400 IN SRV 1 100 5061 px.vc.example.com.
    ```

    then the Subject name must be **px.vc.example.com**
  - The Subject Alternative Name (altNames attribute) entries must include:
    - the target hostname referenced in the Subject name
    - the FQDNs of all of the public DMZ nodes that are involved in call signaling

        - the domain names that are used in any DNS SRV records that route calls to those Conferencing Nodes (e.g. **vc.example.com** from the example **_sipfederationtls** SRV record above).
    - Assign the same certificate to all of the public DMZ nodes that are involved in call signaling.
- The domain name used in the **_sipfederationtls._tcp.<domain>** SRV record has to match the domain in the corresponding A-record. This is required due to the trust model for SfB/Lync federation. For example:
    - An SRV record such as _sipfederationtls._tcp.**vc.example.com** must have a corresponding A-record with the same domain, such as px.**vc.example.com**.
    - You cannot, for example, configure the _sipfederationtls._tcp.vc.example.com SRV record to point to px.**video.example.com** or px01.**otherdomain.com**.

## DNS requirements for SfB/Lync and VTC federation

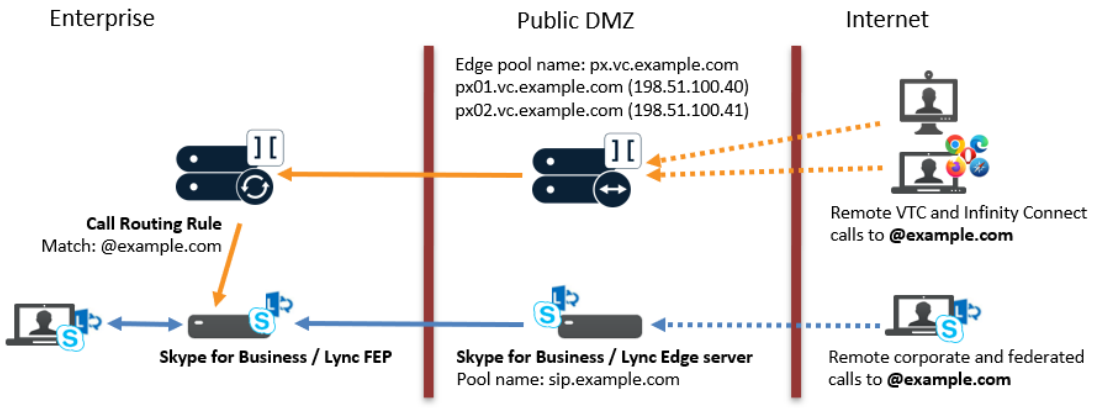
Here is a summary of the DNS requirements to support federation for SfB/Lync and VTC endpoints. These examples assume that:

- The **SfB/Lync** domain is **example.com**.
- The **Pexip Infinity** VTC subdomain is **vc.example.com**.
- There are two Pexip Conferencing Nodes in the public DMZ (px01 and px02, and they have a DNS poolname of px.vc.example.com).

Your standard DNS A records for your public DMZ Conferencing Nodes will typically already exist:

```
px01.vc.example.com.          86400 IN A 198.51.100.40
px02.vc.example.com.          86400 IN A 198.51.100.41
```

### Federation for the main SfB/Lync domain (example.com)




Typically, your main federation DNS SRV record for SfB/Lync clients will already exist.

This SRV record ensures that federated SfB/Lync clients that are calling contacts who have a "user@example.com" style name are routed to the SfB/Lync Edge server. For our example.com domain it would typically be:

```
_sipfederationtls._tcp.example.com. 86400 IN SRV 1 100 5061 sip.example.com.
```

To allow external VTC systems to dial SfB/Lync clients with user@example.com contact names, dial directly into SfB/Lync meetings, or dial a Pexip Virtual Reception (for example sfb.lobby@example.com) you must configure additional public DNS SRV records. These example records will direct calls from H.323 devices, SIP devices and Infinity Connect clients (via the _pexapp SRV record) that are placed to the top-level **example.com** domain to your Pexip Conferencing Nodes in the public DMZ (that are hosted in the **vc.example.com** subdomain):

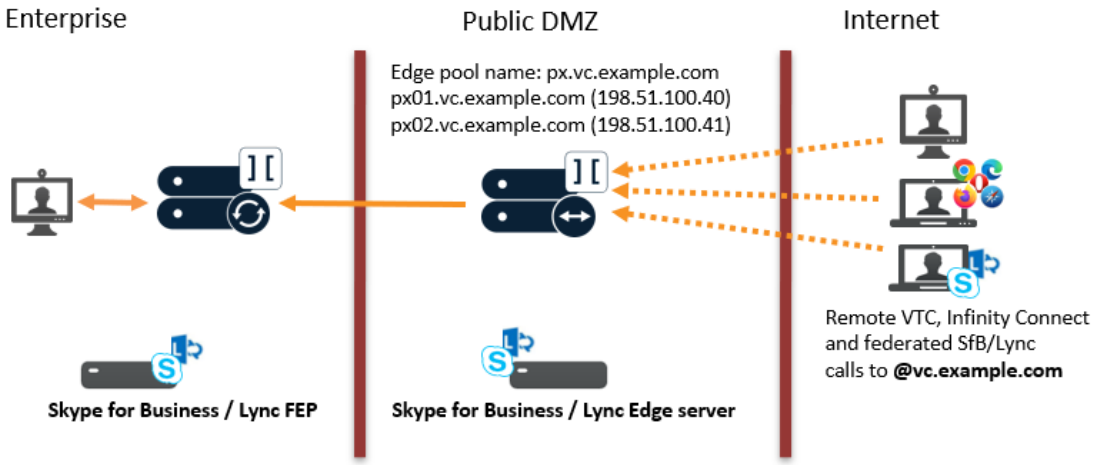
```
_h323cs._tcp.example.com. 86400 IN SRV 10 10 1720 px01.vc.example.com.
_h323cs._tcp.example.com. 86400 IN SRV 10 10 1720 px02.vc.example.com.

_h323ls._udp.example.com. 86400 IN SRV 10 10 1719 px01.vc.example.com.
_h323ls._udp.example.com. 86400 IN SRV 10 10 1719 px02.vc.example.com.

_sip._tcp.example.com.    86400 IN SRV 10 10 5060 px01.vc.example.com.
_sip._tcp.example.com.    86400 IN SRV 10 10 5060 px02.vc.example.com.

_sips._tcp.example.com.   86400 IN SRV 10 10 5061 px01.vc.example.com.
_sips._tcp.example.com.   86400 IN SRV 10 10 5061 px02.vc.example.com.
```

```
_pexapp._tcp.example.com. 86400 IN SRV 10 100 443 px01.vc.example.com.
_pexapp._tcp.example.com. 86400 IN SRV 20 100 443 px02.vc.example.com.
```

Note that before configuring these DNS records you should check that there are no other example.com records already configured that are routing such calls elsewhere. (You can use the tool at http://dns.pexip.com to lookup and check SRV records for a domain.)

You then need to configure appropriate Virtual Reception and/or Call Routing Rules on your Pexip Infinity system that will route those calls (placed to @example.com) onwards to the SfB/Lync server. See Using Pexip Infinity as a Skype for Business gateway for more information.

**Federation for the Pexip Infinity subdomain (vc.example.com)**




To enable federation for SfB/Lync clients that want to connect to internal VTC systems (e.g. calls placed to alias@vc.example.com) through your Pexip Conferencing Nodes in the public DMZ, you need a federation DNS SRV record for your Pexip Infinity subdomain.

The **_sipfederationtls._tcp.vc.example.com** DNS SRV and associated round-robin A-records shown below will route calls from federated SfB/Lync clients that are placed to the Pexip Infinity subdomain (@vc.example.com) to your Pexip Conferencing Nodes in the public DMZ (using the pool hostname px.vc.example.com):

```
_sipfederationtls._tcp.vc.example.com. 86400 IN SRV 1 100 5061 px.vc.example.com.
px.vc.example.com.                     86400 IN A 198.51.100.40
px.vc.example.com.                     86400 IN A 198.51.100.41
```

Note that these A-records specified for the **px.vc.example.com** pool 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.

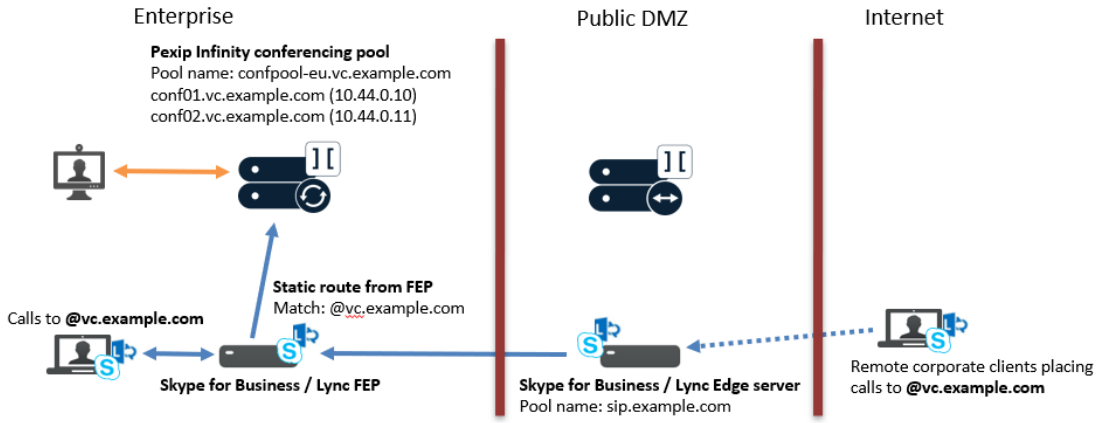
In addition, the following public DNS SRV records will route calls from H.323 devices, SIP devices and Infinity Connect clients (via the _pexapp SRV record) placed to your **@vc.example.com** subdomain to your Pexip Conferencing Nodes in the public DMZ:

```
_h323cs._tcp.vc.example.com. 86400 IN SRV 10 10 1720 px01.vc.example.com.
_h323cs._tcp.vc.example.com. 86400 IN SRV 10 10 1720 px02.vc.example.com.

_h323ls._udp.vc.example.com. 86400 IN SRV 10 10 1719 px01.vc.example.com.
_h323ls._udp.vc.example.com. 86400 IN SRV 10 10 1719 px02.vc.example.com.

_sip._tcp.vc.example.com.    86400 IN SRV 10 10 5060 px01.vc.example.com.
_sip._tcp.vc.example.com.    86400 IN SRV 10 10 5060 px02.vc.example.com.

_sips._tcp.vc.example.com.   86400 IN SRV 10 10 5061 px01.vc.example.com.
_sips._tcp.vc.example.com.   86400 IN SRV 10 10 5061 px02.vc.example.com.

_pexapp._tcp.vc.example.com. 86400 IN SRV 10 100 443 px01.vc.example.com.
_pexapp._tcp.vc.example.com. 86400 IN SRV 20 100 443 px02.vc.example.com.
```

## Local DNS requirements for on-premises SfB/Lync and VTCs

This section shows example local DNS records to enable on-premises SfB/Lync and VTC systems to integrate with Pexip Infinity.

### Internal and remote corporate SfB/Lync routing to VTC systems




In our example deployment, remote corporate and on-premises SfB/Lync clients can call VTC systems by calling <alias>@vc.example.com.

Even though vc.example.com is not the SfB/Lync domain, as these are corporate clients the call is always routed to the SfB/Lync server, and that server is configured with a static route to direct any calls placed to @vc.example.com to the application pool of Conferencing Nodes.

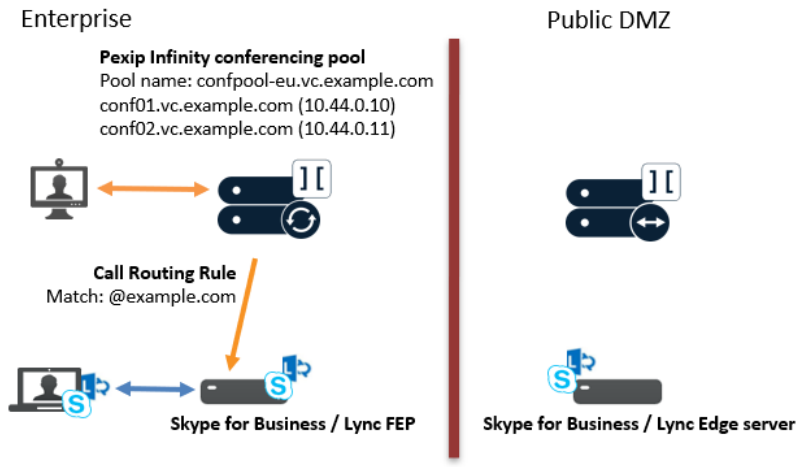
In DNS, ensure that the following records are configured:

- An A-record for each Conferencing Node. In our example this is 2 records with host names of **conf01** and **conf02**, and they each point to the individual IP address of the node.
- Another A-record per Conferencing Node. This time the host name of every record should be **confpool-eu.vc.example.com** (the application pool name of the Conferencing Nodes), and again associate it with the IP address of each Conferencing Node. This step is not required for Skype for Business servers, but is necessary for Lync servers as it allows Lync to spread the traffic across all of the Conferencing Nodes.

For example (change the IP addresses as appropriate for your actual deployment):

```
conf01.vc.example.com.          86400 IN A 10.44.0.10
conf02.vc.example.com.          86400 IN A 10.44.0.11
confpool-eu.vc.example.com.     86400 IN A 10.44.0.10  (only required for Lync deployments)
confpool-eu.vc.example.com.     86400 IN A 10.44.0.11  (only required for Lync deployments)
```

### Internal VTC systems routing to SfB/Lync




In our example deployment, on-premises VTC systems and Infinity Connect clients can call SfB/Lync clients or join SfB/Lync meetings via Pexip Infinity by calling <user/meeting_ID>@example.com.

To route those calls to SfB/Lync, Pexip Infinity must be configured with suitable Call Routing Rules (see Using Pexip Infinity as a Skype for Business gateway for more information).

In these examples, the local DNS records to support H.323 and SIP endpoints, and Infinity Connect clients that dial **@example.com** i.e. calls to SfB/Lync clients and meetings, would be:

```
_h323cs._tcp.example.com. 86400 IN SRV 10 10 1720 conf01.vc.example.com.
_h323cs._tcp.example.com. 86400 IN SRV 10 10 1720 conf02.vc.example.com.

_h323ls._udp.example.com. 86400 IN SRV 10 10 1719 conf01.vc.example.com.
_h323ls._udp.example.com. 86400 IN SRV 10 10 1719 conf02.vc.example.com.

_sip._tcp.example.com.    86400 IN SRV 10 10 5060 conf01.vc.example.com.
_sip._tcp.example.com.    86400 IN SRV 10 10 5060 conf02.vc.example.com.

_sips._tcp.example.com.   86400 IN SRV 10 10 5061 conf01.vc.example.com.
_sips._tcp.example.com.   86400 IN SRV 10 10 5061 conf02.vc.example.com.

_pexapp._tcp.example.com. 86400 IN SRV 10 10 443  conf01.vc.example.com.
_pexapp._tcp.example.com. 86400 IN SRV 10 10 443  conf02.vc.example.com.

conf01.vc.example.com.    86400 IN A 10.44.0.10
conf02.vc.example.com.    86400 IN A 10.44.0.11
```

In addition, those VTC devices and Infinity Connect clients may also want to call into Pexip Infinity-hosted VMRs or other gatewayed devices with addresses in the form <alias>**@vc.example.com**. The local DNS records to support those calls would be:

```
_h323cs._tcp.vc.example.com. 86400 IN SRV 10 10 1720 conf01.vc.example.com.
_h323cs._tcp.vc.example.com. 86400 IN SRV 10 10 1720 conf02.vc.example.com.

_h323ls._udp.vc.example.com. 86400 IN SRV 10 10 1719 conf01.vc.example.com.
_h323ls._udp.vc.example.com. 86400 IN SRV 10 10 1719 conf02.vc.example.com.

_sip._tcp.vc.example.com.    86400 IN SRV 10 10 5060 conf01.vc.example.com.
_sip._tcp.vc.example.com.    86400 IN SRV 10 10 5060 conf02.vc.example.com.

_sips._tcp.vc.example.com.   86400 IN SRV 10 10 5061 conf01.vc.example.com.
_sips._tcp.vc.example.com.   86400 IN SRV 10 10 5061 conf02.vc.example.com.

_pexapp._tcp.vc.example.com. 86400 IN SRV 10 10 443  conf01.vc.example.com.
_pexapp._tcp.vc.example.com. 86400 IN SRV 10 10 443  conf02.vc.example.com.

conf01.vc.example.com.       86400 IN A 10.44.0.10
conf02.vc.example.com.       86400 IN A 10.44.0.11
```

(The A records for the individual Conferencing Nodes are the same for routing via **@example.com** and via **@vc.example.com**.)

# Example public DMZ / hybrid deployment

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

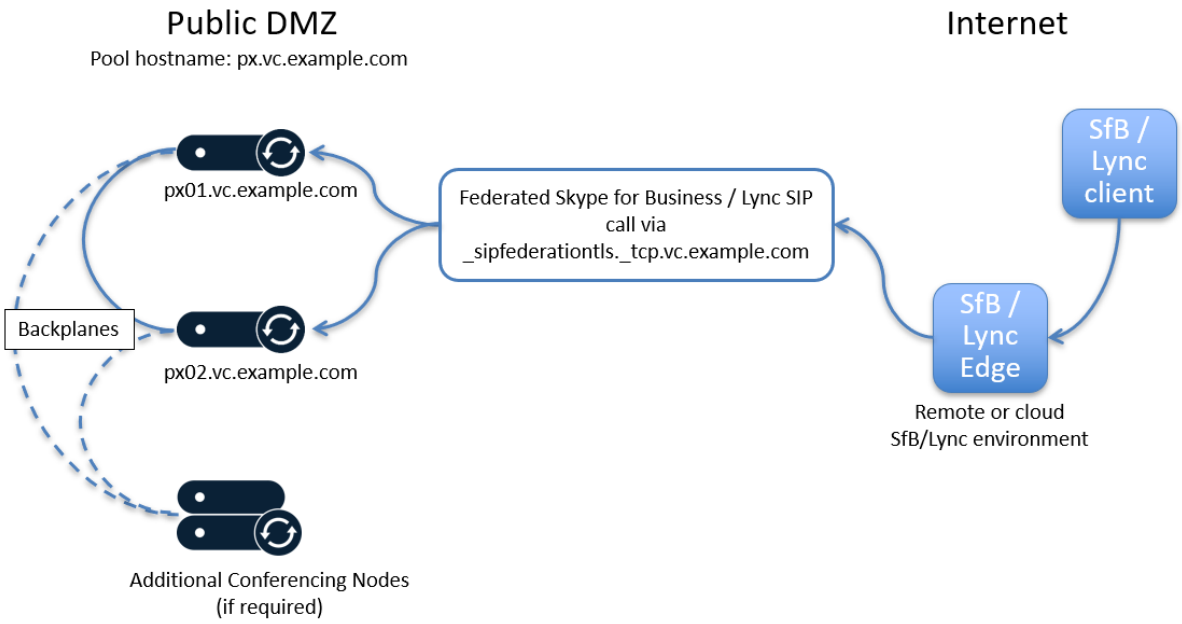
You should follow these public DMZ guidelines for a hybrid deployment of on-premises and Office 365 where SfB/Lync users may be homed in either environment.

## Deployment requirements

For integrating Pexip directly with remote SfB/Lync 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 SfB/Lync client is considered an outbound call, even if the SfB/Lync client had dialed in to the conference, as RDP is a separately initiated SIP session.
- The SfB/Lync 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***

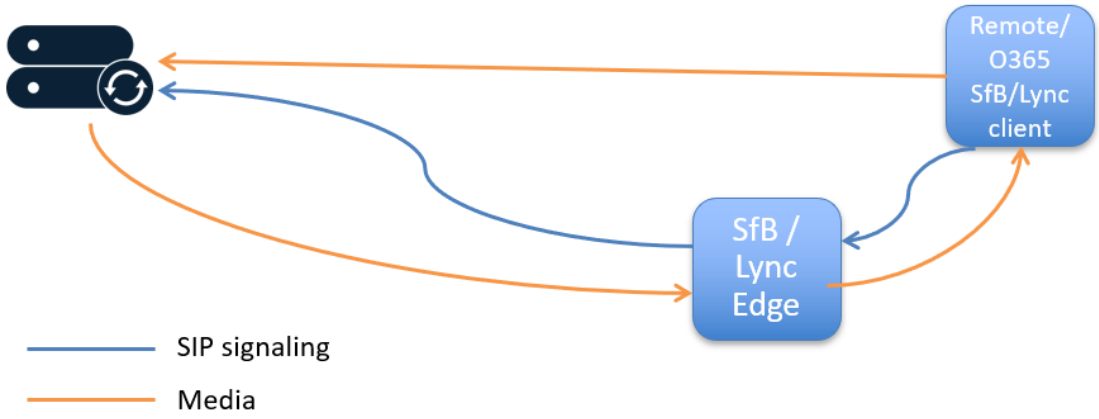
The diagram above shows the example deployment which forms the basis of the public DMZ deployment in this guide. In this scenario, all Conferencing Nodes are deployed in a public DMZ network. Two Conferencing Nodes are configured to receive incoming calls (handle the SIP signaling). Additional Conferencing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

Those Pexip nodes may be Transcoding Conferencing Nodes, or in large deployments you could use dedicated Proxying Edge Nodes to manage the signaling and media connections with the SfB/Lync clients (or any other endpoints).

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 external or Office 365-hosted SfB/Lync clients. Since media negotiation between Pexip Infinity and SfB/Lync 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 / hybrid deployments

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

- px01.vc.example.com
- px02.vc.example.com

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. These nodes may be Transcoding Conferencing Nodes (and optionally with additional overflow Transcoding Conferencing Nodes — px03.vc.example.com, px04.vc.example.com and so on — for extra capacity), or you could deploy px01 and px02 as Proxying Edge Nodes in front of a pool of Transcoding Conferencing Nodes.

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 SfB/Lync 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, **vc.example.com**.
5. Create a SfB/Lync federation DNS SRV record and its associated A-records for the SIP domain **vc.example.com** (which will use the **px.vc.example.com** hostname and round-robin DNS to refer to the 2 Conferencing Nodes).
6. Ensure that SfB/Lync 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 SfB/Lync 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.

#### Hybrid deployments

You should follow these public DMZ guidelines for a hybrid deployment of on-premises and Office 365 where SfB/Lync users may be homed in either environment. Currently Microsoft does not support Trusted Application routing from an Office 365 tenant which is part of a hybrid deployment. Therefore, our recommended approach for a hybrid deployment is to **only** use federation, which is explained in this section. In this scenario, all users route to Pexip Infinity via the SfB/Lync federation DNS SRV record.

## Planning DNS names for your environment

In this example environment, the subdomain **vc.example.com** is used as the SIP domain and is used in all of the configuration examples. Use this as a model for your deployment, adapting the naming patterns as appropriate for your own environment.

You can use your main domain (such as **example.com**) for your Pexip environment, but If that domain is already in use by Office365 (you will typically have the **sip.example.com** hostname associated with that environment), then — to avoid any conflicts — you must use a subdomain for your Pexip environment i.e. **<subdomain>.example.com**.

See Certificate and DNS examples for public DMZ / hybrid integrations for more information about synchronizing your DNS records and certificate names.

## Assigning publicly-issued TLS server certificates to Conferencing Nodes

To enable a Pexip Infinity public DMZ deployment to receive incoming SfB/Lync calls from federated peers, one or more of the Conferencing Nodes (**px01.vc.example.com** and **px02.vc.example.com** in our example) in the public DMZ must be configured with a publicly-issued TLS server certificate. This ensures that remote SfB/Lync 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 (or in any overflow locations).

However, if outbound Pexip Infinity to SfB/Lync 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 SfB/Lync 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 target hostname referenced by the _sipfederationtls._tcp SRV record (the pool name of the Conferencing Nodes).

  In our examples, if the DNS SRV record is:

  ```
  _sipfederationtls._tcp.vc.example.com. 86400 IN SRV 1 100 5061 px.vc.example.com.
  ```

  then the Subject name must be **px.vc.example.com**
- The Subject Alternative Name (altNames attribute) entries must include:
  - the target hostname referenced in the Subject name
  - the FQDNs of all of the public DMZ nodes that are involved in call signaling
  - the domain names that are used in any DNS SRV records that route calls to those Conferencing Nodes (e.g. **vc.example.com** from the example **_sipfederationtls** SRV record above).
- Assign the same certificate to all of the public DMZ nodes that are involved in call signaling.

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 = px.vc.example.com
altNames = px.vc.example.com, px01.vc.example.com, px02.vc.example.com, vc.example.com
```

- See Certificate creation and requirements for more information about creating certificate signing requests.
- See Certificate and DNS examples for public DMZ / hybrid integrations for more information about synchronizing your DNS records and certificate names.

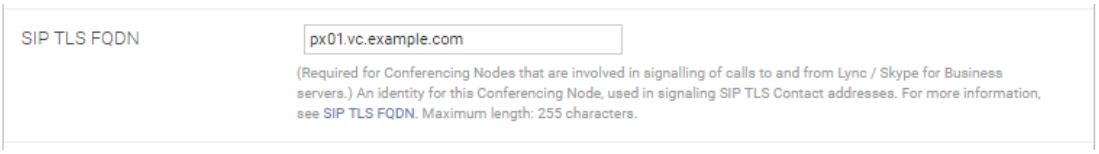
To assign a server certificate and private key to one or more Conferencing Nodes:

1. From the Management Node, go to **Platform > 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. **px01.vc.example.com** and **px02.vc.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 > 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 > Conferencing Nodes**, choosing each Conferencing Node in turn and populating the **SIP TLS FQDN** field:



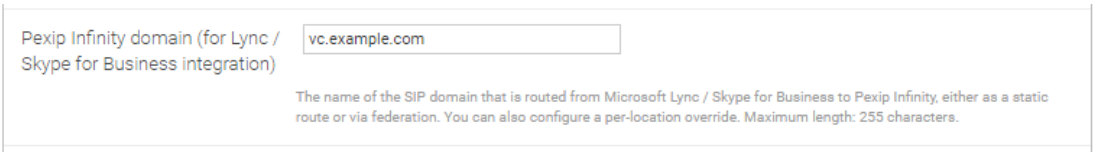

The example above shows that the **SIP TLS FQDN** for the **px01.vc.example.com** Conferencing Node has been set to **px01.vc.example.com**. This FQDN has to match one of the Subject Alternative Names in the certificate installed on the Conferencing Node. You must do this for each Conferencing Node that supports inbound calling (those that are referenced by the px.vc.example.com round-robin DNS A-records, which in our example also includes the **px02.vc.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 SfB/Lync to Pexip Infinity for this deployment. This domain is inserted into the From header in outbound calls from Pexip Infinity to SfB/Lync, and ensures that SfB/Lync can route messages back to Pexip Infinity when, for example, initiating content sharing.

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




Typically this will be set to the same SIP domain/subdomain as used elsewhere in the Pexip deployment, which is **vc.example.com** in this case.

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

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

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

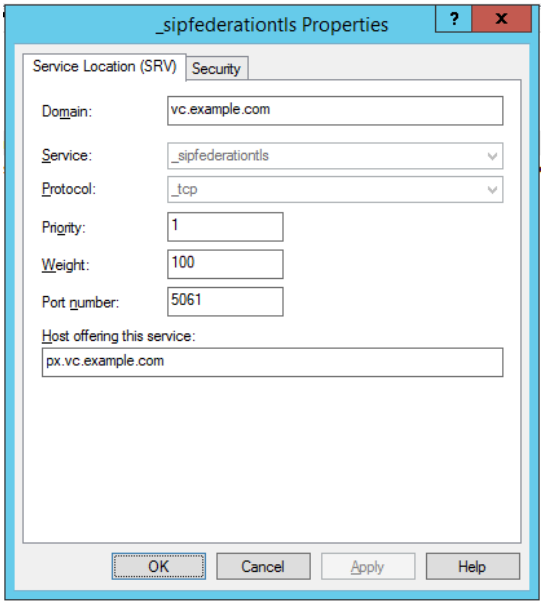
The DNS SRV record should:

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

The domain name used in the **_sipfederationtls._tcp.<domain>** SRV record has to match the domain in the corresponding A-record. This is required due to the trust model for SfB/Lync federation. For example:

- An SRV record such as _sipfederationtls._tcp.**vc.example.com** must have a corresponding A-record with the same domain, such as px.**vc.example.com**.
- You cannot, for example, configure the _sipfederationtls._tcp.vc.example.com SRV record to point to px.**video.example.com** or px01.**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 **px.vc.example.com** in our case).

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

| Hostname | Host IP address |
|---|---|
| px.vc.example.com. | 198.51.100.40 |
| px.vc.example.com. | 198.51.100.41 |

Even if you only intend initially to use a single Conferencing Node to receive incoming SfB/Lync calls, this pool-based approach allows you to easily add more nodes in the future. (In your actual deployment, the hostnames (including the pool hostname) and host IP addresses should be changed to use the real hostnames and IP addresses of your Conferencing Nodes.)

Note that these A-records specified for the **px.vc.example.com** pool 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 |
|---|---|
| px01.vc.example.com. | 198.51.100.40 |
| px02.vc.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.

In these examples, the DNS records would be:

```
_sipfederationtls._tcp.vc.example.com. 86400 IN SRV 1 100 5061 px.vc.example.com.
px.vc.example.com.                     86400 IN A 198.51.100.40
px.vc.example.com.                     86400 IN A 198.51.100.41
px01.vc.example.com.                   86400 IN A 198.51.100.40
px02.vc.example.com.                   86400 IN A 198.51.100.41
```

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

Note that:

- The remote SfB/Lync environment must be configured to allow SfB/Lync federation towards the **vc.example.com** domain.
- To make an outbound call to another SfB/Lync user in a remote SfB/Lync 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 Skype for Business / Lync servers are not associated with a location

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

1. Go to **Platform > 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 SfB/Lync 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. px03.vc.example.com.
- Configure the new Conferencing Node's **SIP TLS FQDN** setting to reflect its DNS FQDN e.g. px03.vc.example.com.
- Add a DNS A-record for the new hostname e.g.

  ```
  px03.vc.example.com.       86400 IN A 198.51.100.42
  ```

It is not necessary to create a new round robin DNS A-record for your Conferencing Node pool (**px.vc.example.com** in our case) 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.

# Certificate and DNS examples for public DMZ / hybrid integrations

This topic contains example Conferencing Node naming patterns, certificate, and DNS requirements for enabling direct federation with remote Skype for Business / Lync environments. It also includes the DNS requirements for B2B federation with remote VTC systems.

You can use these examples as the basis for your own integration, changing the example domain and DNS names as appropriate for your particular environment.

## Common rules for all example scenarios

These examples show different naming scenarios for your Pexip Infinity environment that illustrate the relationships between node hostnames, the certificates on those nodes and their associated DNS requirements:

- Example 1: B2B and SfB/Lync federation to vc.example.com (VTC subdomain)
- Example 2: B2B and SfB/Lync federation to companyname.vc (alternative main domain)

### Common naming and certificate rules

Each pool of Conferencing Nodes that are handling the signaling for a domain/subdomain must be dedicated to that domain/subdomain. Thus, if you want to support multiple domains/subdomains, you must have multiple pools of Conferencing Nodes. In our examples this would be one pool of nodes to handle the signaling for the **vc.example.com** subdomain, and a separate pool of nodes to handle the signaling for **companyname.vc**. However, each pool of nodes can share and make use of a common overflow location of Transcoding Conferencing Nodes (see Shared overflow/transcoding resources for more information).

In all of these scenarios, for all of your Conferencing Nodes in the public DMZ that are involved in call signaling:

- The **SIP TLS FQDN** setting on each Conferencing Node **must** match the node's DNS FQDN and it must be unique per node. For example, if the node's DNS FQDN is **px01.vc.example.com** then its **SIP TLS FQDN** setting must also be **px01.vc.example.com**.
- The certificate on each Conferencing Node **must** include the hostname referenced by the _sipfederationtls._tcp SRV record that points to those nodes, plus the names of all of the Conferencing Nodes that are involved in call signaling:
  - The Subject name (commonName attribute) should be set to the target hostname referenced by the _sipfederationtls._tcp SRV record (the pool name of the Conferencing Nodes).

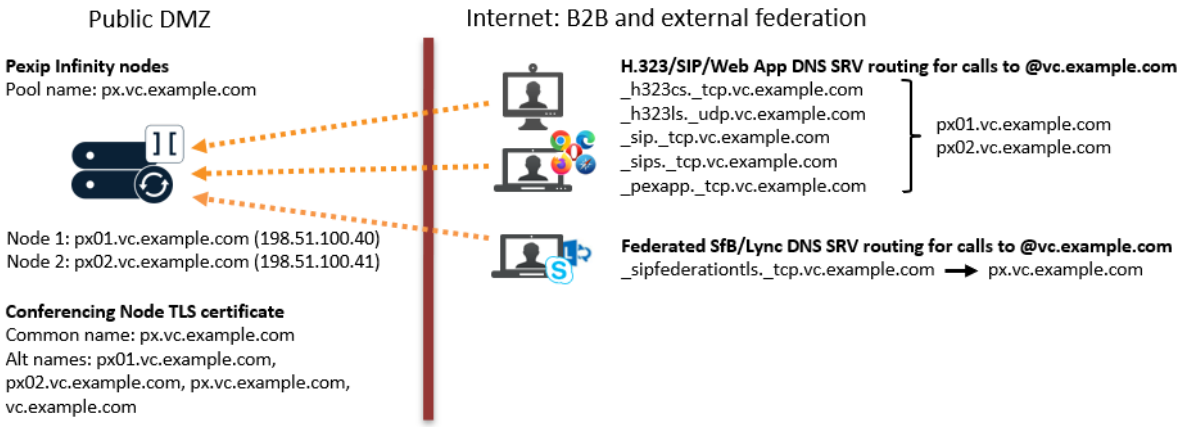
    In our examples, if the DNS SRV record is:

    ```
    _sipfederationtls._tcp.vc.example.com. 86400 IN SRV 1 100 5061 px.vc.example.com.
    ```

    then the Subject name must be **px.vc.example.com**
  - The Subject Alternative Name (altNames attribute) entries must include:
    - the target hostname referenced in the Subject name
    - the FQDNs of all of the public DMZ nodes that are involved in call signaling
    - the domain names that are used in any DNS SRV records that route calls to those Conferencing Nodes (e.g. **vc.example.com** from the example **_sipfederationtls** SRV record above).
  - Assign the same certificate to all of the public DMZ nodes that are involved in call signaling.
- The domain name used in the **_sipfederationtls._tcp.<domain>** SRV record has to match the domain in the corresponding A-record. This is required due to the trust model for SfB/Lync federation. For example:
  - An SRV record such as _sipfederationtls._tcp.**vc.example.com** must have a corresponding A-record with the same domain, such as px.**vc.example.com**.
  - You cannot, for example, configure the _sipfederationtls._tcp.vc.example.com SRV record to point to px.**video.example.com** or px01.**otherdomain.com**.

## Example 1: B2B and SfB/Lync federation to vc.example.com (VTC subdomain)

This example sets up B2B and SfB/Lync federation to the VTC subdomain of vc.example.com. A subdomain is typically required if the enterprise domain (and sip.<domain>) is already associated with an Office365 environment.




The following **_sipfederationtls._tcp.vc.example.com** DNS SRV and associated round-robin A-records will be utilized by calls from federated SfB/Lync clients that are placed to the vc.example.com Pexip domain. The DNS records will route the call to your Pexip Conferencing Nodes in the public DMZ (using the pool hostname px.vc.example.com):

```
_sipfederationtls._tcp.vc.example.com. 86400 IN SRV 1 100 5061 px.vc.example.com.
px.vc.example.com.                     86400 IN A 198.51.100.40
px.vc.example.com.                     86400 IN A 198.51.100.41
```

Note that these A-records specified for the **px.vc.example.com** pool 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:

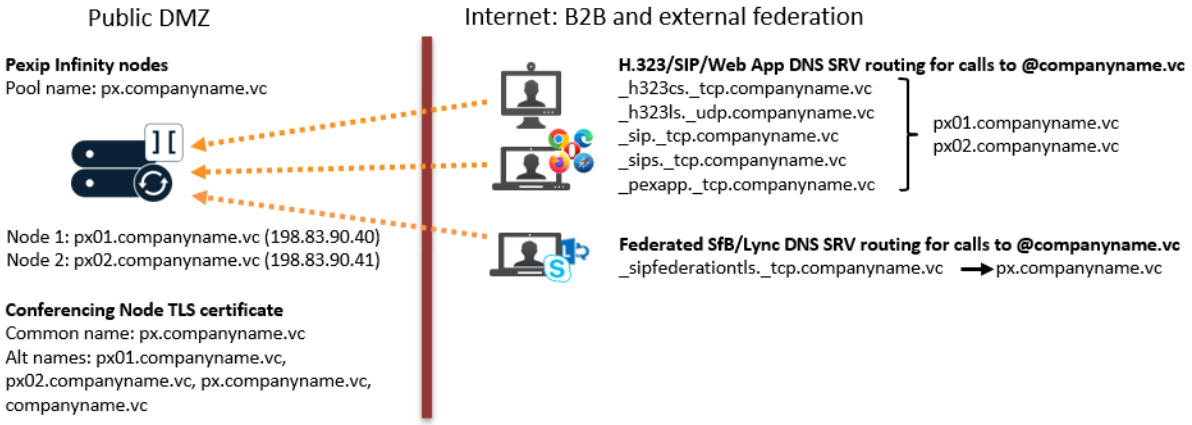
```
px01.vc.example.com.        86400 IN A 198.51.100.40
px02.vc.example.com.        86400 IN A 198.51.100.41
```

In addition, the following DNS SRV records will route calls from H.323 devices, SIP devices and Infinity Connect clients (via the _pexapp SRV record) placed to the @vc.example.com subdomain to your Pexip Conferencing Nodes in the public DMZ:

```
_h323cs._tcp.vc.example.com. 86400 IN SRV 10 10 1720 px01.vc.example.com.
_h323cs._tcp.vc.example.com. 86400 IN SRV 10 10 1720 px02.vc.example.com.

_h323ls._udp.vc.example.com. 86400 IN SRV 10 10 1719 px01.vc.example.com.
_h323ls._udp.vc.example.com. 86400 IN SRV 10 10 1719 px02.vc.example.com.

_sip._tcp.vc.example.com.    86400 IN SRV 10 10 5060 px01.vc.example.com.
_sip._tcp.vc.example.com.    86400 IN SRV 10 10 5060 px02.vc.example.com.

_sips._tcp.vc.example.com.   86400 IN SRV 10 10 5061 px01.vc.example.com.
_sips._tcp.vc.example.com.   86400 IN SRV 10 10 5061 px02.vc.example.com.

_pexapp._tcp.vc.example.com. 86400 IN SRV 10 100 443 px01.vc.example.com.
_pexapp._tcp.vc.example.com. 86400 IN SRV 20 100 443 px02.vc.example.com.
```

## Example 2: B2B and SfB/Lync federation to companyname.vc (alternative main domain)

This example shows how to enable B2B and SfB/Lync federation to a different top-level enterprise domain — companyname.vc in this case.




The following **_sipfederationtls._tcp.companyname.vc** DNS SRV and associated round-robin A-records will be utilized by calls from federated SfB/Lync clients that are placed to the companyname.vc Pexip domain. The DNS records will route the call to your Pexip Conferencing Nodes in the public DMZ (using the pool hostname px.companyname.vc):

```
_sipfederationtls._tcp.companyname.vc. 86400 IN SRV 1 100 5061 px.companyname.vc.
px.companyname.vc.                     86400 IN A 198.83.90.40
px.companyname.vc.                     86400 IN A 198.83.90.41
```

Note that these A-records specified for the **px.companyname.vc** pool 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:

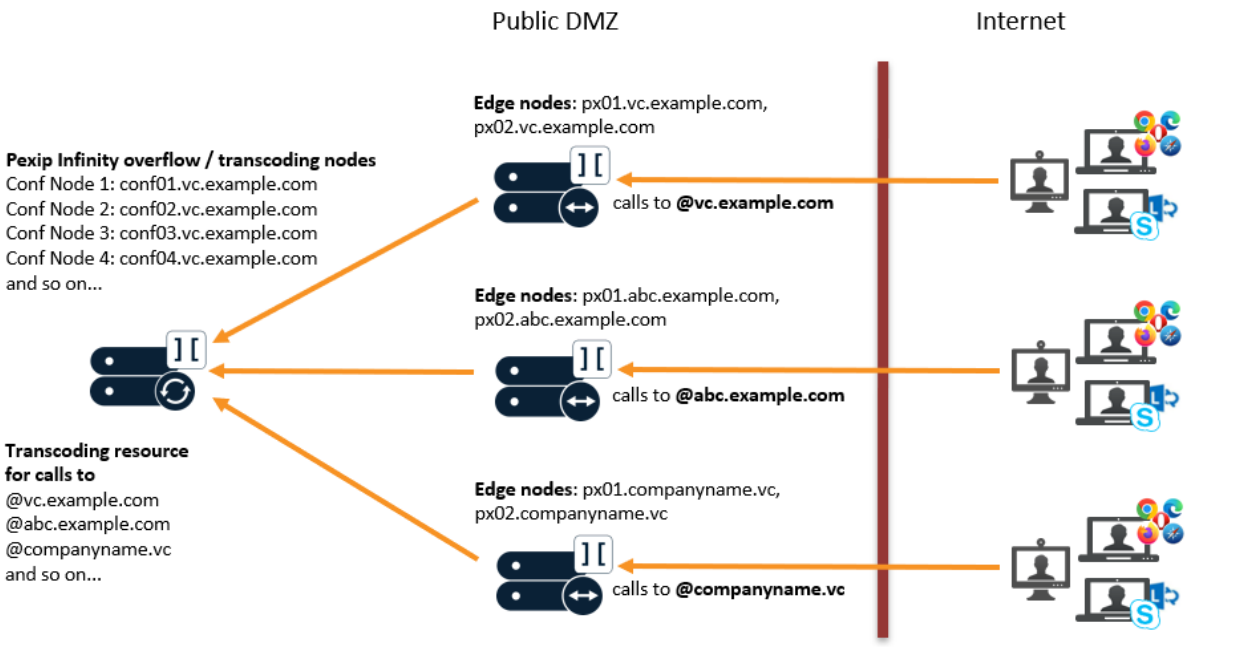
```
px01.companyname.vc.        86400 IN A 198.83.90.40
px02.companyname.vc.        86400 IN A 198.83.90.41
```

In addition, the following DNS SRV records will route calls from H.323 devices, SIP devices and Infinity Connect clients (via the _pexapp SRV record) placed to the @companyname.vc domain to your Pexip Conferencing Nodes in the public DMZ:

```
_h323cs._tcp.companyname.vc. 86400 IN SRV 10 10 1720 px01.companyname.vc.
_h323cs._tcp.companyname.vc. 86400 IN SRV 10 10 1720 px02.companyname.vc.

_h323ls._udp.companyname.vc. 86400 IN SRV 10 10 1719 px01.companyname.vc.
_h323ls._udp.companyname.vc. 86400 IN SRV 10 10 1719 px02.companyname.vc.

_sip._tcp.companyname.vc.    86400 IN SRV 10 10 5060 px01.companyname.vc.
_sip._tcp.companyname.vc.    86400 IN SRV 10 10 5060 px02.companyname.vc.

_sips._tcp.companyname.vc.   86400 IN SRV 10 10 5061 px01.companyname.vc.
_sips._tcp.companyname.vc.   86400 IN SRV 10 10 5061 px02.companyname.vc.

_pexapp._tcp.companyname.vc. 86400 IN SRV 10 100 443 px01.companyname.vc.
_pexapp._tcp.companyname.vc. 86400 IN SRV 20 100 443 px02.companyname.vc.
```

## Shared overflow/transcoding resources

While each pool of Conferencing Nodes that are handling the signaling for a domain/subdomain must be dedicated to that domain/subdomain, all of those pools can share and make use of a common overflow pool of Transcoding Conferencing Nodes. The following example shows how a common pool of transcoding resources can be used to handle calls for multiple domains — vc.example.com, abc.example.com and companyname.vc in this case.




The Edge nodes (that are handling the signaling connection with the devices for calls to their respective domain/subdomain):

- must have appropriate certificates installed for the domain/subdomain they are handling for federated SfB/Lync clients (as described above).
- must have appropriate associated DNS records to route calls for their respective domain/subdomain to those nodes (as described above).
- they can be Proxying Edge Nodes (and so all media transcoding is forwarded to the overflow nodes).
- or they can be Transcoding Conferencing Nodes (and thus media transcoding is only performed on nodes in the overflow location when the Edge nodes are at capacity).

The Transcoding Conferencing Nodes in the overflow location (providing they are not receiving any call signaling):

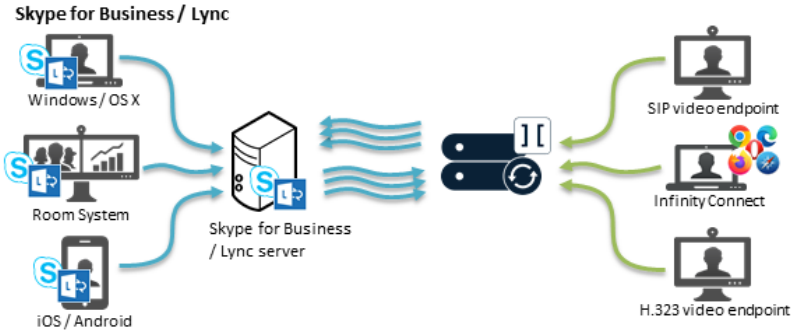
- do not require certificates to be installed.
- do not require associated DNS records.

This means that even if you need to handle calls from multiple domains, you can provide a large, common pool of shared transcoding resources and easily add more Transcoding Conferencing Node resources as and when required (including dynamic bursting to a cloud service if required).

# Using Pexip Infinity as a Skype for Business gateway

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

- invite H.323/SIP endpoints and registered Infinity Connect clients into a SfB/Lync meeting via manual dialout or drag and drop from the contacts list
- use the Infinity Gateway to route incoming calls directly into an ad hoc or scheduled SfB/Lync meeting
- when dialed into a Pexip VMR conference, invite other SfB/Lync or external contacts into that same Pexip VMR (this creates a new SfB/Lync meeting which is merged with the existing Pexip VMR)




- receive and initiate person-to-person calls with standards-based devices, and then optionally add other participants (to escalate to a multipoint SfB meeting).

## Using the Infinity Gateway

The Infinity 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 Virtual Meeting Room, Virtual Auditorium, Virtual Reception, scheduled conference, Media Playback Service, 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 Infinity Gateway call to the destination alias according to the rule's call target settings (which protocol, location 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 a Virtual Meeting Room, Virtual Auditorium, Virtual Reception, scheduled conference, Media Playback Service, or Test Call Service.

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

Select Call Routing Rule to change

Action: ------ Go 0 of 3 selected Enter search here Search

| Priority | Name | Description | Incoming | Outgoing | Call location | Registered only | Connect | SIP | Lync/SfB H323 | 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 SfB meeting | | ✓ | ✗ | Any Location | ✗ | ✓ | ✓ | ✗ | ✓ | 88(\d{5,7})@example\.com | \1 | Lync/SfB meeting direct (Conference ID in dialed alias) | 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 Skype for Business / Lync to dial out to other devices via the gateway

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

To configure the rule:

1. Go to **Services > 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)<br>Match SIP<br>Match Lync / Skype for Business (MS-SIP)<br>Match H.323 | Select **Match Lync / Skype for Business (MS-SIP)** and leave the other protocols unselected.<br>(This rule is only handling call requests received from the SfB/Lync environment.) |
| Match against full alias URI | Leave unselected. |
| Destination alias regex match | Enter a regular expression that will match the calls received from the SfB/Lync environment. For example, to match any alias in the vc.example.com domain:<br>**.+@vc.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 outbound call. If you do not need to change the alias, leave this field blank. |
| Call target | Select either ***Registered device or external system*** or ***Registered devices only***, or an external platform such as ***Google Meet meeting***, depending upon your requirements. |
| Protocol | The protocol used to place the outgoing call. This will be either ***SIP*** or ***H.323***.<br>If you want to place the call over both ***SIP*** and ***H.323***, you will need to create 2 rules, one per protocol.<br>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** Route calls from Lync / Skype for Business *
The name used to refer to this Call Routing Rule. Maximum length: 250 characters.

Service tag
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
A description of the Call Routing Rule. Maximum length: 250 characters.

**Priority** 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 ☑
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 ☐
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 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 ☐
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) ☐
Select whether this rule should apply to incoming calls from Infinity Connect clients (WebRTC / RTMP).

Match SIP ☐
Select whether this rule should apply to incoming SIP calls.

Match Lync / Skype for Business (MS-SIP) ☑
Select whether this rule should apply to incoming Lync / Skype for Business (MS-SIP) calls.

Match H.323 ☐
Select whether this rule should apply to incoming H.323 calls.

**Alias match and transform**

Match against full alias URI ☐
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** .+@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
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)**

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)**

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**: Main video + presentation *

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.

**Maximum call quality**: Use global setting

Sets the maximum call quality for each participant. For more information see Setting and limiting call quality.

**Media encryption**: Use global setting

Controls the media encryption requirements for participants connecting to this service.
**Use global setting**: use the global media encryption setting (Platform > Global Settings).
**Best effort**: each participant will use media encryption if their device supports it, otherwise the connection will be unencrypted.
**Required**: all participants must use media encryption.
**No encryption**: all H.323, SIP and MS-SIP participants must use unencrypted media.

**Theme**: <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.

### Outgoing call placement

**Call target**: Registered device or external system *

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 (Conference ID in dialed alias)**: 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 just 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**: Automatic

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**: SIP *

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**: Use DNS

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.

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

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

To configure the rule:

1. Go to **Services > 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)<br>Match SIP<br>Match Lync / Skype for Business (MS-SIP)<br>Match H.323 | Select one or more of **Match Infinity Connect (WebRTC / RTMP)**, **Match SIP** and **Match H.323** as appropriate.<br>(Do not select **Match Lync / Skype for Business (MS-SIP)** as this rule is only handling call requests received from outside the SfB/Lync environment.) |
| 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 SfB/Lync environment. For example, to match any alias in the example.com domain:<br>**.+@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 SfB/Lync 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 SfB/Lync clients via an external SfB/Lync server). |
| Outgoing location | If required, you can ensure that the outgoing call to SfB/Lync is handled by a Conferencing Node in a specific location.<br>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 SfB/Lync server that you want to use to handle the call, for example ***fepool-eu***. |

3. Select **Save**.

### Add Call Routing Rule

**Name** Route to Lync / Skype for Business clients *
The name used to refer to this Call Routing Rule. Maximum length: 250 characters.

Service tag
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
A description of the Call Routing Rule. Maximum length: 250 characters.

**Priority** 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 ☑
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 ☐
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 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 ☐
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) ☑
Select whether this rule should apply to incoming calls from Infinity Connect clients (WebRTC / RTMP).

Match SIP ☑
Select whether this rule should apply to incoming SIP calls.

Match Lync / Skype for Business (MS-SIP) ☐
Select whether this rule should apply to incoming Lync / Skype for Business (MS-SIP) calls.

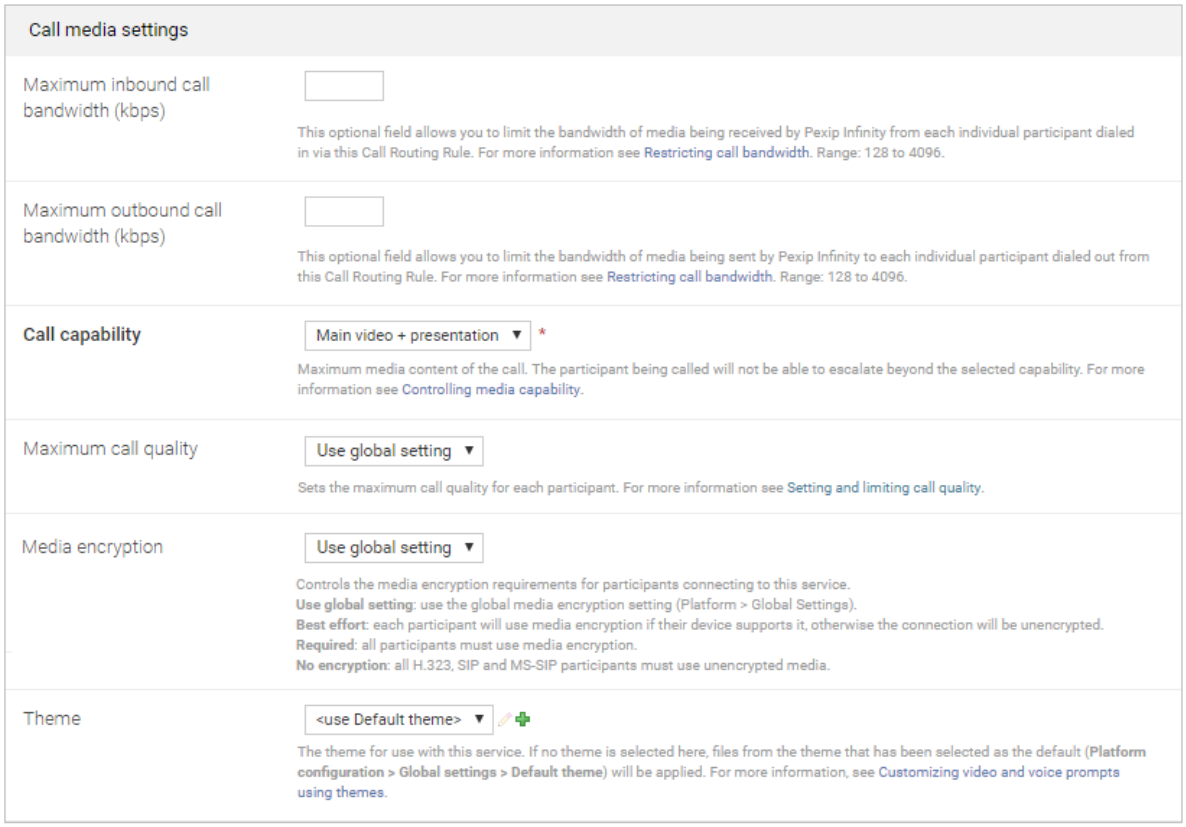
Match H.323 ☑
Select whether this rule should apply to incoming H.323 calls.

**Alias match and transform**

Match against full alias URI ☐
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** .+@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
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)

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)

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**: Main video + presentation *

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.

Maximum call quality: Use global setting

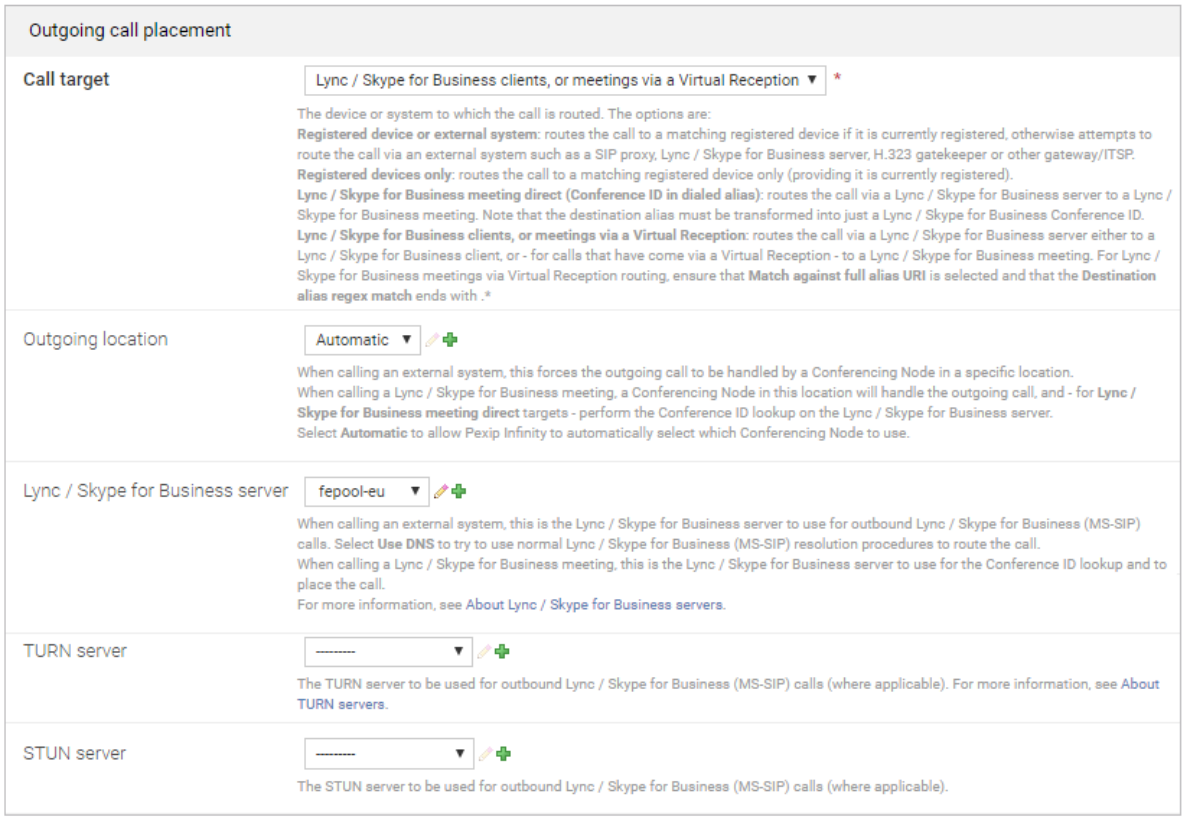
Sets the maximum call quality for each participant. For more information see Setting and limiting call quality.

Media encryption: Use global setting

Controls the media encryption requirements for participants connecting to this service.
**Use global setting**: use the global media encryption setting (Platform > Global Settings).
**Best effort**: each participant will use media encryption if their device supports it, otherwise the connection will be unencrypted.
**Required**: all participants must use media encryption.
**No encryption**: all H.323, SIP and MS-SIP participants must use unencrypted media.

Theme: <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.



Outgoing call placement

**Call target**: Lync / Skype for Business clients, or meetings via a Virtual Reception *

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 (Conference ID in dialed alias)**: 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 just 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: Automatic

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.

Lync / Skype for Business server: fepool-eu

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.

TURN server: --------

The TURN server to be used for outbound Lync / Skype for Business (MS-SIP) calls (where applicable). For more information, see About TURN servers.

STUN server: --------

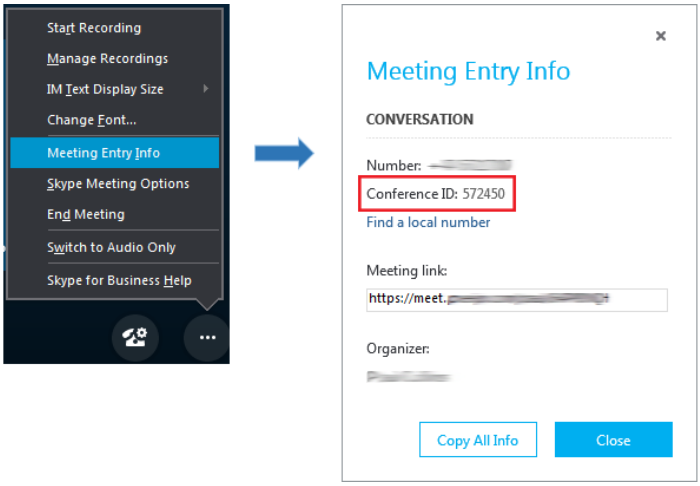
The STUN server to be used for outbound Lync / Skype for Business (MS-SIP) calls (where applicable).

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

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

All calls are routed into the SfB/Lync meetings by means of the SfB/Lync Conference ID that is associated with the SfB/Lync meeting. The SfB/Lync Conference ID is typically a 5-7 digit number. For scheduled meetings it will normally be included in the meeting invitation.

For ad hoc conferences, existing SfB/Lync 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 SfB/Lync IVR gateway or "lobby" by configuring a Virtual Reception to prompt the caller to enter the Conference ID of the required conference, and then use a Call Routing Rule to route the call into the SfB/Lync meeting.
- **Routing directly via the Infinity 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 SfB/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 Infinity Gateway). Also included are some guidelines for SfB/Lync configuration to use Pexip Infinity as a SfB/Lync gateway.

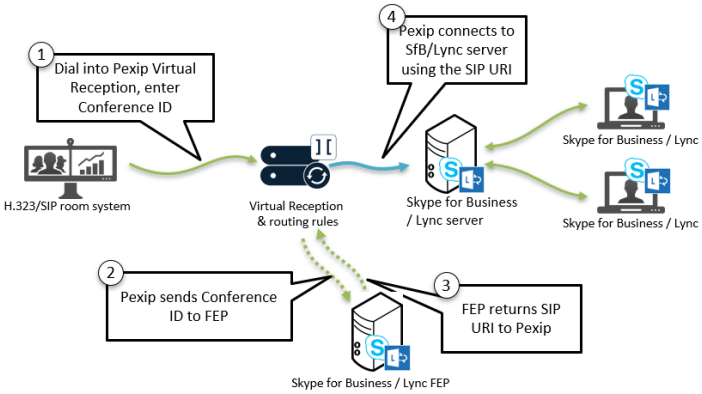
Note that:

- Routing into an ad hoc or scheduled SfB/Lync meeting via its Conference ID is only supported within on-premises SfB/Lync deployments, as the Conferencing Nodes must be trusted applications within the SfB/Lync environment.
- Non-SfB/Lync video callers will see a holding screen until a SfB/Lync client joins the conference with video.
- No indicators or name overlays are included in the external device's video stream that is sent to the SfB/Lync meeting.
- Each participant who is gatewayed via Pexip Infinity into a SfB/Lync meeting consumes two call licenses (one for the inbound leg of the call and one for the outbound leg, as is standard for calls via the Infinity Gateway calls). Any external participants who are connected directly to the SfB/Lync meeting do not consume a license. When viewing the status of the gateway call (**Status > Conferences**), the **Participants** tab also lists the other participants in the conference. Note that only the gatewayed participant is shown as consuming a license. The outbound leg of the gateway call (into the SfB/Lync meeting), which consumes the second license of each gateway call, is not represented in the participant list.

## Routing indirectly via a Virtual Reception (IVR gateway)

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

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



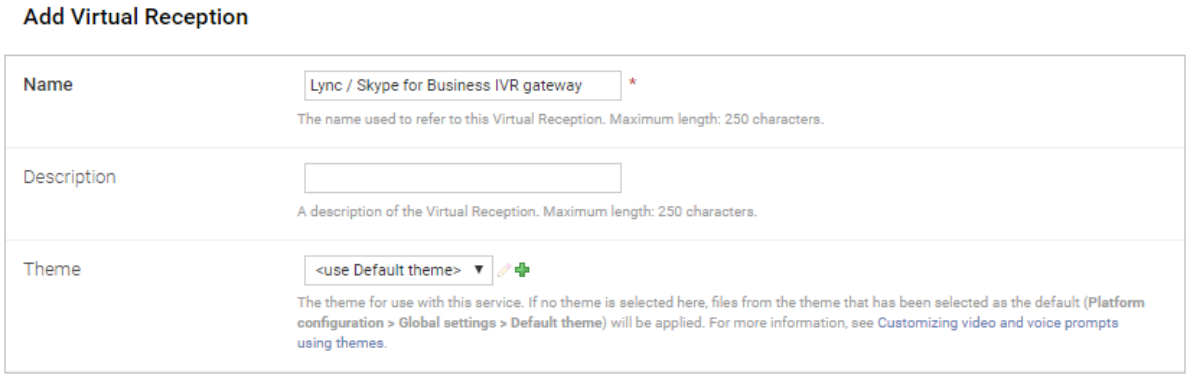

The Virtual Reception requests the caller to enter the SfB/Lync Conference ID (typically a 5-7 digit number) which it then uses to retrieve the full conference URI from the SfB/Lync server. The Infinity Gateway then matches this conference URI and routes the caller to the appropriate SfB/Lync meeting.

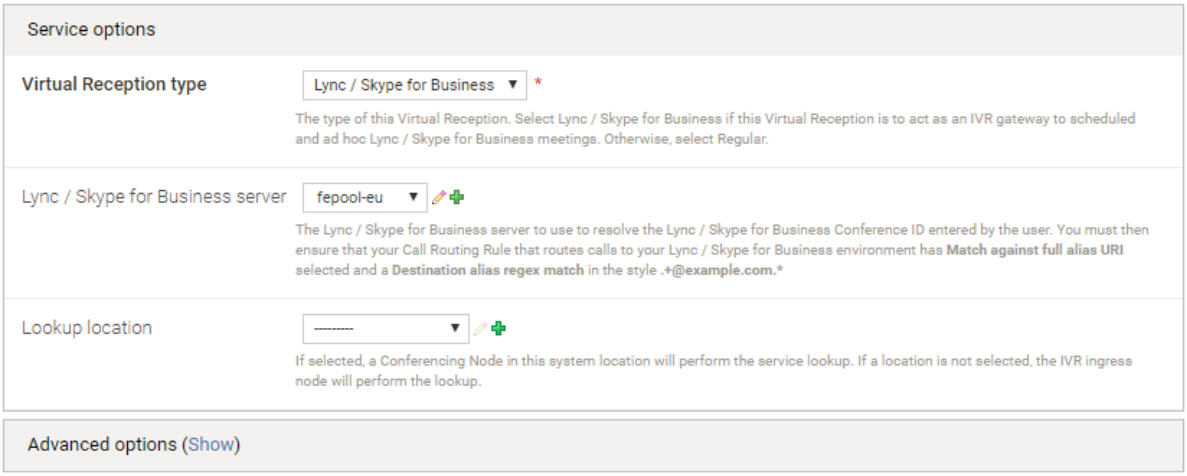
To configure the Virtual Reception:

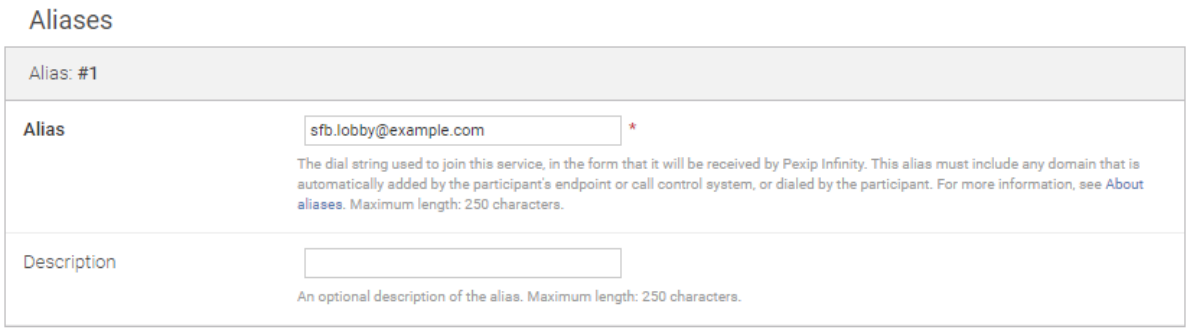
1. Go to **Services > Virtual Receptions** and select **Add Virtual Reception**.
2. Configure the following fields (leave all other fields with default values or as required for your specific deployment):

| Option | Description |
|---|---|
| Name | The name you will use to refer to this Virtual Reception, for example "Skype for Business / Lync IVR gateway". |
| Theme | Optionally, you may want to assign a specific theme to this Virtual Reception to brand it as the gateway to SfB/Lync conferences, for example by customizing the voice prompts. |
| Virtual Reception type | Select ***Lync / Skype for Business***. |
| Lync / Skype for Business server | Select the SfB/Lync server to use to resolve the SfB/Lync Conference ID, for example ***fepool-eu***. |
| Lookup location | You can optionally specify the system location that will perform the SfB/Lync Conference ID lookup on the SfB/Lync server. If a location is not selected, the IVR ingress node will perform the lookup.<br>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 SfB/Lync FEP. This allows you to nominate the location (in which the Conferencing Nodes are trusted by SfB/Lync) to perform the lookup. |
| Alias | Enter the alias that users will dial to use this SfB/Lync gateway Virtual Reception, for example **sfb.lobby@example.com**. |

3. Select **Save**.





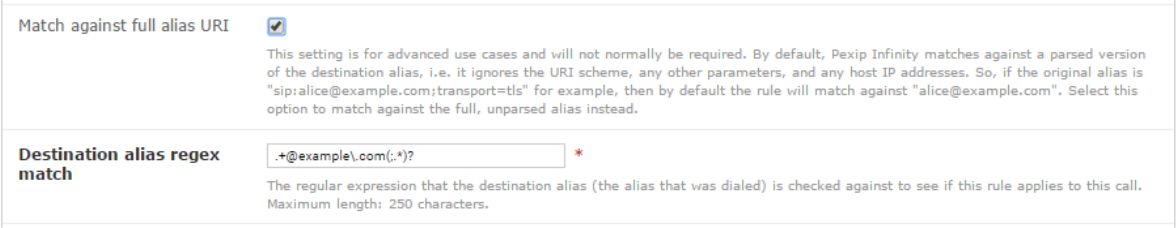




To configure the Call Routing Rule:

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

| Option | Description |
|---|---|
| Match against full alias URI | Select this option.<br>(The alias of the SfB/Lync 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:<br>**.+@example\.com(;.*)?** |

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




### Using the SfB/Lync IVR gateway service

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

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

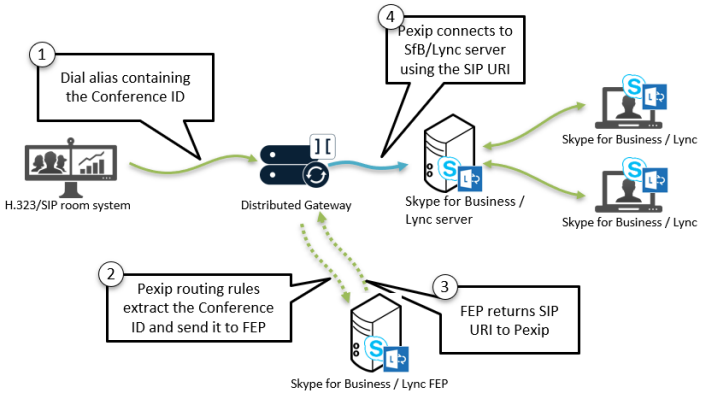
Note that:

- SIP and H.323 endpoints can bypass having to enter the destination alias via DTMF tones. They would do this by including the SfB/Lync 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 **sfb.lobby@example.com** and the SfB/Lync Conference ID is **572450**, then the endpoint can dial **sfb.lobby**572450@example.com** to be transferred directly into the SfB/Lync conference.
- Infinity Connect web app users can also be provided with a preconfigured link URL that, when clicked, will automatically provide the SfB/Lync Conference ID to the Virtual Reception and take the user directly into the SfB/Lync conference. The URL needs to be in the format:
  https://**<address>**/webapp/conference/**<reception_alias>**?name=**<name>**&extension=**<Conference ID>**
  for example **https://vc.example.com/webapp/conference/sfb.lobby@example.com?name=Alice&extension=572450**

## Routing directly via the Infinity Gateway

To route calls to SfB/Lync meetings directly via the Infinity Gateway you need:




- To decide on an alias pattern that participants will dial to access the SfB/Lync meetings. The alias pattern will typically include the SfB/Lync 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 SfB/Lync meeting with a Conference ID of 12345. Note that a prefix is only required if you have a conflicting dial plan on your video conferencing side that could clash with your SfB/Lync Conference IDs.
- A Call Routing Rule that matches that alias pattern and transforms it such that it contains just the SfB/Lync Conference ID which it can then pass on to the target SfB/Lync server.

To configure the rule:

1. Go to **Services > 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)<br>Match SIP<br>Match Lync / Skype for Business (MS-SIP)<br>Match H.323 | Select one or more of **Match Infinity Connect (WebRTC / RTMP)**, **Match SIP** and **Match H.323** as appropriate.<br>(Do not select **Match Lync / Skype for Business (MS-SIP)** as this rule is only handling call requests received from outside the SfB/Lync 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 SfB/Lync meeting. For example, to match any alias in the style of 88<ConferenceID>@example.com you could use:<br>**88(\d{5,7})@example\.com**<br>Note that \d{5,7} which matches the numeric 5-7 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.<br>In our example, to extract the Conference ID from the dialed alias we would use: **\1**<br>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 (Conference ID in dialed alias)***.<br>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 SfB/Lync server so that the call can be routed into the SfB/Lync meeting. |
| Outgoing location | If required, you can ensure that the outgoing call to SfB/Lync 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 SfB/Lync server that you want to use to perform the Conference ID lookup and to handle the call, for example ***fepool-eu***. |

### Add Call Routing Rule

**Name** Route calls to SfB meeting *
The name used to refer to this Call Routing Rule. Maximum length: 250 characters.

Service tag
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
A description of the Call Routing Rule. Maximum length: 250 characters.

**Priority** 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 ☑
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 ☐
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 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 ☐
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) ☑
Select whether this rule should apply to incoming calls from Infinity Connect clients (WebRTC / RTMP).

Match SIP ☑
Select whether this rule should apply to incoming SIP calls.

Match Lync / Skype for Business (MS-SIP) ☐
Select whether this rule should apply to incoming Lync / Skype for Business (MS-SIP) calls.

Match H.323 ☑
Select whether this rule should apply to incoming H.323 calls.

**Alias match and transform**

Match against full alias URI ☐
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** 88(\d{5,7})@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 \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)**

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)**

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**: Main video + presentation *

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.

**Maximum call quality**: Use global setting

Sets the maximum call quality for each participant. For more information see Setting and limiting call quality.

**Media encryption**: Use global setting

Controls the media encryption requirements for participants connecting to this service.
**Use global setting**: use the global media encryption setting (Platform > Global Settings).
**Best effort**: each participant will use media encryption if their device supports it, otherwise the connection will be unencrypted.
**Required**: all participants must use media encryption.
**No encryption**: all H.323, SIP and MS-SIP participants must use unencrypted media.

**Theme**: <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.

### Outgoing call placement

**Call target**: Lync / Skype for Business meeting direct (Conference ID in dialed alias) *

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 (Conference ID in dialed alias)**: 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 just 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**: Automatic

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.

**Lync / Skype for Business server**: fepool-eu

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.

**TURN server**: --------

The TURN server to be used for outbound Lync / Skype for Business (MS-SIP) calls (where applicable). For more information, see About TURN servers.

**STUN server**: --------

The STUN server to be used for outbound Lync / Skype for Business (MS-SIP) calls (where applicable).

### Using the direct SfB/Lync gateway service

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

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

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

To ensure that a numeric SfB/Lync Conference ID is generated, your SfB/Lync 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 SfB/Lync's meeting lobby

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

### 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 SfB/Lync meeting, by default, the SfB/Lync Conference ID lookup is invoked from the ingress node (the same Conferencing Node that is handling the incoming call) and the call to SfB/Lync 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.

### Anonymous (unauthenticated) participant timeout

There is a SfB/Lync setting (**AnonymousUserGracePeriod**) that represents the amount of time an anonymous (unauthenticated) user, such as a gateway participant, can remain in a SfB/Lync meeting without an authenticated user being present in that same meeting. The default value is 90 minutes.

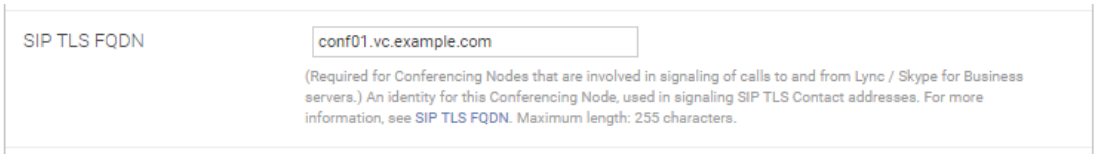
You can check the current value by using the following PowerShell command: `Get-CsUserServicesConfiguration` and you can set the timeout value with: `Set-CsUserServicesConfiguration`

For more information, see https://docs.microsoft.com/en-us/powershell/module/skype/Set-CsUserServicesConfiguration.

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

For any Pexip Infinity and SfB/Lync 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 > Conferencing Nodes**, choosing each node in turn and populating the **SIP TLS FQDN** field.




The example above shows the **SIP TLS FQDN** for the conf01 Conferencing Node, which is set to **conf01.vc.example.com**.

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

# Integrating Pexip Infinity with Office 365 (O365) environments

To deploy Pexip Infinity in a public DMZ and enable direct federation with Office 365 Skype for Business environments, see Pexip Infinity configuration for public DMZ / hybrid deployments.

# 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 Skype for Business and Lync, either as part of an on-prem deployment or when deploying Pexip in a public DMZ for enabling direct federation with remote SfB/Lync environments.

For an on-prem integration between SfB/Lync 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.

We strongly recommend that all Pexip Infinity Conferencing Node certificates should have both "Server Authentication" and "Client Authentication" Enhanced Key Usage properties.

## Creating a certificate signing request (CSR)

The on-prem and public DMZ SfB/Lync 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 SfB/Lync 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 Skype for Business / Lync environments (as per RFC 5922). If you are using SIP or Skype for Business / Lync, 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 target hostname referenced by the _sipfederationtls._tcp SRV record (the pool name of the Conferencing Nodes).

  In our examples, if the DNS SRV record is:

  ```
  _sipfederationtls._tcp.vc.example.com. 86400 IN SRV 1 100 5061 px.vc.example.com.
  ```

  then the Subject name must be **px.vc.example.com**
- The Subject Alternative Name (altNames attribute) entries must include:
  - the target hostname referenced in the Subject name
  - the FQDNs of all of the public DMZ nodes that are involved in call signaling
  - the domain names that are used in any DNS SRV records that route calls to those Conferencing Nodes (e.g. **vc.example.com** from the example **_sipfederationtls** SRV record above).
- Assign the same certificate to all of the public DMZ nodes that are involved in call signaling.

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 (such as **confpool-eu.vc.example.com** in our examples).
- The Subject Alternative Name (altNames attribute) entries must include the Trusted Application Pool FQDN (i.e. a repeat of the Subject name), plus the FQDNs of all of the nodes in the pool that are involved in signaling.
- Assign the same certificate to all of the enterprise nodes that are involved in call signaling.

See Assigning the certificate to 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 | ***User-provided custom Common Name*** | ***User-provided custom Common Name*** |
| Custom subject name | px.vc.example.com | confpool-eu.vc.example.com |
| Subject alternative names | px01.vc.example.com, px02.vc.example.com, vc.example.com (and px.vc.example.com will also be included automatically) | conf01.vc.example.com, conf02.vc.example.com, conf03.vc.example.com (and confpool-eu.vc.example.com will also be included automatically) |

See Certificate and DNS examples for public DMZ / hybrid integrations and Certificate and DNS examples for an on-premises integration for more information.

### 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.

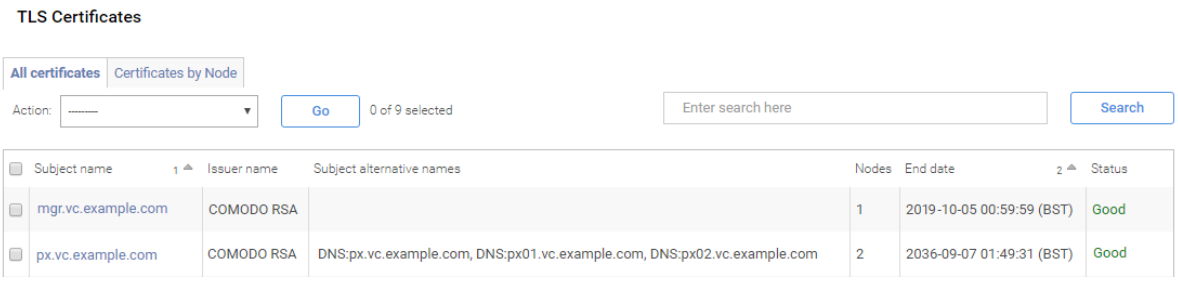
Thus, if for instance you need to add two additional nodes, you can create a new CSR containing the original altNames and the two additional altNames, submit the CSR to the certificate vendor, pay the additional fee (which is usually per SAN entry), get an updated SAN/UC certificate and then upload this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

If you expect to deploy more nodes in the future, and have a predictable naming scheme for your nodes, you can also add extra altNames in anticipation of those future nodes.

## Assigning a certificate to a Conferencing Node

In Pexip Infinity, certificates are managed from the Pexip Infinity Administrator interface under **Platform > 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:



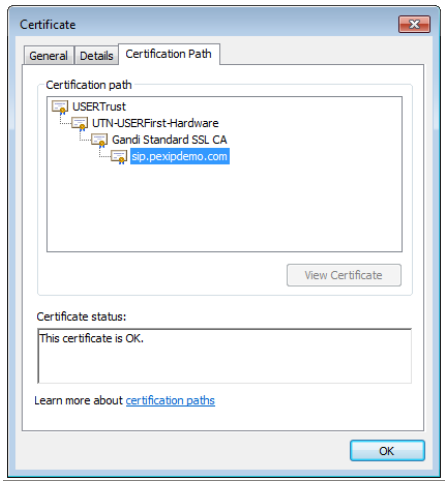

## Certificates issued by intermediate CAs

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 > 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:



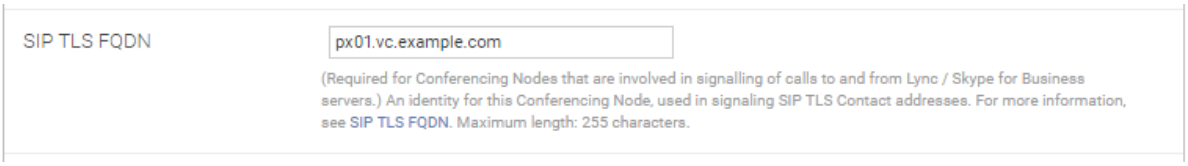

In this particular case, **UTN-USERFirst-Hardware** and **Gandi Standard SSL CA** are the intermediate Certificate Authorities for the **sip.pexipdemo.com** certificate. This means that we would have to bundle together these two CA certificates in a text file and upload it using the **Import** trusted 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 > 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 **px.vc.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 (**px01.vc.example.com** in this example) as the **SIP TLS FQDN** for this Conferencing Node (and **px01.vc.example.com** would also be the DNS A-record pointing to the publicly-reachable IP address of the Conferencing Node in question):




In our on-premises example, the node with a hostname of **conf01.vc.example.com** would have its **SIP TLS FQDN** also set to **conf01.vc.example.com**, and so on for the other Conferencing Nodes.

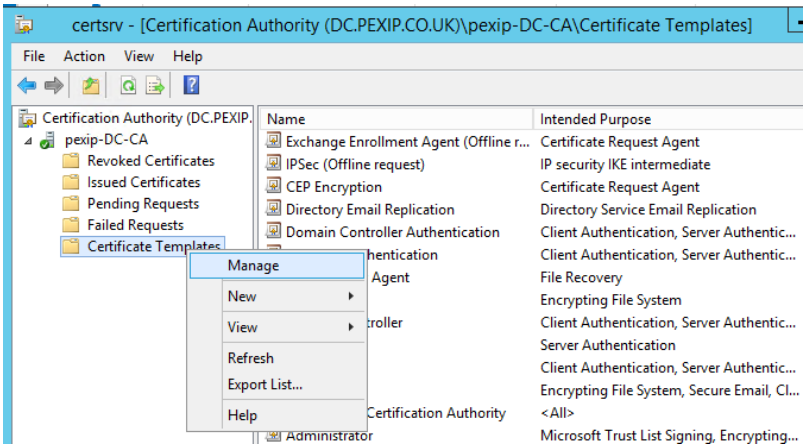
## Configuring Windows Server Manager to use a certificate template with client and server capabilities

If a Conferencing Node connects with a video network infrastructure device that performs a TLS verification process, the server certificate on the Conferencing Node needs Client Authentication capabilities. By default, the "Web Server" certificate template used

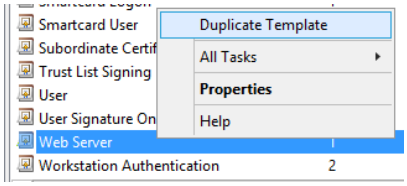
by the Microsoft Certification Authority tool in Active Directory Certificate Services (AD CS) creates a certificate with Server Authentication capabilities only. This section describes how to configure Windows Server Manager to use a certificate template with client and server capabilities.

To set up a certificate template with Server and Client Authentication (using Windows Server Manager 2016):

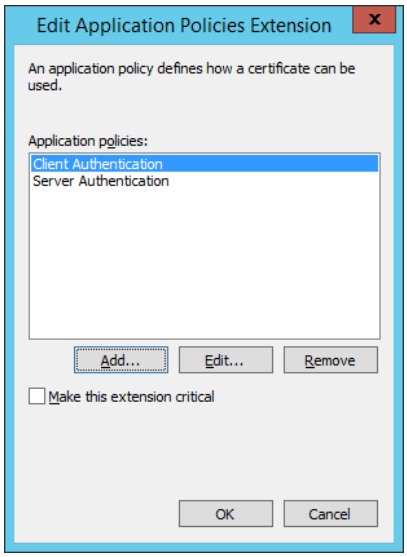
1. In Windows (server edition), launch **Server Manager**.
2. Launch the **Certification Authority** tool.
3. Expand the navigation tree for your Certification Authority and select **Certificate Templates**.
4. Right-click on **Certificate Templates** and select **Manage** to open the **Certificate Templates Console**.




5. Create a new template based on the existing **Web Server** template:
   a. Right-click on **Web Server** (in the list of templates) and select **Duplicate Template**.

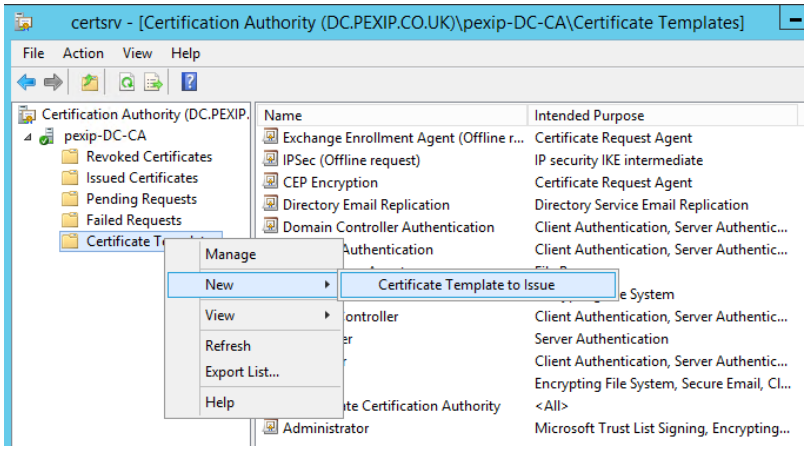



   b. On the **General** tab, enter the **Template display name** and **Template name** for your new template, for example "Web Client and Server" and "WebClientServer" respectively.
   c. On the **Extensions** tab, select **Application Policies** and select **Edit**.
   d. Add **Client Authentication** to the set of application policies:
      i. Select **Add**.
      ii. Select **Client Authentication** and select **OK**.
      iii. Select **OK**.




e. Select **OK** to complete the addition of the new template.

6. You can now close down the Certificate Templates Console.
7. Add the new template to your Certificate Authority:
   a. From the **Certification Authority** tool, expand the navigation tree for your Certification Authority, right-click on **Certificate Templates** and select **New > Certificate Template to Issue**.




   b. Select your new **Web Client and Server** template and select **OK**.

The new Web Client and Server template can now be used when submitting a certificate request to that Microsoft Certification Authority.

Note that all CSRs generated via Pexip Infinity's inbuilt CSR generator always request client certificate and server certificate capabilities.

# 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.

You can create a new CSR for any given subject name / node, or if you have an existing certificate already installed on a Pexip Infinity node that you need to replace (for example if it is due to expire) you can create a CSR based on the existing certificate data.

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

This topic covers:



## Requesting a certificate signing request (CSR) for an existing certificate / subject name

You can generate a certificate signing request (CSR) for an existing certificate / subject name, for example if your current certificate is soon due to expire and you want to replace it. Before generating the CSR you can change the certificate data to be included in the new request, such as adding extra subject alternative names (SANs) to those already present in the existing certificate.

To generate a CSR for an existing certificate / subject name:

1. Go to **Platform > TLS Certificates**.
2. Select the subject name of the certificate for which you want to generate a CSR.

   The certificate data is shown.
3. Go to the bottom of the page and select **Create certificate signing request**.

   You are taken to the Add Certificate signing request page, and the CSR data is defaulted to the contents of the certificate you selected.
4. If required you can change the certificate data, such as the subject alternative names (SANs) and subject fields.

   Note that you cannot change the private key — the CSR uses the same private key as the original certificate.
5. Select **Save**.

   The CSR is generated and you are taken to the **Change Certificate signing request** page.
6. 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 Uploading the signed certificate associated with a certificate signing request).

Note that:

- The validity, expiry date etc. of the existing certificate is not affected when you create a CSR to replace it.
- You cannot generate a CSR for an existing temporary / self-signed certificate.
- If the CSR generation fails with a "It was not possible to automatically create a certificate signing request from this certificate" message, then there was a problem with validating the original certificate data, most likely an invalid subject name or an invalid country code. In this case you will have to create the CSR manually.

## Creating a new 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:

| | |
|---|---|
| TLS Certificate | ***Create non-renewal CSR*** is selected by default. This lets you create a new CSR.<br>To create a renewal CSR based on an existing certificate, choose a different subject name / issuer from the list (in which case the subject name and private key fields below are not displayed). |
| 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.<br>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.<br>If you want to specify a custom Common Name instead, select ***User-provided custom Common Name***. |
| 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 ***User-provided custom Common Name*** above. |
| Private key type | Select the type of private key to generate, or select ***Upload user-provided private key*** if you want to provide your own private key.<br>Default: RSA (2048bit) |
| Private key | Only applies if you have selected ***Upload user-provided private key*** above.<br>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. |
| Private key passphrase | Only applies if you have selected ***Upload user-provided private key*** above.<br>If the private key is encrypted, you must also supply the associated passphrase. |
| Subject alternative names | Select the subject alternative names (SANs) 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.<br>You can choose from the same list of names presented in the **Subject name** field. Note that the name you choose as the Common Name is automatically included in the generated CSR's list of SANs (even if you remove it from the **Subject alternative names** list shown here).<br>In some deployments it may be more practical to generate a single CSR in which all of your Conferencing Node FQDNs are included in the list of SANs. This means that the same single server certificate returned by the CA can then be assigned to every Conferencing Node.<br>When integrating with Microsoft Skype for Business / Lync, SAN 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). |
| Additional subject alternative names | Optionally, enter a comma-separated list of additional subject alternative names to include in the CSR. For example:<br>◦ When receiving SIP or Skype for Business / Lync (MS-SIP) calls, the certificate on the Conferencing Node receiving the call should include the domain names (e.g. vc.example.com) that are used in any DNS SRV records that are used to route calls to those Conferencing Nodes.<br>◦ When integrating with on-prem Skype for Business / Lync deployments you would typically need to add the trusted application pool FQDN. |
| **Additional subject fields**<br>(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**<br>(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.<br>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.<br>Default: enabled. |

4. Select **Save**.
   You are taken to the **Change Certificate signing request** page.
5. 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.
6. 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 taken to the **Change Certificate signing request** page.
3. 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.
   - if you are uploading a replacement certificate (same subject name and private key) it will replace the existing certificate and maintain any existing node assignments.
   - 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

This section describes some of the error messages you may see when attempting to upload a signed certificate.

| Error message | Possible cause | Resolution |
|---|---|---|
| Certificate and private key do not appear to be part of the same key pair | This most likely means that you have tried to upload the certificate against the wrong CSR. | Select the correct CSR and try again. |

## 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

This section contains information about how Pexip Infinity manages presence information in Microsoft Skype for Business and Lync environments for Pexip services and contacts.

## Publishing presence information

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

Note that an Infinity Gateway contact publishes an 'Available' presence if the contact alias matches any Call Routing Rule (**Match Lync / Skype for Business (MS-SIP)** must be selected as one of the rule's incoming protocols). 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 SfB/Lync 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 SfB/Lync client contact list as they would not match the rule, have no presence, and hopefully alert the SfB/Lync user to a possible typing mistake.

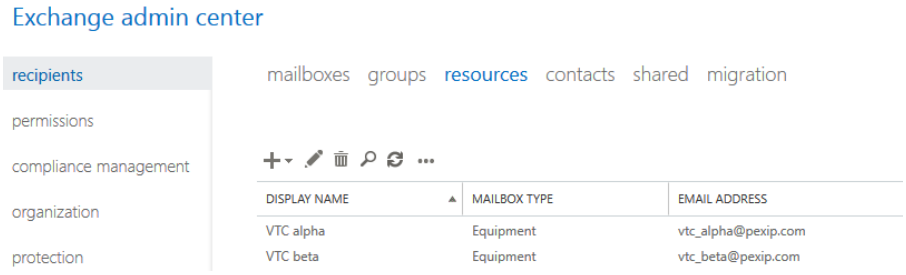
### Making a VTC endpoint searchable from a Skype for Business / Lync client

If your environment has VTC endpoints that can be called from SfB/Lync clients via the Infinity Gateway, you can make those endpoints searchable within the SfB/Lync client's address book. To do this:

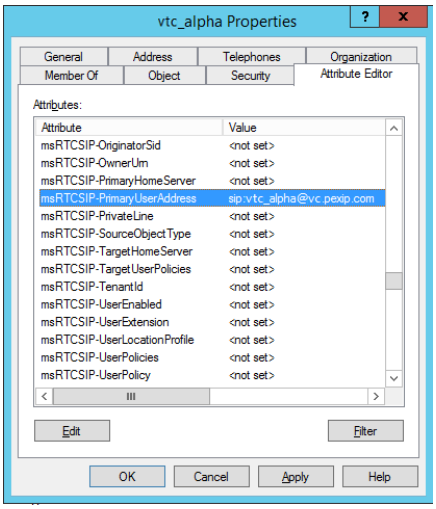
- If you have a resource that already exists in Exchange, you should populate **msRTCSIP-Primaryuseraddress** for this resource with the address the SfB/Lync client should dial to reach that resource.
- If the endpoint is not a resource (e.g. it is a desktop system, or a system that belongs to a business partner), then you should create a contact object in AD with **msRTCSIP-PrimaryUserAddress** set to the address the SfB/Lync client should dial to reach that endpoint.

You must also ensure that the address (domain) dialed by the SfB/Lync client is routed to Pexip Infinity and that a corresponding Call Routing Rule exists in Pexip Infinity to ensure it is routed (via SIP or H.323) to the device.

For example, you may have the following VTC resources configured:

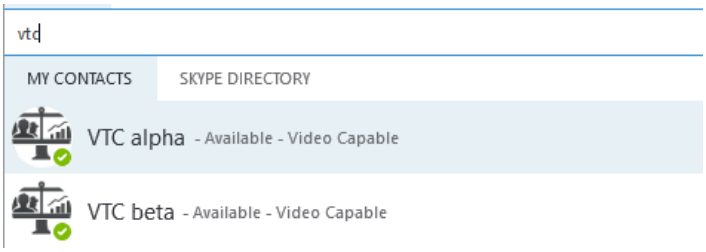


You can then use the Active Directory Users and Computers tool or ADSI Edit to configure these resources and set the **msRTCSIP-Primaryuseraddress** to the dialable address of that VTC resource, which is sip:vtc_alpha@vc.pexip.com in this example:

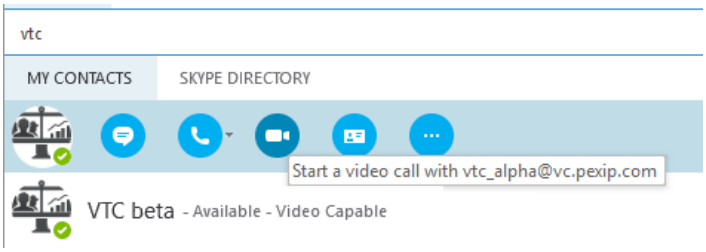



The resources will then show up in your searches within SfB/Lync, and can be used to start a video call to the configured address. Presence will show as available (although this may take some time initially) providing there is a Call Routing Rule in Pexip Infinity that matches the address pattern.

For example, searching for "vtc":




...and then initiating a video call:



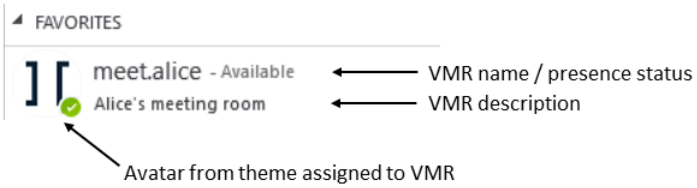

Note that the contact avatar that is displayed is taken from the Pexip Infinity theme that is associated with the Call Routing Rule that matches the address pattern. See Customizing the contact list avatar below for more information.

## Customizing the contact list avatar

You can customize the avatar that is displayed in SfB/Lync users' contact lists to represent the Pexip VMR / Virtual Auditorium, or gateway contact.

The avatar that is displayed in the SfB/Lync user's contact list is the content of the **presence_avatar_image.jpg** file contained in the theme associated with the VMR or Call Routing Rule as appropriate. If no theme has been associated with the VMR or Call Routing Rule, 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 SfB/Lync client.

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


FAVORITES
meet.alice - Available
Alice's meeting room
VMR name / presence status
VMR description
Avatar from theme assigned to VMR

# Initiating RTMP streaming from Skype for Business clients

Skype for Business / Lync* clients can use the Infinity Gateway service to dial out to an RTMP streaming or recording service.

This allows those SfB/Lync clients to initiate a dedicated RTMP multimedia stream to enterprise CDN (Content Delivery Network) streaming and recording services such as Wowza, Quickchannel, Qumu, VideoTool, Microsoft Stream and Azure Media Services, and to public streaming services such as YouTube, Facebook and Periscope.

To do this, you must:

1. Set up the streaming service and obtain the address to which the video stream will be sent (see https://docs.pexip.com/admin/integrate_streaming.htm for more information).
2. Set up a Call Routing Rule on Pexip Infinity that will match the contact address dialed from the SfB/Lync client and then call out to the streaming service.

   The contact address dialed from the SfB/Lync needs to be based upon (but not the same as) the streaming URL as it must be in a format dialable from the SfB/Lync client (avoiding : and / characters). The routing rule will then transform the dialed address into the streaming URL and initiate the call over RTMP. By using suitable regular expressions (regexes), you can make your rule re-usable for future streaming URLS to the same service.
3. You can then supply the appropriate address to the SfB/Lync users that they can use to dial out to the streaming service.

   For streaming services that always use a different stream name for every recording, you will have to provide the user with the address each time. If the streaming service supports a persistent URL (such as with Periscope or YouTube) they could add the address as a SfB/Lync contact for regular use.

See Using Pexip Infinity as a Skype for Business gateway for complete information about how to configure the Infinity Gateway to integrate with Skype for Business / Lync.

## Example streaming to YouTube

Let's assume that:

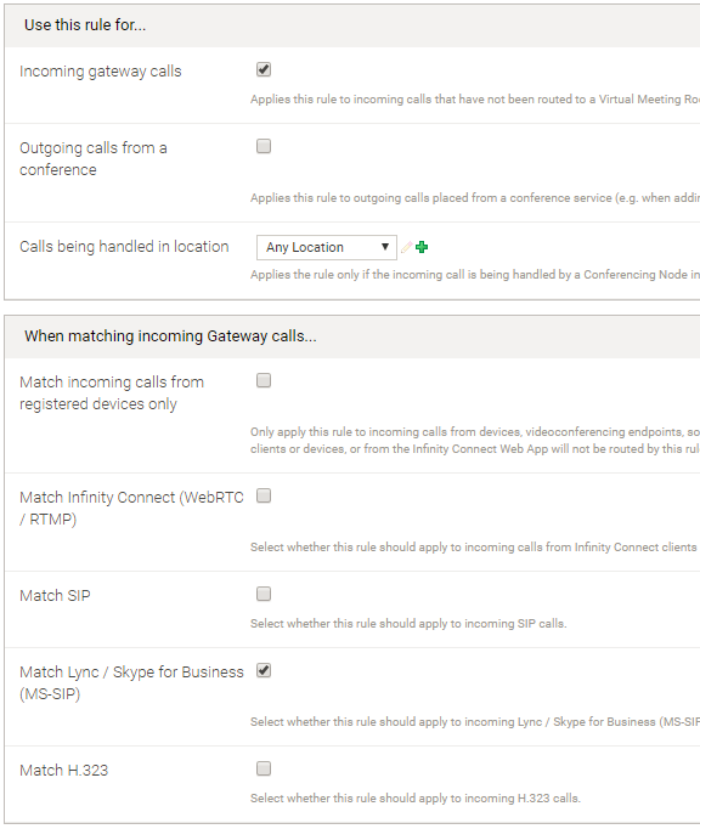
- The YouTube streaming URL is: **rtmp://a.rtmp.youtube.com/live2/qtr9-c85x-dxmw-av4t**
- The address to be called from the SfB/Lync client is: **rtmp_a.rtmp.youtube.com_live2_qtr9-c85x-dxmw-av4t@vc.example.com**

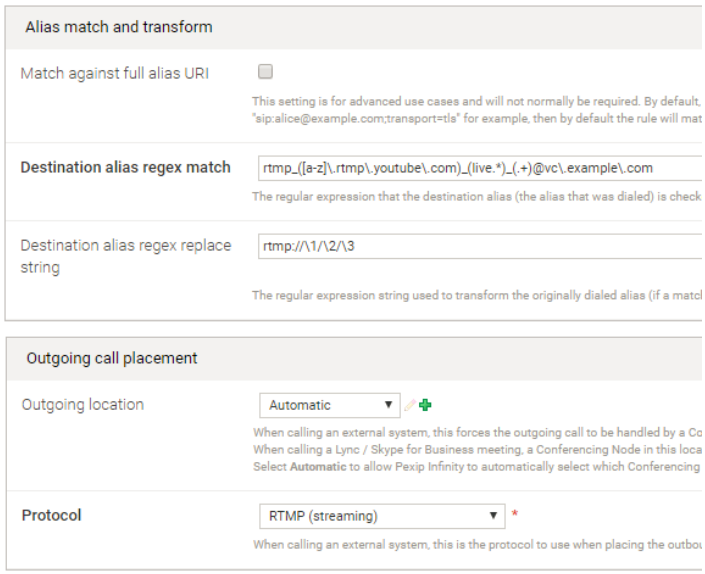
  i.e. it is in the format **rtmp_<resource portion of the URL with / characters converted to _ characters>@<SIP domain routed to Pexip Infinity>**

Your Call Routing Rule on Pexip Infinity should be configured like this:

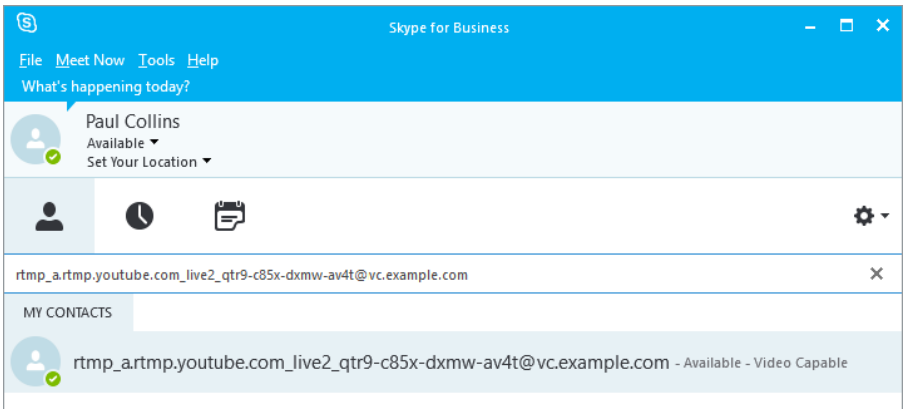
| Option | Description |
|---|---|
| Incoming gateway calls | Ensure this option is selected. |
| Outgoing calls from a conference | Leave unselected. |
| Match Infinity Connect (WebRTC / RTMP)<br>Match SIP<br>Match Lync / Skype for Business (MS-SIP)<br>Match H.323 | Select **Match Lync / Skype for Business (MS-SIP)** and leave the other protocols unselected.<br>(This rule is only handling call requests received from the SfB/Lync environment.) |
| Match against full alias URI | Leave unselected. |

| Option | Description |
|---|---|
| Destination alias regex match | Enter a regular expression that will match the format of the streaming address received from the SfB/Lync environment and uses match groups to allow the address elements to be rebuilt in the replace string. For example:<br>**rtmp_([a-z]\.rtmp\.youtube\.com)_(live.*)_(.+)@vc\.example\.com**<br>This expression matches:<br>• strings starting with **rtmp_**<br>• followed by a single letter (a-z) and then **.rtmp.youtube.com** (which is placed into match group 1)<br>• followed by _ (which we are using in the dial string in place of the / characters in the streaming URL)<br>• followed by **live** and then zero, one or more characters until the next _ character (which is placed into match group 2)<br>• followed by _<br>• followed by one or more characters until the @ character (which is placed into match group 3)<br>• followed by @vc.example.com (the domain routed from SfB/Lync to Pexip Infinity in our example deployment) |
| Destination alias regex replace string | The replace string must build the streaming URL to be dialed from Pexip Infinity, based on the elements extracted into match groups from the addressed dialed from the SfB/Lync client.<br>For example:<br>**rtmp://\1/\2/\3**<br>This builds the streaming URL based on "rtmp://" followed by match group 1, followed by "/" followed by match group 2, followed by "/" followed by match group 3. |
| Protocol | Select ***RTMP (streaming)***. |






You can then call the alias from within the SfB/Lync client:




### YouTube addresses with less variation

If your YouTube streaming URL addresses are more predictable, you can simplify your rule's alias regex matching logic. For example, if the streaming URLs always start **rtmp://a.rtmp.youtube.com/live2/** you could use:

- SfB/Lync addresses in the format: **youtube_<stream_name>@vc.example.com** for example **youtube_qtr9-c85x-dxmw-av4t@vc.example.com**
- The rule would then match against: **youtube_([-a-z0-9]+)@vc\.example\.com**
- The replace string would be: **rtmp://a.rtmp.youtube.com/live2/\1**

## Streaming to services with persistent URLs

Some streaming services, such as Periscope, support persistent URLs i.e. the same URL can be re-used for subsequent streams. In these cases, streaming initiated from SfB/Lync clients can be simpler to use as you could store the address as a SfB/Lync contact for regular use.

Here is another example of addresses and rule matching, this time using Periscope. Let's assume that:

- The Periscope streaming URL always takes the format **rtmp://<prefix>.pscp.tv:80/x/<stream_name>**
  For example: **rtmp://de.pscp.tv:80/x/w99qbwg1cz9x**
- The address to be called from the SfB/Lync client is in the format **periscope_<resource portion of the periscope URL>_<stream_**

**name>@<SIP domain routed to Pexip Infinity>**

For example: **periscope_de.pscp.tv_w99qbwg1cz9x@vc.example.com**

In this case, you could configure your Call Routing Rule with:

- A regex match string of: **periscope_([a-z][a-z]\.pscp\.tv)_([a-z0-9]+)@vc\.example\.com**
- A replace string of: **rtmp://\1:80/x/\2**

# 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 Skype for Business / Lync federation in a Pexip Infinity public DMZ deployment.

In our example public DMZ deployment, federation support for the SIP domain **vc.example.com** was implemented. This comprised:

- two Conferencing Nodes: **px01.vc.example.com** and **px02.vc.example.com**
- a global Pexip Infinity domain of **vc.example.com**
- a **_sipfederationtls._tcp.vc.example.com** DNS SRV record pointing to **px.vc.example.com**
- the same SAN certificate installed on every Conferencing Node, configured as:

```
commonName = px.vc.example.com
altNames = px.vc.example.com, px01.vc.example.com, px02.vc.example.com, vc.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. **companyname.vc** to this existing deployment.

## Adding an additional subdomain

To add an additional subdomain, such as **abc.example.com**, to an existing deployment:

1. Add a new system location.
   - You must add a new Pexip Infinity system location (**Platform > 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 > Global Settings > Connectivity**) has been set to **vc.example.com**.
   - You must override this global setting for each new location. Go to **Platform > 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 **px01.abc.example.com** and **px02.abc.example.com** and assign them to location **abc**.
4. Configure additional DNS A records and DNS SRV records for the pool of new Conferencing Nodes.

   For example, for the nodes supporting the subdomain **abc.example.com**, you would create:
   - SRV-record: **_sipfederationtls._tcp.abc.example.com**, pointing to pool hostname **px.abc.example.com** on port **5061**
   - Pool round-robin A-record: **px.abc.example.com**, pointing to your 1st Conferencing Node (the publicly-reachable IP address of px01.abc.example.com)
   - Pool round-robin A-record: **px.abc.example.com**, pointing to your 2nd Conferencing Node (the publicly-reachable IP address of px02.abc.example.com)
   - Standard A-record: **px01.abc.example.com**, pointing to the publicly-reachable IP address of px01.abc.example.com
   - Standard A-record: **px02.abc.example.com**, pointing to the publicly-reachable IP address of px02.abc.example.com

   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 px.**abc.example.com**; you cannot, for example, configure the _sipfederationtls._tcp.abc.example.com SRV-record to point to px.example.com). This is required due to the trust model for SfB/Lync 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 pool hostname referenced by the _sipfederationtls._tcp SRV record, and the SANs should include the FQDNs of all of the nodes in the location, plus the pool hostname and the domain name used in the _sipfederationtls SRV record.

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

```
commonName = px.abc.example.com
altNames = px.abc.example.com, px01.abc.example.com, px02.abc.example.com, 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 > 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 **vc.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. **companyname.vc** to an existing deployment:

1. Add a new system location.
   - You must add a new Pexip Infinity system location (**Platform > Locations**) to support each additional domain.
   - For example, add a new system location **xyz** to support the domain **companyname.vc**.
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 > Global Settings > Connectivity**) has been set to **vc.example.com**.
   - You must override this global setting for each new location. Go to **Platform > 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 **companyname.vc**.
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 **px01.companyname.vc** and **px02.companyname.vc** and assign them to location **xyz**.
4. Configure additional DNS A records and DNS SRV records for the pool of new Conferencing Nodes.

   For example, for the nodes supporting the domain **companyname.vc**, you would create:
   - SRV-record: **_sipfederationtls._tcp.companyname.vc**, pointing to pool hostname **px.companyname.vc** on port **5061**
   - Pool round-robin A-record: **px.companyname.vc**, pointing to your 1st Conferencing Node (the publicly-reachable IP address of px01.companyname.vc)
   - Pool round-robin A-record: **px.companyname.vc**, pointing to your 2nd Conferencing Node (the publicly-reachable IP address of px02.companyname.vc)
   - Standard A-record: **px01.companyname.vc**, pointing to the publicly-reachable IP address of px01.companyname.vc
   - Standard A-record: **px02.companyname.vc**, pointing to the publicly-reachable IP address of px02.companyname.vc

   Note that the domain name used in the SRV-record has to match the domain in the corresponding A-record (e.g. _sipfederationtls._tcp.**companyname.vc** must use the same domain as px.**companyname.vc**. This is required due to the trust model for SfB/Lync 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 pool hostname referenced by the _sipfederationtls._tcp SRV record, and the SANs should include the FQDNs of all of the nodes in the location, plus the pool hostname and the domain name used in the _sipfederationtls SRV record.

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

   ```
   commonName = px.companyname.vc
   altNames = px.companyname.vc, px01.companyname.vc, px02.companyname.vc, companyname.vc
   ```

   When hosting an additional top-level domain (**companyname.vc** 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 > 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 **vc.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 > 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.
- When integrating with on-premises Microsoft Skype for Business / Lync systems, Conferencing Nodes do not need to use a TURN server for media routing to remote or federated SfB/Lync clients, providing they can reach the public-facing interface of the SfB/Lync Edge server. However, if the Conferencing Nodes are behind a NAT then they do need access to a STUN/TURN server so that each node can discover its NAT address. In Skype for Business / Lync deployments it is essential that a Conferencing Node can discover its NAT address.
- 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 Skype for Business and Lync, the following ports have to be allowed through any firewalls which carry traffic for the involved devices:

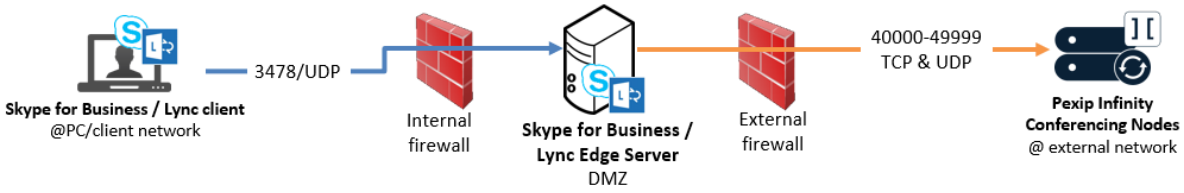
| Direction | Purpose | Protocol | Source | Destination |
|---|---|---|---|---|
| Between the SfB/Lync FEP and the Conferencing Node (bidirectional) | SIP signaling | TCP | <any> | 5061 |
| From SfB/Lync clients towards the Conferencing Nodes | RTP/RTCP media | UDP | <any> | 40000–49999 |
| From SfB/Lync clients towards the Conferencing Nodes | HTTP conference avatar | TCP | <any> | 80 |
| From the Conferencing Nodes towards a SfB/Lync Edge Server (AV Edge Interface) | RTP/RTCP/RDP media | UDP / TCP | 40000–49999 | 50000–59999 |
| From the SfB/Lync Edge Server (AV Edge Interface) towards Conferencing Nodes | RTP/RTCP/RDP media | UDP / TCP | 50000–59999 | 40000–49999 |
| From the Conferencing Nodes towards SfB/Lync clients or SfB/Lync servers | RTP/RTCP/RDP/VbSS 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 SfB/Lync Web Conferencing service | PSOM (PowerPoint presentation from SfB/Lync) | TCP (TLS) | 55000–65535 | 443 / 8057 ‡‡ |
| From the Conferencing Nodes towards the SfB/Lync Front End Server or Edge Server | HTTPS (PowerPoint presentation from SfB/Lync) | TCP (TLS) | 55000–65535 | 443 |
| From the Conferencing Nodes towards the Web Application Companion (WAC) server / Office Web Apps (OWA) server / Office Online Server (OOS) | HTTPS (PowerPoint presentation from SfB/Lync) | TCP (TLS) | 55000–65535 | 443 |
| ‡‡ Typically 443 for Web Conferencing Edge and 8057 for a SfB/Lync Front End Server / FEP. | | | | |

For a complete list of Pexip Infinity Conferencing Node port usage, see Pexip Infinity port usage.

### Skype for Business / Lync clients behind strict firewalls

If your SfB/Lync clients are behind a strict network, and only the minimum ports are allowed for B2B SfB/Lync communication, you may need to allow a few extra flows outbound:

- Your PC must be able to connect outbound to the internal interface of your SfB/Lync AV Edge Servers on port 3478/UDP (blue arrow).
- Your SfB/Lync AV Edge servers must be able to connect outbound to Pexip Conferencing Nodes for media, on port range 40000–49999 TCP & UDP for optimal HD video and content sharing (orange arrow).



# Appendix 4: Troubleshooting and limitations

## SfB/Lync 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 SfB/Lync client (via the FEP):
  - Management Node support log (**History & Logs > Support Log**)
  - SfB/Lync FEP logging tool
- Check if the Conferencing Node receiving the call is in maintenance mode.

### Detail

If the SfB/Lync 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 SfB/Lync client. This can be done both on the Conferencing Node (with the support log) and on the FEP serving the SfB/Lync client (using the SfB/Lync debugging tools).

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

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

After ICE negotiation has completed between the SfB/Lync client and the Conferencing Node, the SfB/Lync 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.

#### Conferencing Node is in maintenance mode

If a Conferencing Node in a trusted application pool is placed into maintenance mode, and a SfB/Lync server sends a call to that node, the node will respond with 503 Service Unavailable and the call will then fail (SfB/Lync will not try another node in the pool).

Therefore, if you need to place a Conferencing Node into maintenance mode, we recommend that you wait until all SfB/Lync calls on that node have completed, and then you should temporarily remove the node from the trusted application pool and then place it into maintenance mode. The node should then be returned to the trusted application pool after it has been taken back out of maintenance mode.

## SfB/Lync 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 SfB/Lync client is correctly configured with an audio and video device.
- Verify that the call from the SfB/Lync client is placed as a video call rather than a SfB/Lync (audio-only) call.

- Verify (with SIP logs) that the SIP call setup behaves as expected:
  - INVITE from SfB/Lync 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 SfB/Lync client receives RTP media from Pexip Infinity (using for instance Wireshark).
- Verify that Pexip Infinity Conferencing Node receives RTP media from SfB/Lync client (using for instance tcpdump).

## Collecting SIP logs using the SfB/Lync 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**;
- Skype for Business Server 2015: **C:\Program Files\Skype for Business Server 2015\Debugging Tools\CLSLogger.exe**

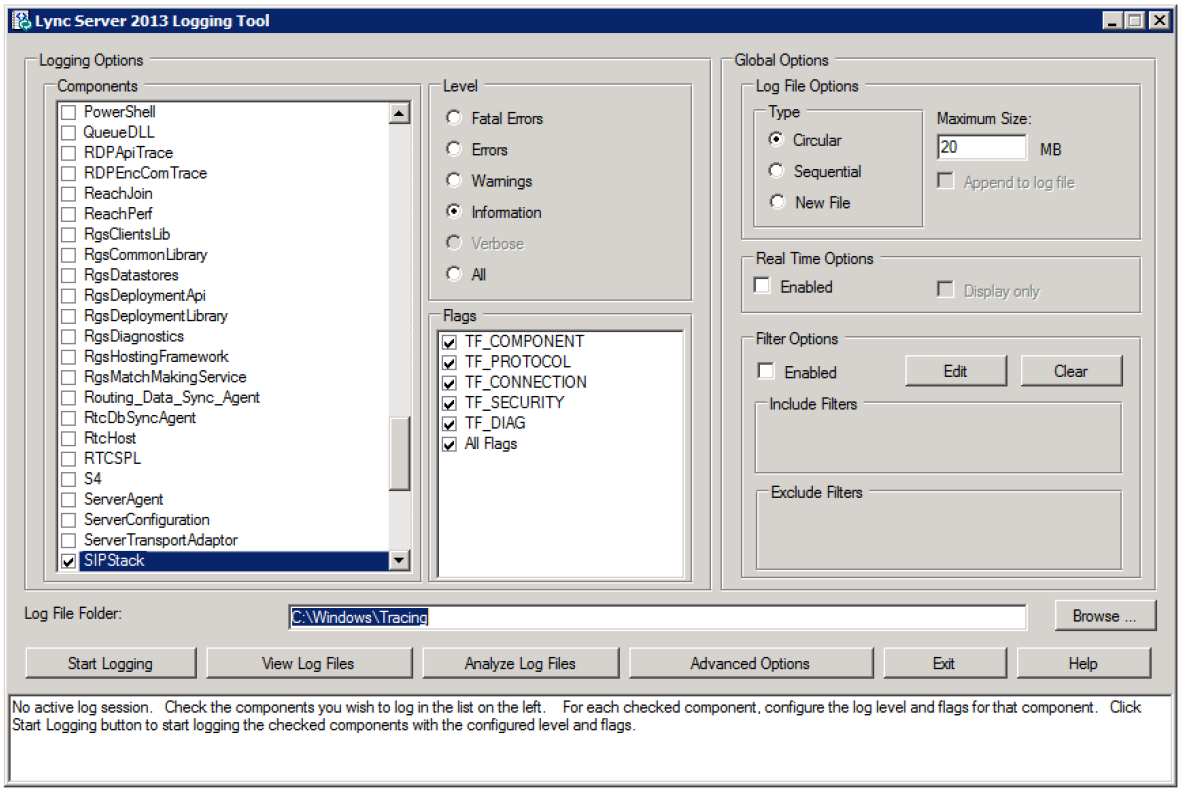
Note however that a different location may have been chosen at the time of installation.

After opening the logging tool, the following selection is normally suitable for initial troubleshooting of failing calls between SfB/Lync 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 SfB/Lync 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 SfB/Lync meeting with no participants

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

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

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

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

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

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 SfB 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 Skype for Business server, and on Pexip Infinity (**Platform > Global Settings > Connectivity > Enable VbSS For Skype For Business**).

## 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 SfB/Lync client to a locked conference

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

However, other participants in the Pexip Infinity conference will not see the message. The SfB/Lync 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).

## SfB/Lync participants do not receive presentations / content sharing

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

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

## Content from Pexip participants not included in a Skype for Business / Lync meeting recording

If a Skype for Business client running on Windows 7 attempts to record a Skype for Business / Lync meeting, the recording will not include any content from Pexip participants calling into the meeting through the Infinity Gateway.

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

If a SfB/Lync participant in a SfB/Lync meeting is presenting while another device joins the SfB/Lync meeting via the Infinity Gateway, the SfB/Lync 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.

## SfB/Lync 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 SfB/Lync clients.

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

## 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 SfB/Lync meetings via the Virtual Reception (IVR gateway)

The following table describes the typical problems and suggested resolutions for issues related to connecting to SfB/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).

## Problems connecting gateway calls to SfB/Lync clients

The following table describes the typical problems and suggested resolutions for issues related to allowing devices to call SfB/Lync clients via the gateway.

| Symptom | Possible cause | Resolution |
|---|---|---|
| The SfB/Lync server returns a 400 Bad request response. | The Call Routing Rule towards the SfB/Lync server has the wrong **Call target** type, such as ***Lync / Skype for Business meeting direct (Conference ID in dialed alias)***. | Ensure that the **Call target** is set to ***Lync / Skype for Business clients, or meetings via a Virtual Reception***. |

For more information, see Configuring rules to allow devices to call Skype for Business / Lync clients via the gateway.

## Gateway clients are disconnected from SfB/Lync meetings

The following table describes the typical problems and suggested resolutions for issues related to gatewayed participants being disconnected from SfB/Lync meetings.

| Symptom | Possible cause | Resolution |
|---|---|---|
| Gatewayed participants are disconnected from SfB/Lync meetings. Participant history shows a disconnect reason of "CCCP call disconnected: Conference Terminated - Enterprise User Absent". | All of the SfB/Lync clients have left the meeting and the gateway participants have been timed out.<br><br>(Note that "CCCP call disconnected" can also appear in other situations.) | There is a SfB/Lync setting (**AnonymousUserGracePeriod**) that represents the amount of time an anonymous (unauthenticated) user, such as a gateway participant, can remain in a SfB/Lync meeting without an authenticated user being present in that same meeting. The default value is 90 minutes.<br><br>You can check the current value by using the following PowerShell command: `Get-CsUserServicesConfiguration` and you can set the timeout value with: `Set-CsUserServicesConfiguration`<br><br>For more information, see https://docs.microsoft.com/en-us/powershell/module/skype/Set-CsUserServicesConfiguration. |

## 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 that are connected to a Pexip VMR that is merged with a Skype for Business / Lync meeting, or that are in a gateway call, can't see shared content when a SfB/Lync user presents PowerPoint files, the most likely reason is that **SIP TLS verification mode** is ***On*** (**Platform > Global Settings > Security**) and that Pexip Infinity does not trust the SfB/Lync 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 > Trusted CA Certificates**).

## Shared PowerPoint files are slow to display to Pexip participants

Depending on the size of the PowerPoint file, it can take a long time to display the presentation content to Pexip participants. This delay occurs while Pexip Infinity waits for the SfB/Lync server to make the presentation files (JPEG images) available.

The time spent waiting is shown in the Pexip Infinity support log, for example:

```
Level="INFO" Name="support.ms_data_conf.ms_data_conf" Message="Got download information for all PowerPoint JPEGs" Content-ID="1" Ppt-title="example.pptx" Download-URL-Base="https://webpool.infra.lync.com/DataCollabWeb/Fd/29f...J89/" Waited="118.913 seconds"
```

## Occasional dropped video frames

On rare occasions, some SfB/Lync users in a SfB/Lync meeting may occasionally experience dropped video frames from VTC endpoints that are gatewayed into that meeting.

## Pexip only transmits low resolutions to mobile SfB clients

A mobile SfB client (iOS and Android), or SfB Mac client that is dialed into a Pexip Infinity VMR will never request anything higher than 360p. This means that although Pexip Infinity may receive a higher resolution video from the SfB client, it will only send up to a maximum of 640x360 to the SfB client (and limited to 180p to mobile and 360p to tablet devices).