Cisco Expressway with Microsoft Infrastructure

Deployment Guide

First Published: December 2013

Last Updated: September 2018

Cisco Expressway X8.11.1

Microsoft Lync Server 2010 or 2013

Skype for Business Server 2015

Contents

Preface

Change History

Table 1   Deployment Guide Change History

Date	Change	Reason
September 2018	Updated software version from X8.11 to X8.11.1, as version X8.11 is no longer available.	Software withdrawn.
July 2018	Added Interoperability Direction Statement, page 5; **this document is no longer being actively maintained**.	New interoperability model introduced X8.9 to X8.11.
February 2017	Republished with corrections.	Updated supported versions table.
December 2016	Republished.	X8.9 release.
July 2016	Add SIP Broker feature and migration scenarios. Improved MS client support. IM&P integration. Replace "Lync" with generic Microsoft Interoperability, associated UI changes. Scope of support for Skype for Business.	X8.8 release.
February 2016	Republished with corrections.	Deployment diagram clarified and media flow diagrams corrected.
February 2016	Republished with screen sharing from Skype for Business (desktop versions) support updated.	New information.
December 2015	Republished.	Scope of support for Lync screen sharing in point to point scenarios clarified.
December 2015	Republished.	Screen sharing from Lync now supported with MCU conferences.
November 2015	Screen sharing from Lync feature now supported with clustered gateway.	X8.7 release.
November 2015	X8.6 version republished.	Scope of support for screen sharing from Lync clarified.
August 2015	X8.6 Expressway version republished.	Screen share toplogy diagrams corrected.
July 2015	Document revised and restructured. Screen sharing from Lync feature added.	X8.6 release.
December 2014	Updated.	X8.5 release.
July 2014	X8.2 version revised.	Content defect CSCup55116.
June 2014	X8.2 version revised to include Federation appendix.	New information.
June 2014	Updated.	X8.2 release.
December 2013	Initial release of Expressway version of this document.	Expressway product launched.

Interoperability Direction Statement

Expressway enables Microsoft clients to interoperate with Cisco and other standards-based SIP infrastructure. Cisco is committed to continue supporting that interoperability using a new deployment model introduced in X8.9.

Expressway currently has two overlapping models for interoperating with Microsoft SIP infrastructure:

- **Expressway's Microsoft Interoperability service**: this option enables the "Gateway Expressway" and "SIP Broker" deployments. The Expressway transcodes the different implementations of SIP.
- **Session classification**: this option is available in Expressway X8.9 and later. The Cisco Meeting Server transcodes the different implementations of SIP.

We intend to stop supporting the older model and we encourage customers to use the new model for interoperating between Cisco and Microsoft SIP infrastructure. We will not extend Expressway's Microsoft Interoperability service to support newer Microsoft clients and infrastructure options.

Table 2   Important differences between the interoperability models

Compare	Expressway's Microsoft Interoperability service	Expressway session classification with Cisco Meeting Server
Description and benefits	We actively developed this feature until X8.8. It is now the "Microsoft Interoperability service", but was previously the "Lync B2BUA". - Instant messaging and Presence between Cisco Jabber and Microsoft clients (SIP Broker deployment) - Bidirectional video and audio, with desktop share from Microsoft side (Gateway Expressway deployment)	We introduced this deployment in X8.9 and refined it in X8.10 and X8.11. - Instant messaging and Presence between Cisco Jabber and Microsoft clients (does not require Meeting Server) - Bidirectional video, audio, and desktop share - Conferencing interoperability for Microsoft clients - A dual homed solution to maintain user experience for Cisco and Microsoft users - Business to business federation
Licensing	- *Microsoft Interoperability* key on Expressway - Rich Media Session (RMS) licenses on Expressway	- Requires Meeting Server licensing - Does not require *Microsoft Interoperability* key on Expressway - Does not require RMS licenses for on-premises interoperation
Supported Microsoft versions	- Lync Server 2013 - Skype for Business Server 2015	- Lync Server 2013 - Skype for Business Server 2015 - Office 365
Known limitations	- No business to business federations (on-premises, mixed infrastructure only) - Dedicated Expressway required - Limited support for mobile clients - Unidirectional presentation transcoding: RDP -> BFCP but not BFCP -> RDP - No AV MCU integration	- Expressway-E TURN Server feature gaps in X8.10 - On-premises integration with Microsoft infrastructure is pending verification**

** Expressway X8.10 does not completely support on-premises integration between Microsoft and Cisco infrastructure. This limitation is removed in X8.11. If you need AVMCU integration ("dual homing") with Expressway X8.10, you can configure a direct integration between Meeting Server and the Microsoft Front End

Introduction

This deployment guide describes how to configure a Cisco Collaboration video network to interwork with a Microsoft environment, using the Microsoft Interoperability service on a dedicated Cisco Expressway (" Gateway" Expressway).

It also highlights the capabilities and limitations of interoperation between Expressway and Microsoft.

To enable video calling, screen sharing, messaging and presence between Cisco Unified Communications Manager-registered collaboration endpoints and Microsoft clients, you need to configure:

- A SIP trunk between the Gateway Expressway and Unified CM
- The Microsoft Interoperability service on the Gateway Expressway to route calls to Microsoft
- Static routes from Microsoft FE Servers to the Gateway Expressway
- Static routes from Cisco Unified Communications Manager IM and Presence Service publishers to Microsoft FE Servers

Deployment Scope

The following major Expressway-based deployments do not work together. They cannot be implemented together on the same Expressway (or traversal pair):

- Mobile and Remote Access
- Microsoft interoperability, using the Expressway-C-based B2BUA
- Jabber Guest services

What is the Gateway Expressway and Why Should I Use It?

A Gateway Expressway is an Expressway-C (or cluster of Expressway-Cs) that provides interoperability between a Cisco Collaboration network and the Microsoft environment.

We require that you dedicate an Expressway-C to this role so that you:

- Minimize the impact of adding Microsoft interoperability to your existing Cisco Collaboration network.
- Limit the number of Expressways that need the **Microsoft Interoperability** option key.
- Reduce the number of static routes that you need to define from the Microsoft environment.

    Each static route matches a single SIP domain to a single FQDN, or IP address, but you can create appropriate DNS records to map an FQDN to a cluster of Expressways.
- Reduce the number of third-party applications that you configure Microsoft to trust.

    Microsoft FE Server will only accept SIP messages from peers that it trusts. By dedicating a Gateway Expressway (or cluster), you reduce the number of trusted applications that you need to configure in Microsoft.

Recommendations

- We recommend that you use TLS connectivity throughout the deployment. We do not recommend TCP because:
  - Microsoft SIP infrastructure uses TLS by default
  - TCP prevents the use of encryption
  - TCP may not work for Microsoft environments that include hardware load balancers (HLBs) and / or Director

- A static route using TCP must go to the destination IP address. So, with TCP you cannot get redundancy from a clustered Gateway Expressway, which you can when you configure a TLS static route to the cluster's FQDN

■ If the Gateway is a cluster, you must configure the primary peer and allow the configuration to be replicated to the other peers automatically. When you see the † in the web interface, it indicates that a field must be completed on each peer.

Deployment Components

We are integrating your Microsoft environment with your video network to provide video calling and screen sharing between Cisco Collaboration endpoints and Microsoft clients.

Figure 1   Topology used in this deployment guide
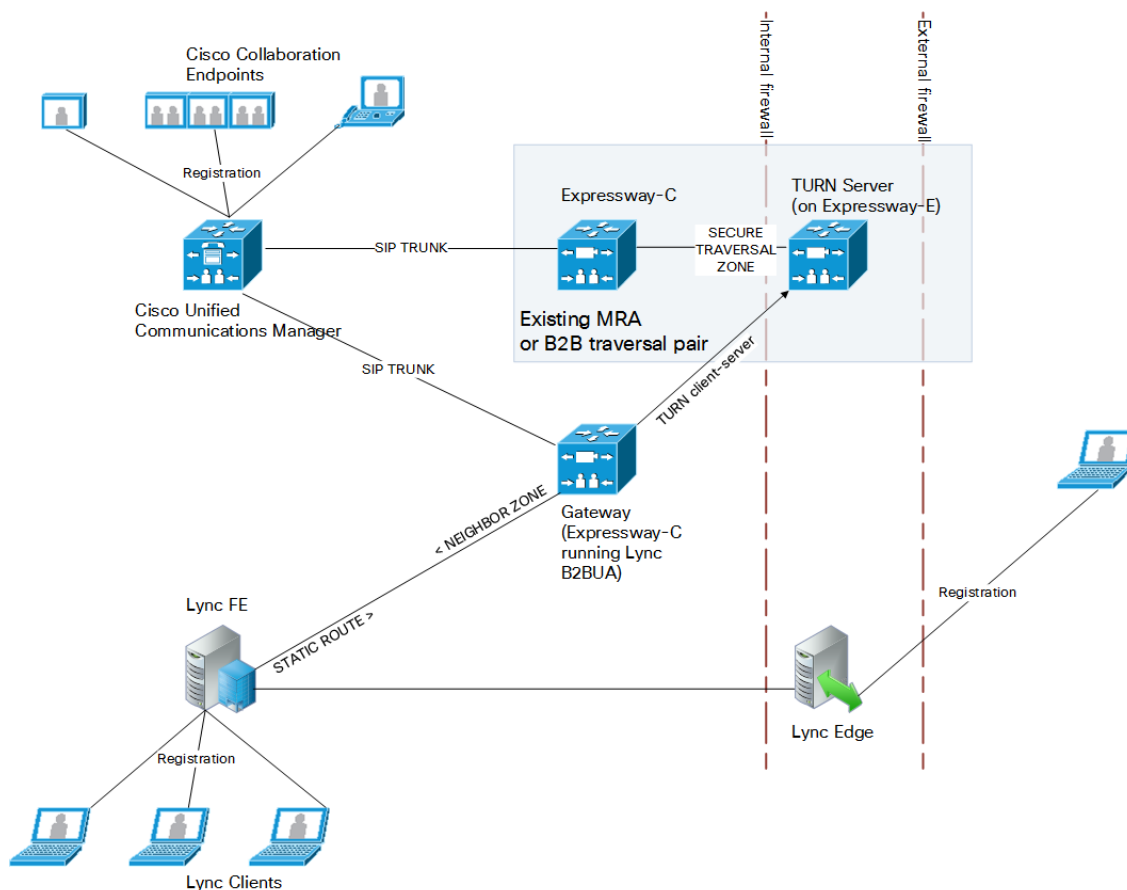
What's in the diagram?

The Microsoft deployment has:

- A pool of Microsoft Servers with Front End Server role (one server shown for clarity).
- A Microsoft Server with Edge Server role.
- On-premises Microsoft clients registered to Microsoft FE Server.
- Off-premises Microsoft clients registered to Microsoft Edge.

The Cisco video deployment has:

- Unified CM for primary call control of the Cisco Collaboration video network.
- On-premises Cisco Collaboration endpoints registered to Unified CM.
- A dedicated Expressway-C for interoperability with the Microsoft environment (referred to as Gateway Expressway).
- Cisco Expressway-E in the DMZ to provide TURN services.

  Note: The diagram shows a separate Cisco Expressway-C and Cisco Expressway-E traversal pair, trunked to Unified CM. This configuration is not required for Microsoft interoperability, but you can use the Cisco Expressway-E from your MRA or B2B solution for TURN services. The (MRA) Cisco Expressway-C shown here is not required in this deployment, so it is not shown in other diagrams in this document.

Example Values in this Deployment

The example presented uses the following values:

- The Microsoft environment uses `example.com` as the SIP domain. The SIP domain for Microsoft need not be the same as the AD domain of Microsoft clients (the Microsoft login domain used in the login user name may be different from the SIP domain used in the sign-in address).
- The Cisco video network's domain is `video.example.com` (used for video device registrations).
- Endpoints registered to the video network are provisioned by Unified CM and register with a DN in the format 3xxx.
- Microsoft clients registered to Microsoft FE servers are identified by URIs, for example:
  - David with a URI `david.jones@example.com`
  - Alice with a URI `alice.parkes@example.com`
- Microsoft Front End Server is configured with a static domain route which routes URIs with the Expressway's video network domain (`video.example.com`) to the Gateway Expressway. Take care when using domain static routes; any traffic for that domain that Microsoft cannot handle locally will be routed to Expressway.

Features and Limitations

Microsoft Environment

The scale of your Microsoft deployment could mean that your deployment model is more complex than what is described in this guide. Appendix 3: Extended Microsoft Deployments, page 70 describes some of the different options and how the deployment model varies in each case.

Lync / Skype for Business Versions Supported in This Deployment

The following matrix shows which Microsoft Lync and Skype for Business client versions are supported in the Expressway gateway deployment. Clients in the first column are registered to one of the server versions in the other columns. Find your client and server version to check whether the combination is supported in this Expressway deployment.

Table 3   Microsoft Lync and Skype for Business Support in this Deployment

Clients (below), when registered to servers (right)	Lync Server 2010	Lync Server 2013	Skype for Business Server 2015
Lync 2010 (Windows desktop)	Supported	Supported	Not supported
Lync for Mac 2011(audio only[1])	Supported	Supported	Not supported
Lync 2013 for Windows (Windows desktop) that does not have the Skype for Business UI update[2]	Not applicable	Supported	Supported
Lync 2013 for Windows (Windows desktop) that has the option to use the Skype for Business UI[2]	Not applicable	Supported	Supported
Lync 2013 (iOS mobile)[3]	Not applicable	Supported	Not supported
Lync 2013 (Android mobile)[3]	Not applicable	Supported	Not supported
Lync 2013 (Windows Mobile)[3]	Not applicable	Supported	Not supported
Skype for Business 2015 (Windows desktop, native client)	Not applicable	Supported	Supported
Skype for Business 2016 (Windows desktop, native client)	Not applicable	Supported	Supported
Skype for Business (iOS mobile)	Not applicable	Not supported	Limited support[4]
Skype for Business (Android mobile)	Not applicable	Not supported	Limited support[4]
Skype for Business (Windows Mobile)	Not applicable	Not supported	Not supported

1. Lync 2011 for Mac uses an unsupported video codec
2. Newer Lync 2013 client versions have an option to use the Skype for Business user interface (since the updates in Security Bulletin MS15-044 https://support.microsoft.com/en-us/kb/3039779)
3. Mobile clients that are deprecated by Skype for Business versions

4. We do not support these clients in calls to MCU bridges. We do support them in other call scenarios, including calls to TelePresence Server bridges.

MS Lync / Office 365 Calls May Fail if Expressway-E Cluster Node Placed in Maintenance Mode

This applies if you have clustered Expressway-E nodes and interoperate with Microsoft environments. If you place one of the Cisco Expressway-Es in Maintenance Mode, Lync or Office365 calls may fail. This is due to the Microsoft server DNS lookup behavior. (It does a DNS lookup for the _sipfederationtls SRV records in the Expressway domain and caches the result. If the DNS query resolves to the Expressway-E that is in Maintenance Mode, call requests will fail until either the Microsoft server cache expires, or the Expressway-E is back in service.)

Microsoft Server Limitations in this Deployment

Skype for Business Server 2015

Skype for Business Server 2015 is supported with X8.8 and later versions of Expressway, except where we have stated limitations.

The **Microsoft Interoperability** option key is required for all types of communication with Skype for Business Server 2015.

Microsoft Lync Server 2013

The B2BUA provides interworking between standard H.264 AVC and Lync 2013's H.264UC SVC codec. You can still configure the B2BUA to use Cisco AM GW transcoders with Lync 2013, but it is not necessary and we recommend that they are not deployed with Lync 2013.

Lync 2013 no longer supports H.263, so X8.1 or later software is required to interoperate successfully with Lync 2013.

The **Microsoft Interoperability** option key is required for all types of communication with Lync 2013.

Microsoft Lync Server 2010

The **Microsoft Interoperability** option key must be installed to enable encrypted calls to and from Microsoft Lync 2010 Server (for both native SIP calls and calls interworked from H.323). It is also required by the B2BUA when establishing ICE calls to Lync 2010 clients.

The B2BUA can use the Cisco AM GW to transcode between standard codecs (such as H.264) and Microsoft RT Video and RT Audio to allow high definition calls between Microsoft Lync 2010 clients and Cisco endpoints.

Screen sharing from Microsoft clients toward video network endpoints is not supported on Lync Server 2010.

Earlier versions

This version of Expressway does not interoperate with any versions of Microsoft Office Communications Server or Live Communications Server.

Voice and Video Calling

SIP Calls

- SIP endpoints registered to Unified CM can make calls to Microsoft clients registered to a Microsoft Server.
- Microsoft clients registered to a Microsoft Server can make calls to SIP endpoints registered to Unified CM.
- SIP signaling and RTP media is always routed through the Microsoft Interoperability B2BUA for calls involving Microsoft clients. Each B2BUA instance (one per Expressway) can handle 100 simultaneous calls between Microsoft and the Expressway video environment.
- Media encryption (SRTP) is supported when TLS is used between Expressway and Microsoft and the **Microsoft Interoperability** option key is added to the Gateway Expressway.
- Microsoft clients can be the object of a transfer (even if there is an AM gateway involved in the call).
- The maximum resolution of an SVC to AVC converted call is 720p 30fps.

- Hold and resume works from either party (Cisco collaboration endpoint or Microsoft client).
- A Microsoft client sometimes notifies that it has no audio device configured when selecting resume. Follow the client's instructions to update the audio device to get hold/resume working.

Upspeeding a Voice Call to Video

- If a voice call is made from a Microsoft client to a UCM-registered endpoint, and then the video button is selected to enhance the call to a video call, the video endpoint will correctly upspeed to video.

MXP Endpoints

Video from MXP endpoints to Lync 2013 H.264 SVC is limited to 15fps (video with other endpoints is 30fps).

Integration with Cisco Unified Communications Manager IM and Presence Service

Enables messaging and presence between Microsoft clients and Cisco Jabber

- Requires IM and Presence Service 10.x or later
- Requires Lync Server 2010 or Lync Server 2013.
- Requires Expressway X8.8 (with **Microsoft Interoperability** option key)

Screen Sharing

- Microsoft clients can share their screen with standards-based endpoints in the video network, because the Gateway Expressway can transcode RDP media into H.264.
- Mobile versions of Lync and Skype for Business cannot share their screens.
- The reverse transcode (from H.264 to RDP) is not supported. If the endpoint is capable of putting the presentation in the main video channel, then the Microsoft user can see the presentation that way. Otherwise, if the parties are in a conference, the conference bridge will compose the presentation (from the standards-based endpoint) into the main video it sends to the Microsoft user.
- Lync Server 2013 or Skype for Business Server 2015 are required for screen sharing. Other server versions are not supported for this feature.
- The following Microsoft clients can share their screen through the Gateway Expressway:
  - Lync 2013 for Windows (desktop version)
  - Skype for Business 2015 (desktop version)
  - Skype for Business 2016 (desktop version)
- Screen sharing from the Microsoft client is supported when the client is in a conference on a Cisco TelePresence Server, with the following caveat:
  - In a conference hosted by a Conductor-managed TelePresence Server, a Microsoft client cannot share its screen if the conference has dialed out to the Microsoft client. The Microsoft client can share its screen if it has dialed in to the conference.
- Screen sharing from Microsoft is supported when the Microsoft client is in conferences hosted on MCU 5300 Series or MCU MSE Series bridges, with the following caveat:
  - When another endpoint steals the floor from the Microsoft presenter, the MCU does not revoke the floor. The Microsoft client looks like it is still sharing, from the original presenter's point of view, when the other participants are not seeing the Microsoft user's screen. See issue number CSCux48258.
- Screen sharing from Microsoft is not supported when the Microsoft client is in conferences hosted on MCU 4200 Series and MCU 4500 Series bridges.

- Point to point calls with screen sharing from the Microsoft client have been tested and validated with TC, CE, and DX endpoints, with the following caveats:

  - TC endpoints must be running TC version 7.2 or later to be able to compose main video and content when they are presenting.

  - CE endpoints must be running CE version 8.0 or later to be able to compose main video and content when they are presenting.

  - DX Series endpoints must be running firmware version 10.2(5) or later. The DX Series cannot compose content and main video, so Microsoft users will see the content instead of the main video when these endpoints are presenting.

- We do support screen sharing from Microsoft to SIP or H.323 standards-based endpoints, but we cannot explicitly test and validate all cases.

- Cisco Jabber Video for TelePresence is not supported for point to point screen sharing from/to Microsoft clients.

- Cisco Jabber is not supported for point to point screen sharing from/to Microsoft clients.

Screen Sharing Performance Considerations

On all platforms, the default maximum number of concurrent transcoding sessions is 10. We recommend the following numbers, depending on your platform:

Table 4   Recommended Number of Desktop Transcode Sessions by Platform

On this platform:	Set **Maximum RDP transcode sessions** to:
Medium OVA	10
‡ CE500/ CE1000/ CE1100, or Large OVA	20
Clusters	Same as the individual platform setting. The **Maximum RDP transcode sessions** you enter on the primary applies to each peer in the cluster.

‡ From X8.10, the requirement to have a 10 Gbps NIC in order to achieve the scalability of a large system is removed. It is now possible to have the capacity of a large system with a 1 Gbps NIC subject to your bandwidth constraints.

These numbers were chosen conservatively. They are based on the additional CPU load caused by transcoding 1920 by 1080 screens while the Gateway Expressway was processing 100 concurrent 720p video calls from Microsoft.

If you want to increase the maximum number of sessions, consider the following:

- A screen share transcoding session requires more media ports than a video call, so you may need to increase the media port range; the default range accommodates 100 video calls, 20 of which are sharing their desktop.

- Screen share transcoding loads the CPU more heavily than video (AV) calls. Testing shows that CPU load increases in a roughly linear way when increasing the number of transcode sessions. There is a similar characteristic when increasing the number of AV calls without screen sharing, so you should be able to get more shares if the Expressway is processing fewer concurrent AV calls overall.

- Higher resolutions and/or multiple monitors also affect performance. The transcoder will output the same resolution that it receives from the Microsoft client, up to a maximum resolution of 1920x1200. Beyond that, the transcoder will scale the shared screen down to fit within 1920x1200. If the received resolution exceeds 3840x2160, the transcoder crops the screen to fit within that resolution before scaling it down. The transcoder will also scale down if it needs to respond to constraints on resources, for example, bandwidth limitations.

Screen Sharing Deployments

The following deployments support screen sharing from Microsoft clients:

Features and Limitations

Figure 2   Microsoft environment to conference managed by TelePresence Conductor trunked to Unified CM
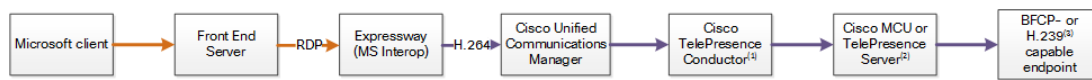
Figure 3   Microsoft environment to SIP endpoint registered to Unified CM
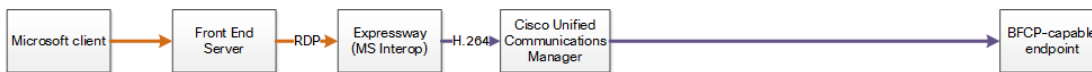
Notes:

1. If you use the Optimize Resources feature with Microsoft client screen sharing, you need the following software versions:
   - TelePresence Conductor XC4.0 or later
   - TelePresence Server 4.2 or later

2. Requires an H.323 registrar, not shown in the diagram.

Video Codecs

If you use Lync 2010 for Windows, the other video endpoints must support H.263; this is the common video codec supported by endpoints and the Lync client. (Lync 2010 for Windows does not support H.264)

The Lync 2010 client for Apple Mac OS X only supports RTVideo. It does not support H.263 or H.264. To make video calls between this client and Cisco Collaboration video endpoints, you need the Cisco AM GW to transcode between RTVideo and H.263/H.264.

Video codec selection

When the B2BUA receives a call with no SDP—that is, without a list of codecs that can be used for the call (for example, a call that has been interworked from H.323)—the B2BUA must populate the SDP with a "pre-configured" list of codecs from which the Microsoft client can select, because it does not support INVITES with no SDP.

The codecs offered and selected, therefore, may not reflect the best codecs that could have been selected by the endpoints.

Conferencing

Protocols

In this deployment, we do not support H.323 between Expressway and TelePresence Server. We recommend that you disable H.323 on the TelePresence Server.

Cisco TelePresence Server

Supported Microsoft clients can join conferences hosted on a TelePresence Server.

The TelePresence Server must be trunked to Unified CM or controlled by a TelePresence Conductor that is trunked to Unified CM.

Microsoft users can share their screen in a TelePresence Server conference. They will receive presentation from other participants in the composited video stream from the TelePresence Server.

Cisco TelePresence MCU Series

Supported Microsoft clients can join conferences hosted on a MCU.

The MCU must be trunked to Unified CM or controlled by a TelePresence Conductor that is trunked to Unified CM.

Microsoft users can share their screen in an MCU conference. They will receive presentation from other participants in the composited video stream from the MCU.

There is a known issue with the MCU which does not revoke the floor after it stops sharing the content from the Microsoft client. To the Microsoft user it looks like they are still sharing the screen, but other participants have stopped seeing the screen.

Lync Conference (AV MCU) not supported

When a point to point call involves a standards-based endpoint and a Microsoft client, you cannot invite a third party into the call because the Microsoft client tries to start a Lync conference. The Expressway and the standards-based endpoints do not support endpoints joining Lync conferences.

Configuration

Prerequisites

Microsoft Environment

- FE Servers are running Lync Server 2010, Lync Server 2013, or Skype for Business Server 2015.

  Note:

  During our next major release (after X8.8), we are no longer working with Microsoft Lync Server 2010 and associated clients. We cannot guarantee that newer features will work as expected with these products.

  If you are using Lync Server 2010 and associated clients, we recommend that you upgrade your Microsoft environment to Lync Server 2013 or Skype for Business Server 2015.

- Microsoft FE Server is configured and operational and you have access to Active Directory for managing users.

- The server topology has successfully been validated using the Topology Validation Tool.

- Microsoft clients should be able to call each other (there is more detail on setting this up in Verify Calls Between Microsoft Clients, page 76).

Cisco Collaboration Environment

- Minimum versions: The dedicated Gateway Expressway(s) must be running X8.1 or later for video interoperability.

  X8.6 or later is required for Microsoft client screen sharing. X8.7 or later is required for Microsoft client screen sharing through a clustered Gateway Expressway.

  X8.8 or later is required for brokering SIP SIMPLE from Microsoft infrastructure towards Cisco Unified Communications Manager IM and Presence Service.

- The Expressway pair at the network edge is configured as described in *Cisco Expressway Basic Configuration Deployment Guide* on the Cisco Expressway Configuration Guides page.

- Unified CM is trunked to the Cisco Expressway-C as described in *Cisco Expressway and CUCM via SIP Trunk Deployment Guide* on the Cisco Expressway Configuration Guides page.

- The Gateway Expressway cluster must have Rich Media Session licenses.

- Each Gateway Expressway peer must have a Microsoft Interoperability key.

- The Expressway-E (cluster) must have a TURN Relay licenses (for calls from off-site Microsoft users).

- Unified CM-registered endpoints should be able to call each other.

Configuration

DNS Records

- The FQDNs of all Microsoft FE servers are resolvable by the DNS server used by the Gateway Expressway (Gateway Expressway and FE Servers should use the same DNS server).
- The FQDNs of each Gateway Expressway is resolvable by DNS. If the Gateway Expressway is a cluster, the FQDN of the cluster must be resolvable by DNS (with a round-robin A-record for each peer).
- The DNS server must support reverse DNS lookup (typically by PTR records) if you enable TLS (recommended).

Configuration Overview

This document describes how to configure Lync and the Expressway in B2BUA mode to enable:

1. Unified CM-registered endpoints to call internal or external Lync clients registered to Lync (Enable Calls to Microsoft Environment, page 18)
2. Internal or external Lync clients to call Unified CM-registered endpoints (Enable Calls from Microsoft Environment, page 38 and Enable Calls from External Microsoft Clients, page 45)
3. Screen sharing from Lync clients to Unified CM-registered endpoints (Enable Screen Sharing from Microsoft, page 47)
4. Chat/presence between Cisco Jabber and Microsoft soft clients (Lync 2013, Skype for Business)

   See Enable Chat / Presence from Microsoft Clients, page 47.

The configuration process describes each of these stages separately, so that individual stages can be implemented and tested before moving on to the next.

Enable Calls to Microsoft Environment

Table 5   Overview of Tasks Required to Enable Calls from Collaboration Endpoints to Microsoft Clients (All Internal)

Command or Action	Purpose
Configure the Gateway Expressway, page 18	Prepare the Gateway Expressway to work in your environment: configure DNS and NTP, and enter a cluster name
Trunk the Gateway Expressway to Unified CM, page 20	To route calls destined for Microsoft domains towards the Gateway Expressway
Connecting Expressway to Unified CM Using TLS, page 26	Secure the trunk to the Unified CM to enable encrypted media between Unified CM registered endpoints and Microsoft clients
Configure Microsoft Server Environment , page 31	Enable SIP TLS, trust the Gateway Expressway, and configure media encryption
Configure the Microsoft Interoperability Service and Search Rules on the Gateway Expressway, page 34	To route calls destined for Microsoft domains towards the internal Microsoft environment
Test Calls from Internal Endpoint to Internal Microsoft Client, page 37	To verify this part of the configuration.

Configure the Gateway Expressway

Table 6   Prepare the Gateway Expressway for the Network

Command or Action	Purpose
Task 1: Configure DNS and Local Hostname, page 18	So that the Gateway Expressway can resolve trusted Microsoft Servers (B2BUA hosts)
Task 2: Enter a Cluster Name, page 19	So that Microsoft Server static routes can resolve the Gateway Expresswaycluster
Task 3: Configure an NTP Server, page 19	To synchronize the Gateway Expressway with the Microsoft Server environment

Task 1: Configure DNS and Local Hostname

Configure the DNS Server Details

If possible, you should configure the Gateway Expressway peers to use the same DNS servers used by the FE Servers.

On a Microsoft Server:

1. From the Windows **Start** menu choose **Run**.
2. Type `cmd` into the **Open** field and click *OK*. A command window opens.
3. In the cmd.exe window type:

Configuration

```
ipconfig /all
```
4. Note down the DNS server addresses.

Note: a DNS server IP address of 127.0.0.1 means that the FE Server is using a DNS server on its own hardware. Instead of entering 127.0.0.1 on the Expressway, use the IP address of the FE Server platform instead.

On each Gateway Expressway peer:

1. Go to **System > DNS**.
2. If the DNS server that the FE Server uses can provide all DNS lookups needed by Expressway:
   a. Set **Default DNS Server Address 1** to the IP address of DNS server noted earlier.
   b. If the FE Server has more than one DNS server defined, configure the additional default DNS server fields (**Address 2**, **Address 3** and so on) with the IP addresses of the additional servers.
3. [Conditional] If the Expressway is already using different DNS servers for other types of calls, you can use the **Per-domain DNS servers** feature to add the Microsoft environment's DNS servers and domains.
4. [Conditional] If necessary, configure a **Per-domain DNS server address** to contain the address of the Front End Server, and enter the Microsoft domain e.g. `example.com` as the associated **Domain name**.

   (This may be required in some network setups: If the Microsoft Server embeds hostnames inside contact headers, these may be unresolvable outside of the Windows domain.)
5. Click **Save**.

Enter System Host Name and DNS Domain

Give each Gateway Expressway peer a unique **System host name** and check it has the correct **DNS Domain**:

1. Go to **System > DNS** and set:
   a. **System host name** to a unique hostname for this Expressway.
   b. **Domain name** to the domain name for this Expressway.
2. Click **Save**.

   Note:

   ■ Concatenate **System host name** with **Domain name** to get the routable FQDN of this Expressway

   ■ These items must be configured to properly enable TLS between Expressway and the Microsoft environment.

   If they are not, the neighbor zone may go active and Expressway may send messaging to the FE Server, but the FE Server will never open a TLS connection back to Expressway.

Task 2: Enter a Cluster Name

You will configure Microsoft FE Server with a static route that always uses the Gateway Expressway's cluster name / FQDN.

For each Gateway Expressway peer (even if there is only one), ensure that **Cluster name** (**System > Clustering > Cluster name**) is the FQDN of the cluster. You may have created the FQDN when setting up the cluster. See *Expressway Cluster Creation and Maintenance Deployment Guide* if you need to change the cluster name.

Task 3: Configure an NTP Server

On each Gateway Expressway peer:

1. Go to **System > Time**.
2. Set **NTP server 1** to the IP address of an NTP server.

Configuration

3. (Optional) Enter the details of additional NTP servers.

4. Set **Time zone** as appropriate to the location of the Expressway.

To find out which time server the FE Server is using, enter `net time /querysntp` at the Windows command line.

Trunk the Gateway Expressway to Unified CM

Table 7   Task summary for trunking the Gateway Expressway to Unified CM

Command or Action	Purpose
Task 1: Check Unified CM Configuration, page 20	Check that Unified CM has the required configuration for trunking to Gateway Expressway.
Task 2: (Pre 9.x) Configure the SIP Profile for Expressway, page 21	Not required for Unified CM 9.x or later. Configure a SIP profile for Expressway.
Task 3: Configure the Region Session Bit Rate for Video Calls, page 23	Prepare the Unified CM region for higher bitrates required by video calls.
Task 4: Configure the SIP Trunk Security Profile, page 23	Prepare the **non-secure** SIP trunk profile for trunking to Gateway Expressway. **Note:** Not required if you are going to use SIP TLS on the trunk. This task is replaced by the corresponding task Configure a SIP Trunk Security Profile on Unified CM, page 29, in the next section Connecting Expressway to Unified CM Using TLS, page 26.
Task 5: Configure the SIP Trunk to the Gateway Expressway, page 23	Create the trunk to the Gateway Expressway.
Task 6: Configure the SIP Trunk to the Cisco Expressway-C, page 25	Create the trunk to the Cisco Expressway-C.
Task 7: Configure the Clusterwide Domain Enterprise Parameters, page 25	Check that the Unified CM has fully qualified domain in the same video network as the Gateway Expressway
Task 8: Check the Message Size Limit on Unified CM, page 26	Make sure the incoming SDP message size in Unified CM is set to an appropriate value. In older versions, the SDP message size was too small for video applications, but the default has changed to 11000 bytes.

Task 1: Check Unified CM Configuration

Ensure that Unified CM contains a basic configuration and has already set up at least:

- System > Server
- System > Cisco Unified CM
- System > Cisco Unified CM Group
- System > Date / Time Group
- System > Presence Group
- System > Region Information
- System > Device Pool
- System > DHCP
- System > Location

Configuration

- System > Physical location
- System > Enterprise parameters
- System > Licensing

Task 2: (Pre 9.x) Configure the SIP Profile for Expressway

Note: This procedure does not apply to Unified CM versions 9.x and later, because the newer versions have a "Standard SIP Profile For Cisco VCS" (you can also use that profile for Expressway).

1. On Unified CM, go to **Device > Device Settings > SIP Profile**.
2. Click **Copy** against the **Standard SIP Profile**.

3. Configure the fields as follows (leave other fields as default values):

Name	"Standard SIP Profile For Cisco VCS" (the profile is named "for Cisco VCS" for consistency with other Unified CM versions)
Default MTP Telephony Event Payload Type	101
Redirect by Application	Select the check box
Use Fully Qualified Domain in SIP Requests	Select the check box
Allow Presentation Sharing using BFCP	Select the check box (in Unified CM 8.6.1 or later)
Timer Invite Expires	180
Timer Register Delta	5
Timer Register Expires	3600
Timer T1	500
Timer T2	Leave as default (typically 4000 or 5000)
Retry INVITE	6
Retry non-INVITE	10
Start Media Port	16384
Stop Media Port	32766
Call Pickup URI	x-cisco-serviceuri-pickup
Call Pickup Group Other URI	x-cisco-serviceuri-opickup
Call Pickup Group URI	x-cisco-serviceuri-gpickup
Meet Me Service URI	x-cisco-serviceuri-meetme
Timer Keep Alive Expires	120
Timer Subscribe Expires	120
Timer Subscribe Delta	5
Maximum Redirections	70
Off Hook To First Digit Timer	15000
Call Forward URI	x-cisco-serviceuri-cfwdall
Abbreviated Dial URI	x-cisco-serviceuri-abbrdial
Reroute Incoming Request to new Trunk based on	Never

4. Click **Save**.

Configuration

Task 3: Configure the Region Session Bit Rate for Video Calls

Ensure that your regions have an appropriate session bit rate for video calls:

1. Go to **System > Region Information > Region**.
2. Select the region (for example the **Default** region).
3. Set **Maximum Session Bit Rate for Video Calls** to a suitable upper limit for your system, for example 6000 kbps.
4. Click **Save** and then click **Apply Config**.

Task 4: Configure the SIP Trunk Security Profile

1. Go to **System > Security > SIP Trunk Security Profile**.
2. (Before version 9.x) Click **Add New** and name the new profile.
3. (9.x onwards) Select **Non Secure SIP Trunk Profile**.
4. Configure the fields as follows:

Name	Non Secure SIP Trunk Profile
Device Security Mode	Non Secure
Incoming Transport Type	TCP+UDP
Outgoing Transport Type	TCP
Incoming Port	5060 Use a different port (such as 5070 or 5071) if you are using 5060 for MRA registrations. The reason is to avoid potential issues with MRA if Unified CM receives registration requests on what it believes to be a SIP trunk. This applies to TCP or TLS connections.
Accept Unsolicited Notification	Select this check box
Accept Replaces Header	Select this check box

5. Click **Save**.

Task 5: Configure the SIP Trunk to the Gateway Expressway

1. On Unified CM, go to **Device > Trunk**.
2. Click **Add New**.
3. Select a **Trunk Type** of *SIP Trunk*.
   – **Device Protocol** displays *SIP*.
   – If asked for a **Trunk Service Type**, select *None (Default)*.
4. Click **Next**.

5. Configure the **Device Information** fields as follows:

Device Name	As required, such as Expressway_system
Device Pool	(As set up in System > Device Pool)
Call classification	OnNet
Location	(As set up in System > Location)
Packet Capture Mode	None
Media Termination Point Required	Clear this check box if any video phones registered to Unified CM are to make or receive video calls with endpoints routed via Expressway. Select this check box if audio devices only are registered to Unified CM.
SRTP Allowed	Select this check box. For background, read Secure RTP between CUCM and VCS or Expressway Configuration Example
Run On All Active Unified CM Nodes	Select this check box

6. Configure the **Call Routing Information > Inbound Calls** fields as follows:

Significant digits	All
Connected Line ID Presentation	Default
Connected Name Presentation	Default
Calling Search Space	(As set up in **Call Routing > Class of Control > Calling Search Space**)
Prefix DN	<blank>
Redirecting Diversion Header Delivery – Inbound	Select this check box

7. Configure the **Call Routing Information > Outbound Calls** fields as follows:

Calling Party Selection	Originator
Calling Line ID Presentation	Default
Calling Name Presentation	Default
Caller ID DN	<blank>
Caller Name	<blank>

8. Configure the **SIP Information** fields as follows:

Destination address is an SRV	Select this check box if a domain is specified for the destination address, and the DNS server uses DNS SRV records to direct the domain to a cluster of Expressways. Do not select this check box if an IP address is specified as the **Destination address**.
Destination address	<FQDN of Expressway / Expressway cluster>. Alternatively you can enter the <IP address of Expressway>. If you are not using SRV records and need to specify multiple peers, click 🔳 to add extra **Destination address** rows.
Destination port	5060 (this displays as zero if you are using SRV records)
Presence Group	Standard Presence Group (or whichever presence group has been configured in **System > Presence Group**)
SIP Trunk Security Profile	Non Secure SIP Trunk Profile
SIP Profile	Standard SIP Profile for Cisco VCS
DTMF Signaling Method	RFC 2833
Normalization Script	vcs-interop (if available, the vcs-interop script may be used with Expressway)

9. Click **Save**.
10. Click **Reset**.
11. Click **Reset**.

Task 6: Configure the SIP Trunk to the Cisco Expressway‑C

If there is not already a trunk between the Unified CM and the Cisco Expressway‑C, then you need to create one as described in in *Cisco Expressway and CUCM via SIP Trunk Deployment Guide* on the Cisco Expressway Configuration Guides page.

Task 7: Configure the Clusterwide Domain Enterprise Parameters

Unified CM must be configured with a **Cluster Fully Qualified Domain Name** so that it can receive calls to addresses in the format <address>@domain. (It is also required when Unified CM is clustered so that Expressway can send the call to any Unified CM node.)

1. Go to **System > Enterprise parameters**, and find the **Clusterwide Domain Configuration** section.
2. Set the **Organization Top Level Domain** to the same domain as the video network, for example video.example.com.

   This ensures that the correct domain of the calling party is displayed to the called party.
3. Set the **Cluster Fully Qualified Domain Name** to the same domain as the video network, for example video.example.com.

   This parameter defines one or more Fully Qualified Domain Names (FQDNs) for this cluster. Multiple FQDNs must be separated by a space. Requests containing URLs (for example, SIP calls) whose host portion matches any of the FQDNs in this parameter will be recognized as a request destined for this cluster and/or devices attached to it.
4. Click **Save**.

Configuration

Task 8: Check the Message Size Limit on Unified CM

SIP messages for video are considerably larger than SIP messages for audio calls, in particular, when a Cisco TelePresence Server is used in the video network.

Ensure that the **SIP Max Incoming Message Size** on Unified CM is set to 11000:

1. Go to **System > Service Parameters**.
2. Select the appropriate server.
3. Select *Cisco CallManager (Active)* as the service.
4. Select **Advanced**.
5. In the **Clusterwide Parameters (Device - SIP)** configure the field as follows:

SIP Max Incoming Message Size	11000

6. Click **Save**.

Connecting Expressway to Unified CM Using TLS

These instructions explain how to take a system that is already configured and working using a TCP interconnection between Expressway and Unified CM, and to convert that trunk to use TLS instead.

Note: CiscoSSL was upgraded to version 5.4.3 in Expressway X8.7.2. Cisco SSL version 5.4.3 rejects keys with fewer than 1024 bits when doing Diffie-Hellman (DH) key exchange. As a result, **SSL interoperability is prevented with versions 9.x and earlier of Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service**. This is because those products generate 768 bit keys for D-H key exchange.

This table summarizes the process to convert to TLS:

Table 8   Overview of Tasks to Create SIP TLS Trunk Between Expressway and Unified CM

Command or Action
Ensure Certificate Trust Between Unified CM and Expressway, page 27
Set the Cluster Security Mode to Mixed Mode, page 28
Configure a SIP Trunk Security Profile on Unified CM, page 29
Update Device Profiles to Encrypt Calls to Unified CM-registered Endpoints, page 31
Update the Unified CM Trunk to Expressway to Use TLS, page 30

Configuration

Table 8   Overview of Tasks to Create SIP TLS Trunk Between Expressway and Unified CM (continued)

Command or Action
Update the Expressway Neighbor Zone to Unified CM to Use TLS, page 31
Verify That the TLS Connection is Operational, page 31

Ensure Certificate Trust Between Unified CM and Expressway

For Unified CM and Expressway to establish a TLS connection with each other:

- Expressway and Unified CM must both have valid server certificates loaded (you must replace the Expressway's default server certificate with a valid server certificate)
- Expressway must trust Unified CM's server certificate (the root CA of the Unified CM server certificate must be loaded onto Expressway)
- Unified CM must trust Expressway's server certificate (the root CA of the Expressway server certificate must be loaded onto Unified CM)

See *Expressway Certificate Creation and Use Deployment Guide* for full details about loading certificates and how to generate CSRs on Expressway to acquire certificates from a Certificate Authority (CA).

Note: In a clustered environment, you must install CA and server certificates on each peer/node individually.

We strongly recommend that you do not use self-signed certificates in a production environment.

Load Server and Trust Certificates on Expressway

Expressway server certificate

Expressway has only one server certificate. By default, this is a certificate signed by a temporary certificate authority. We recommend that it is replaced by a certificate generated by a trusted certificate authority.

To upload a server certificate:

1. Go to **Maintenance > Security > Server certificate**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the **server certificate** PEM file.
3. If you used an external system to generate the Certificate Signing Request (CSR) you must also upload the **server private key** PEM file that was used to encrypt the server certificate. (The private key file will have been automatically generated and stored earlier if the Expressway was used to produce the CSR for this server certificate.)
   - The **server private key** PEM file must not be password protected.
   - You cannot upload a server private key if a certificate signing request is in progress.
4. Click **Upload server certificate data**.

Note: If you are using Unified CM version 8.5(1) or earlier and are having problems establishing a TLS connection between Expressway and Unified CM, we recommend adding the following x509 extended key attributes into the CSR:

- serverAuth (1.3.6.1.5.5.7.3.1) -- TLS Web server authentication
- clientAuth (1.3.6.1.5.5.7.3.2) -- TLS Web client authentication
- ipsecEndSystem (1.3.6.1.5.5.7.3.5) -- IP security end system

Expressway trusted CA certificate

The **Trusted CA certificate** page (**Maintenance > Security > Trusted CA certificate**) allows you to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway. When a TLS connection to Expressway

Configuration

mandates certificate verification, the certificate presented to the Expressway must be signed by a trusted CA in this list and there must be a full chain of trust (intermediate CAs) to the root CA.

The root CA of the Unified CM server certificate must be loaded into the Expressway's trusted CA certificate list.

To upload a new file containing one or more CA certificates, **Browse** to the required PEM file and click **Append CA certificate**. This will append any new certificates to the existing list of CA certificates. If you are replacing existing certificates for a particular issuer and subject, you have to manually delete the previous certificates.

Repeat this process on every Expressway that will communicate with this Unified CM.

Load Server and Trust Certificates on Unified CM

Certificate management for Unified CM is performed in the **Cisco Unified OS Administration** application.

All existing certificates are listed under **Security > Certificate Management**. Server certificates are of type *certs* and trusted CA certificates are of type *trust-certs*.

Unified CM server certificate

By default, Unified CM has a self-signed server certificate **CallManager.pem** installed. We recommend that this is replaced with a certificate generated from a trusted certificate authority.

Unified CM trusted CA certificate

To load the root CA certificate of the authority that issued the Expressway certificate (if it is not already loaded):

1. Click **Upload Certificate/Certificate chain**.
2. Select a **Certificate Name** of *CallManager-trust*.
3. Click **Browse** and select the file containing the root CA certificate of the authority that issued the Expressway certificate.
4. Click **Upload File**.

Repeat this process on every Unified CM server that will communicate with Expressway. Typically this is every node that is running the CallManager service.

Set the Cluster Security Mode to Mixed Mode

The Cisco Unified Communications Manager cluster must be in Mixed Mode to allow the registration of both secure devices and non-secure devices. This allows for best effort encryption between the Expressway and the Cisco Unified Communications Manager. Read Secure RTP between CUCM and VCS or Expressway Configuration Example for background on best effort encryption between Expressway and Unified CM.

Note: This requirement relates to media encryption. Unified CM does **not** need to be in Mixed Mode to support TLS SIP trunks.

As of version 10.0, you can use the CLI to change the cluster security mode. On earlier versions, you must use the Cisco CTL Client plugin to change the cluster security mode. The security mode change updates the CTL file, so you must restart the Cisco CallManager and Cisco Tftp services after the change.

The process is summarized below, but you should refer to the *Cisco Unified Communications Manager Security Guide* for your version, which you can find on the Cisco Unified Communications Manager (CallManager) Maintain and Operate Guides page.

1. Obtain access to the Unified CM publisher node, including hardware security tokens (if using the CTL Client plugin).
2. (Pre 10.0) Download and install the Cisco CTL Client plugin from Unified CM.

3. Run the CTL Client plugin to enable Mixed Mode. On 10.0 or later, you can use `utils ctl set-cluster mixed-mode` at the CLI.
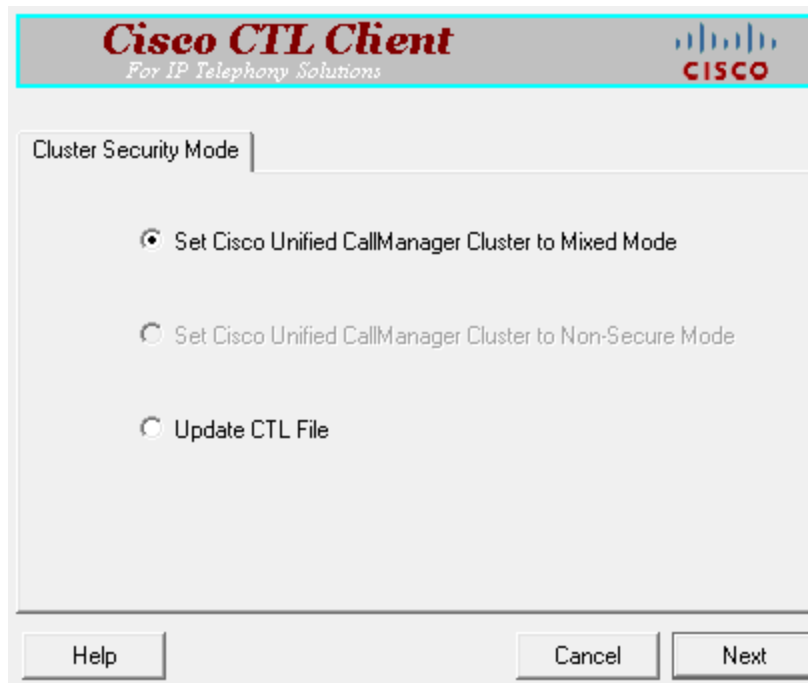
4. Update the CTL file (via the plugin or `utils ctl update CTLFile`).
5. Restart the Cisco CallManager and Cisco Tftp services (via Cisco Unified Serviceability).

Configure a SIP Trunk Security Profile on Unified CM

On Unified CM:

1. Select **Cisco Unified CM Administration**, click **Go** and log in.
2. Go to **System > Security > SIP Trunk Security Profile**.
3. Click **Add New**.

4. Configure the fields as follows:

Name	A name indicating that this is an encrypted profile.
Description	Enter a textual description as required.
Device Security Mode	*Encrypted*.
Incoming Transport Type	*TLS*.
Outgoing Transport Type	*TLS*.
Enable Digest Authentication	Leave unselected.
X.509 Subject Name	The subject name or a subject alternate name provided by the Expressway in its certificate. For Expressway clusters, ensure that this list includes all of the names contained within all of the peers' certificates. To specify multiple X.509 names, separate each name by a space, comma, semicolon or colon.
Incoming Port	5061 Use a different port (such as 5070 or 5071) if you are using 5061 for MRA registrations. The reason is to avoid potential issues with MRA if Unified CM receives registration requests on what it believes to be a SIP trunk. This applies to TCP or TLS connections.
Accept Unsolicited Notification	Select this check box
Accept Replaces Header	Select this check box
Other parameters	Leave all other parameters unselected.

5. Click **Save**.

Update the Unified CM Trunk to Expressway to Use TLS

On Unified CM:

1. Go to **Device > Trunk**.
2. Using Find, select the **Device Name** previously set up for the trunk to the Expressway.
3. Configure the following fields:

SIP Information section	
Destination Port	5061 (unless using DNS SRV, in which case ensure the SRV records are set up correctly).
SIP Trunk Security Profile	Select the trunk profile set up above.

Leave other parameters as previously configured.

4. Click **Save**.
5. Click **Reset**.

Update Device Profiles to Encrypt Calls to Unified CM-registered Endpoints

Endpoints registered to Unified CM need to be configured with a "SIP Secure profile" to provide encrypted media and call negotiation. If such profiles are not available by default, create them at **System > Security > Phone Security**. On the secure profiles, you must set **Device Security Mode** to *Encrypted*.

See *Securing Cisco TelePresence Products* for further information on using the Cisco CTL Client and configuring Unified CM for secure communications.

Update the Expressway Neighbor Zone to Unified CM to Use TLS

Note that Expressway will report that the Unified CM zone is active even while it is communicating with Unified CM over TCP. The changes below are necessary to enable communications over TLS.

On Expressway:

1. Go to **Configuration > Zones > Zones**, then select the zone to Unified CM.
2. Configure the following fields:

SIP section	
Port	5061
Transport	*TLS*
TLS verify mode	*On*
Authentication trust mode	*Off*

Leave other parameters as previously configured.

3. Click **Save**.

Verify That the TLS Connection is Operational

To verify correct TLS operation, check that the Expressway zone reports its status as active and then make some test calls.

1. Check the Expressway zone is active:

   a. Go to **Configuration > Zones > Zones**.
   b. Check the **SIP status** of the zone.

   If the zone is not active, try resetting or restarting the trunk again on Unified CM.

2. Make test calls from Expressway registered endpoints to a Unified CM phone.
3. Make test calls from a Unified CM phone to Expressway registered endpoints.

Configure Microsoft Server Environment

- Task 1: Trust the Gateway Expressway, page 31
- Task 2: Configure Microsoft FE Server Media Encryption Capabilities, page 33

Task 1: Trust the Gateway Expressway

You must create a trusted application pool for each Expressway Gateway cluster, and then add subordinate peers to the application pool. You must then create a trusted application for each pool, and finally enable the new topology.

The context for the following procedure depends on your Microsoft environment, as follows:

Configuration

- If a Director is in use, then configure the Director (pool) to trust the Gateway Expressway and to route traffic to it.

    Other FE Servers receiving calls for the video domain may not know how to route them (depending on Microsoft SIP routing configuration), and may pass the calls to the Director pool for routing.

- If there is a hardware load balancer in front of a set of FE server pools, configure each server pool.
- If there is just a single Microsoft FE Server, configure that server.

Note: When you run the following shell commands, you could see warnings that the machine names were not found in the Active Directory domain. Ignore these warnings, because you do not need to add the Gateway Expressway to the AD domain.

1. Open the Management Shell.
2. Use the command `New-CsTrustedApplicationPool` to create a trusted application pool for each Gateway Expressway cluster.

    Example Command

    ```
    C:\Users\Administrator.example>New-CsTrustedApplicationPool -Identity lyncexp.video.example.com -
    ComputerFqdn exp01.video.example.com -Registrar fepool.example.com -site 1 -RequiresReplication $false
    -ThrottleAsServer $true -TreatAsAuthenticated $true
    ```

    Table 9   Parameter Reference

`-Identity`	The Gateway Expressway **cluster** FQDN, which must match the Common Name or a Subject Alternate Name on the Expressway server certificate
`-ComputerFqdn`	The Gateway Expressway **peer** FQDN (or the primary's FQDN if running a cluster), which must match the Common Name on the Expressway server certificate.
`-Registrar`	The FQDN of the registrar for the FE server pool.
`-Site`	Specifies the siteID on which this application pool is homed. You can use `Get-CsSite` for a list of sites (SiteID) and related pools.
`-RequiresReplication $false`	Specifies that the trusted application must not be replicated between Pools.
`-ThrottleAsServer $true`	Reduces the message throttling because the trusted device is a server, not a client.
`-TreatAsAuthenticated $true`	Specifies that this application is authenticated by default.

Configuration

3. If the Gateway Expressway is a cluster, use the command `New-CsTrustedApplicationComputer` to add subordinate peers to the trusted application pool.

Example Command

```
C:\Users\Administrator.example> New-CsTrustedApplicationComputer -Identity exp02.video.example.com -
Pool lyncexp.video.example.com
```

Table 10   Parameter Reference

`-Identity`	The FQDN of the Expressway peer you're adding, eg. exp02.video.example.com, which must match the Common Name on the peer's server certificate.
`-Pool`	The FQDN of the application pool (the value of `-identity` when you created the application pool).

4. Use the command `New-CsTrustedApplication` to assign a new application to the trusted application pool.

Example Command

```
C:\Users\Administrator.example>New-CsTrustedApplication -ApplicationId ExpresswayApplication1 -
TrustedApplicationPoolFqdn lyncexp.video.example.com -Port 65072
```

Table 11   Parameter Reference

`-ApplicationID`	Names the Gateway Expressway application (this is only used by the Microsoft FE server, it is not a DNS name).
`-TrustedApplicationPoolFQDN`	Specifies the FQDN of the Gateway Expressway.
`-Port`	Specifies TLS/TCP port to use for neighboring, which must match the **Port on B2BUA for Microsoft call communications** on the Gateway B2BUA (default 65072).

5. Run the command `Enable-CsTopology` to enable the configuration.

6. To read and check the application pool and application configurations, use `Get-CsTrustedApplicationPool` and `Get-CsTrustedApplication`.

Task 2: Configure Microsoft FE Server Media Encryption Capabilities

The Microsoft Server defaults to mandatory media encryption, which you may need to change to suit your video network. To read the current media encryption policy, use `get-CsMediaConfiguration`. The default `EncryptionLevel` is `RequireEncryption`.

Also, the headers used in Microsoft SRTP are different from those used by Cisco Collaboration devices. The Expressway B2BUA can modify these headers if the Gateway Expressway has the **Microsoft Interoperability** option key.

When Should I Consider Changing the Default Encryption on Microsoft FE Server?

Your decision depends on the following factors:

- **Is the connection between Microsoft and the Gateway Expressway made over TLS?**

  If the connection is TLS, then mandatory encryption is possible.

  If the connection is not TLS, then the crypto keys will not be sent across the unsecure connection. Mandatory encryption will be impossible and calls will fail. In this case, you must change the default media encryption on Microsoft Server.

Configuration

- **Does the Gateway Expressway have the Microsoft Interoperability option key?**

  This key is required for all Microsoft Interoperability with versions later than Lync Server 2010. If it is installed on the Gateway Expressway, then mandatory encryption is possible.

  The Gateway Expressway might not have this key when interworking with Lync Server 2010. In this case, mandatory encryption will be impossible because the B2BUA will not be able to modify the SRTP headers from Lync. You must change the default media encryption on Lync Server in this case.

- **Do all video endpoints in the network support encrypted media and offer encrypted media?**

  If some endpoints cannot do media encryption, then mandatory encryption will not always work.

How do I Change the Media Encryption Policy on the Microsoft Server?

To configure the media encryption policy, use `Set-CsMediaConfiguration` as follows:

`set-CsMediaConfiguration -EncryptionLevel <value>` where `<value>` is one of `RequireEncryption`, `SupportEncryption`, `DoNotSupportEncryption`.

For example:

`C:\Users\Administrator.example> set-CsMediaConfiguration -EncryptionLevel SupportEncryption`

See TechNet article on Set-CsMediaConfiguration.

Note:

- `EncryptionLevel` is communicated to Microsoft clients and changes their operation. Users must sign out of the Microsoft client and sign back in.

  You may have to wait (up to an hour, depending on complexity) for `EncryptionLevel` to propagate throughout the pool. Restarting Microsoft clients too soon may not change their media encryption policy.

- If the Gateway Expressway has the **Microsoft Interoperability** option key AND it makes a TLS connection to the Microsoft Server, then you can use the default setting `-EncryptionLevel RequireEncryption`.

  In this case, all video endpoints must support encryption or calls will fail. If some endpoints cannot do media encryption, you should use `-EncryptionLevel SupportEncryption`.

Configure the Microsoft Interoperability Service and Search Rules on the Gateway Expressway

- Task 1: Configure the Microsoft Interoperability Service on the Gateway Expressway, page 34
- Task 2: Create a Search Rule to Route Calls to Microsoft Environment, page 35
- Task 3: (If Required) Create Search Rules to Route Calls to Other Domains Supported on Microsoft, page 36

Task 1: Configure the Microsoft Interoperability Service on the Gateway Expressway

The values you enter for **Destination address** and **Listening port** depend on the structure of the Microsoft environment:

If the Microsoft environment...	Configure the signaling destination address and port to be that of the...
is fronted by a Hardware Load Balancer in front of Directors	Hardware Load Balancer
is fronted by a Director or Director pool	Director (pool)
has no Director but has a Hardware Load Balancer in front of Front End Servers	Hardware Load Balancer
is a single FE Server or FE Server Pool	The FE Server or pool

1. Go to **Applications > B2BUA > Microsoft interoperability > Configuration**.
2. Configure the fields as follows:

Microsoft Interoperability	*Enabled*
Destination address	IP address or FQDN of device specified above, for example dirpool.example.com
Listening port	IP port used by device specified above – typically 5061
Signaling transport	*TLS*
Enable RDP transcoding for this B2BUA	*Yes* enables screen sharing from Microsoft clients towards Cisco Collaboration endpoints. The **Maximum RDP transcode sessions** is 10 by default. Click **Show advanced settings** to change that if necessary.
Enable external transcoders for this B2BUA	*No*
Enable broker for inbound SIP	*No*
Offer TURN Services	*No*
Advanced settings	Leave all advanced settings at their default values, unless otherwise indicated

3. Click **Save**.

   The Microsoft Interoperability B2BUA is active now, and a non-configurable neighbor zone called **To Microsoft destination via B2BUA** has been created for you.

Task 2: Create a Search Rule to Route Calls to Microsoft Environment

Search rules are used to specify the URIs to be forwarded to Microsoft (for example, by matching the domain of the destination or by matching some element in the URI).

Search rules can also be used to transform URIs before they are sent to a neighbor, for example to add or modify the domain or add, remove or translate user-id prefixes and even to add extra tags to SIP URIs.

For this scenario, any calls to the domain example.com will be matched (and passed to Microsoft via the B2BUA); no transformation is required.

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.

3. Configure the search rule so that all calls to URIs in the format `identifier@example.com.*` are forwarded to Microsoft.

Rule name	To Microsoft environment
Priority	100
Source	*Any*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	`.+@example\.com`
Pattern behavior	*Leave*
On successful match	*Stop*
Target zone	*To Microsoft destination via B2BUA*

4. Click **Save**.

Note: never use a **Mode** of *Any alias*. Always use a pattern string which matches the Microsoft domain as closely as possible so that only calls, notifies and other messages that are handled by Microsoft get sent to it. If *Any alias* were to be selected, then all calls and other messages would be routed to Microsoft – subject to no higher priority search rules matching – whether or not Microsoft supports that call.

This misconfiguration could introduce delays or cause calls to fail.

Task 3: (If Required) Create Search Rules to Route Calls to Other Domains Supported on Microsoft

If the Microsoft environment supports only a single domain then no other search rules area required here. If ther are other domains and video endpoints should be able to call these devices, you need one or more additional search rules.

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the search rule so that all calls to the relevant URI are routed to Microsoft.

Rule name	xxxx To Microsoft
Priority	100
Source	*Any*
Mode	*Alias pattern match* (never use a **Mode** of *Any alias*)
Pattern type	*Regex*
Pattern string	.+@<relevant domain>.*
Pattern behavior	*Leave*
On successful match	*Stop*
Target zone	*To Microsoft destination via B2BUA*

4. Click **Save**.
5. Repeat for all domains supported on Microsoft (that are not used in the video network).

Calls can now be made between SIP endpoints registered on the video network to Microsoft clients registered on Microsoft FE Server.

Test Calls from Internal Endpoint to Internal Microsoft Client

Test calls from endpoints registered on the video network to Microsoft clients.

For example, call david.jones@example.com or alice.parkes@example.com from endpoints registered on Unified CM.

Note that if Lync for Mac OS X is used and a Cisco AM GW is not installed, the call will result in an audio only call as Lync for Mac does not support any video codecs supported by standards-based endpoints.

Enable Calls from Microsoft Environment

Table 12   Overview of Tasks Required to Enable Calls from Lync Clients to Collaboration Endpoints (All Internal)

Command or Action	Purpose
Configure the B2BUA Trusted Hosts, page 38	Provide the Microsoft Interoperability service on the Gateway Expressway with a list of sources of Microsoft calls. The addresses you need depends on how the Microsoft environment is structured.
Neighbor the Gateway to the Unified CM, page 39	Route Microsoft-originated calls from the Gateway Expressway to the Unified CM.
Configure Static Routes from Microsoft FE Server to Gateway Expressway, page 43	Enable FE Server to route calls for unrecognized destination aliases to the Gateway Expressway.
Test Calls from Internal Microsoft Client to Internal Endpoint, page 44	To verify that calls from Microsoft clients are routed properly.

Configure the B2BUA Trusted Hosts

When you're creating static routes from the Microsoft environment, you must configure the B2BUA to trust the hosts at the source of those routes. The hosts that the Expressway needs to trust depend on the structure of the Microsoft environment:

If...	Trust the...
the Microsoft environment has a single FE Server	Microsoft FE Server
the Microsoft environment has multiple front end servers (the deployment covered by this document)	Microsoft FE Servers which will be sending traffic towards the Gateway Expressways
the Microsoft environment is fronted by a Hardware Load Balancer in front of Directors (see Appendix 3: Extended Microsoft Deployments, page 70)	Hardware Load Balancer and the Directors
the Microsoft environment is fronted by a Director (see Appendix 3: Extended Microsoft Deployments, page 70)	Director
the Microsoft environment has no Director but a Hardware Load Balancer in front of Front End Servers (see Appendix 3: Extended Microsoft Deployments, page 70)	Hardware Load Balancer and the Microsoft FE Servers

1. Go to **Applications > B2BUA > Microsoft interoperability > Trusted hosts**.

2. Click **New**.

3. Configure the fields as follows:

Name	Name to identify the host (for UI purposes)
IP address	IP address of the device
Type	*Microsoft infrastructure*

4. Click **Save**.

5. Repeat these steps until you've added all the Microsoft hosts that are routing traffic to the Expressway.

Notes:

- Note that trusted host verification only applies to calls initiated by Microsoft clients that are inbound to the Expressway video network. It is not necessary to configure trusted hosts if calls are only ever to be initiated from the Expressway video network.

- The Expressway currently has a nominal limit of 25 trusted hosts. If there are more than 25 trusted hosts, the Expressway raises an alarm.

  In practice, you can have more than 25 trusted hosts if you need them in your deployment. We recommend that you keep the number below 50, and you can safely ignore the alarm. If you need to go beyond 50, we recommend adding another Gateway Expressway.

- If you intend to use the Gateway Expressway to integrate Microsoft SIP SIMPLE with IM and Presence Service, you **do not need to add the IM and Presence Service nodes as trusted hosts** on this page.

Neighbor the Gateway to the Unified CM

1. Go to **Configuration > Zones > Zones**.

2. Click **New**.

3. Configure the fields as follows (leave all other fields with default values):

Name	CUCM Neighbor
Type	*Neighbor*
Hop count	15
H.323 mode	*Off* (H.323 is not supported between Expressway and Unified CM)
SIP mode	*On*
SIP port	5060 for TCP or 5061 for TLS (must match the port set on the SIP trunk)
Transport	*TCP* or *TLS*. Choose *TLS* if you want secure transport and encrypted media
Media encryption mode	*Auto*
SIP authentication trust mode	*Off*
Peer 1 address	IP address of Unified CM, or the FQDN of Unified CM. If you are planning to ultimately use a TLS connection, then typically you will need to specify the FQDN of Unified CM here as this is the name that will be used to authenticate the certificate presented by Unified CM.

Zone profile (Advanced section)	This depends upon your version of Unified CM:
	
	 – Select *Cisco Unified Communications Manager* for versions prior to 8.6.1
	 – Select *Cisco Unified Communications Manager (8.6.1 or later)* for 8.6.1 or 8.6.2
	 – Select *Custom* for 9.x or later and:
	     · Set **Call signaling routed mode** to *Always*
	     · Leave all the other fields as their default values
	
	 Note that Unified CM 8.6.1 or later is required for BFCP (dual video / presentation sharing).

This configures the Expressway to use SIP over TCP to communicate with the Unified CM. To use TLS, complete the configuration as described here for TCP and then see Connecting Expressway to Unified CM Using TLS, page 26.

4. Click **Create zone**.

Configuration

Edit zone

Type	Neighbor
Hop count	★ 15 ⓘ

H.323

Mode	Off ▼ ⓘ

SIP

Mode	On ▼ ⓘ
Port	★ 5060 ⓘ
Transport	TCP ▼ ⓘ
Accept proxied registrations	Deny ▼ ⓘ
Media encryption mode	Auto ▼ ⓘ
ICE support	Off ▼ ⓘ

Authentication

Authentication policy	Do not check credentials ▼ ⓘ
SIP authentication trust mode	Off ▼ ⓘ

Location

Peer 1 address	10.50.157.22 ⓘ
Peer 2 address	ⓘ
Peer 3 address	ⓘ
Peer 4 address	ⓘ
Peer 5 address	ⓘ
Peer 6 address	ⓘ

Advanced

Zone profile	Custom ▼ ⓘ
Monitor peer status	Yes ▼ ⓘ
Call signaling routed mode	Always ▼ ⓘ

Create a Search Rule to Route Calls to the Unified CM Neighbor Zone

Search rules specify the range of telephone numbers / URIs to be handled by this neighbor Unified CM. They can also be used to transform URIs before they are sent to the neighbor.

Configuration

In this example deployment, this search rule routes calls with addresses in the format 3xxx@video.example.com to Unified CM.

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields as follows to route the call to Unified CM:

Rule name	Route to CUCM
Description	For example: Send 3xxx@video.example.com calls to CUCM
Priority	100
Protocol	*Any*
Source	*Any*
Request must be authenticated	Configure this setting according to your authentication policy
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	(3\d{3})@video.example.com
Pattern behavior	*Leave* (@domain formatted addresses will work in Unified CM due to the **Cluster Fully Qualified Domain Name** enterprise parameter)
On successful match	*Stop*
Target zone	*CUCM Neighbor*
State	*Enabled*

4. Click **Create search rule**.

See the "Zones and Neighbors" section of *Expressway Administrator Guide* for further details.

Create a Transform to Strip Port Information from URIs

This transform matches URIs received from Unified CM in the form <uri>:<port> and strips off any port information to convert them into just <uri>.

1. Go to **Configuration > Dial plan > Transforms**.
2. Click **New**.

3. Configure the fields as follows:

Priority	Enter a high priority such as 5 (the priority of this transform should be before any transforms that need to be applied for searching neighbor zones)
Description	Strip off any port information
Pattern type	*Regex*
Pattern string	For example: (.+):.*
Pattern behavior	Replace
Replace string	For example: \1
State	Enabled

4. Click **Create transform**.

Configure Static Routes from Microsoft FE Server to Gateway Expressway

This involves configuring domain static routes that route calls for Cisco Collaboration endpoints to Gateway Expressway.

The routes should reside on the Director (pool) if present, otherwise on the FE Server (pool).

Note: Adding and deleting static routes on a Microsoft FE Server does not automatically apply the route to all the other Microsoft Servers that may need the route. You need to add the route to the global static routing configuration. You then need to enable the changed topology to put the changes into effect.

1. Use `New-CsStaticRoute` to create a static route to the Gateway Expressway. Use the following switches:

   `$routename=New-CsStaticRoute`: name and assign a variable to hold the new route.

   `-TLSRoute`: the route uses TLS (recommended)

   `-TCPRoute`: the route uses TCP (not recommended)

   `-Destination`: the Gateway Expressway Cluster FQDN. Use the IP Address in case of TCP routes.

   `-MatchUri`: the SIP domain in which the Gateway Expressway is authoritative.

   `-Port`: the TLS or TCP port to use for neighboring. It should be the same port as **Port on B2BUA for Microsoft call communications**. The default is `65072`, but you can check the **Advanced** B2BUA settings on the Gateway Expressway, at **Applications > B2BUA > Microsoft interoperability > Configuration**.

`-UseDefaultCertificate`: to use the default certificate assigned to the Front End (must be `$true`) when using TLS. Do not use this switch when creating a TCP route.

TLS route example:

```
C:\Users\administrator.example> $Route1=New-CsStaticRoute -TLSRoute -Destination
"lyncexp.video.example.com" -MatchUri "video.example.com" -Port 65072 -UseDefaultCertificate $true
```

TCP route example:

```
C:\Users\administrator.example> $Route1=New-CsStaticRoute -TCPRoute -Destination "10.0.0.2" -MatchUri
"video.example.com" -Port 65072
```

2. Use `Set-CsStaticRoutingConfiguration` to assign the route to the FE Server environment routing configuration:

   `-Identity`: specifies the scope of the routing configuration for the new route. It can be at `global` or supply the identity of a specific pool. If a pool does not have a more specific static route, it will choose the global route.

   `-Route @{Add=$routename}`: the name of the route you're assigning to the Identity (note the curly braces).

   For example:

   ```
   C:\Users\administrator.example> Set-CsStaticRoutingConfiguration -Identity global -Route @
   {Add=$Route1}
   ```

3. Verify the static route assignment using

   ```
   Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty Route
   ```

4. Use `Enable-CsTopology` to put the changed routing configuration into effect for the specified scope.

Note that:

- When FE Server tries to route a call it will first check all its registrations:
  - If any registration is found that matches the called URI, the call will be sent to that device, or if multiple registrations exist, the call will be forked to all registered devices that match the URI.
  - If there is no registration, FE Server will then check the static domain routes and if there is one for this domain then the server routes the call to the specified destination.
- If static routes are set up, Expressway will receive any requests to that domain that Microsoft cannot handle, and thus may receive significant volumes of mis-dial traffic.

Test Calls from Internal Microsoft Client to Internal Endpoint

Test calls from Microsoft clients registered on Microsoft infrastructure to endpoints registered on Expressway-C. For example, call `david.jones.office@video.example.com` from a Microsoft client.

Enable Calls from External Microsoft Clients

Table 13   Configure TURN in the Cisco Collaboration network

Command or Action	Purpose
Activate the TURN Server on the Expressway-E, page 45	Enable the Expressway-E to relay the media between external Microsoft clients and internal endpoints
Configure the Microsoft Interoperability Service to Offer TURN Services to External Microsoft Clients, page 46	To tell Microsoft clients the addresses of the TURN servers when they are establishing connectivity (ICE)

Activate the TURN Server on the Expressway-E

Prerequisites

- Expressway-E is configured as required in *Cisco Expressway Basic Configuration Deployment Guide* on Cisco Expressway Series Configuration Guides page.
- Expressway-E cluster has TURN Relay licenses.

Create a Client Account and Enable TURN Services

1. Sign in to the Expressway-E and go to **Configuration > Traversal > TURN**.
2. Set **TURN services** to *On*.
3. Click **Configure TURN client credentials on local database**.

   A window pops up showing the local authentication accounts.
4. Click **New**.
5. Enter a **Name** that you can recognize as the system that uses this TURN server.

   For example, enter `GatewayB2BUA` or `CMSServer`.
6. Enter a **Password** to authenticate the client system.
7. Click **Create Credential**.
8. Close the pop up window.
9. Leave the default values in place for all other configuration fields.
10. Click **Save**.

    The **TURN server status** section now shows the listening address, the number of active clients, and the number of active relays.

Note: If you need to change any of the defaults on this page in future, restart the TURN server, with your changes, as follows:

1. Make your changes and set **TURN services** to *Off*.
2. Click **Save** and then set **TURN services** to *On*.
3. Click **Save**.

Configure the Microsoft Interoperability Service to Offer TURN Services to External Microsoft Clients

Prerequisites

- The Gateway Expressway has the **Microsoft Interoperability** option key
- There is a TURN server in the DMZ. This topic presumes that you will use the Expressway-E TURN server.

Configure TURN Services on the Gateway Expressway

To enable call connectivity with Microsoft clients calling via an Edge server, you must configure the Gateway Expressway to offer TURN services and tell it the address of the TURN server.

1. Go to **Applications > B2BUA > B2BUA TURN servers**.
2. Click **New**.
3. Configure the fields as follows:

TURN server address	IP address of a Expressway-E which has TURN enabled. (Just a single Expressway; it may be just one peer from a cluster.)
TURN server port	3478 The default TURN listening port on the Expressway-E. On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.
Description	An optional description of this TURN server.
TURN services username and TURN services password	The username and password that the Gateway Expressway uses to authenticate against the TURN server. For example, `GatewayB2BUA`

4. Click **Add address**.
5. Repeat the above steps if additional TURN servers are required.
6. Go to **Applications > B2BUA > Microsoft interoperability > Configuration**.
7. Set **Offer Turn services** to *Yes*.
8. Click **Save**.

Enable Screen Sharing from Microsoft

Prerequisites

- Microsoft clients can make video calls to the Unified CM-registered endpoints
- The **Microsoft Interoperability** key is installed on the Gateway Expressway
- Read Port Reference, page 53 and Screen Sharing, page 12

Enable RDP Transcoding on the Gateway Expressway

1. Go to **Applications > B2BUA > Microsoft interoperability > Configuration**
2. Find **Enable RDP transcoding for this B2BUA** and select *Yes*
3. Adjust the following Advanced settings, if necessary for your environment:

Table 14   Advanced RDP Transcoding Settings

Setting name	Default and description
RDP TCP port range start – end	6000-6099 for incoming TCP presentation streams from Microsoft clients
RDP UDP port range start – end	6100-6199 for outgoing UDP presentation streams towards BFCP-capable endpoints
Maximum RDP transcode sessions	10 Simultaneous transcoding sessions

4. Save the configuration

Test Screen Sharing

1. Open a Microsoft client and make a video call to a Unified CM-registered endpoint.
2. Start sharing the Microsoft user's screen with the endpoint.
3. Verify that the endpoint is showing the shared screen.
4. Repeat the test for for application sharing.

Enable Chat / Presence from Microsoft Clients

This procedure assumes that you have configured calling between Microsoft clients and Cisco Collaboration endpoints—as per this document—using a static route from the Microsoft FE Servers to the Gateway Expressway.

If you are starting from a different scenario, read Appendix 2: Chat / Presence Between Jabber and Microsoft Clients, page 62.

Configure the SIP Broker

1. Log on to the Gateway Expressway. If it is a cluster, log on to the primary peer.
2. Go to **Applications > B2BUA > Microsoft interoperability > Configuration**.
3. Change **Enable broker for inbound SIP** to *Yes*.

4. Enter the IP addresses, hostnames, or FQDNs of the destination IM and Presence Service nodes.

   If you use hostnames, the Expressway will append the domain from **System > DNS > Domain name**.

5. Change the port number if the IM and Presence Service nodes are listening on a different port.

   Note: There is no transport protocol selection in this configuration. The Expressway sends the traffic out on the same transport protocol that carried the inbound traffic from the Microsoft server (TLS by default). **Changing the port number will not change the transport**.

   For example, entering 5060 will not force the Expressway to interwork inbound TLS to outbound TCP towards IM and Presence Service. The IM and Presence Service does not allow TCP chat federation anyway.

6. Save the configuration.

Configure IM and Presence Service to Trust the Gateway and Microsoft FE Server

You must configure each IM and Presence Service cluster to trust the Gateway Expressway peers and Microsoft FE Servers that are interacting with IM and Presence Service.

You need to repeat the following tasks on all publisher nodes used in this deployment.

Create a Static Route From IM&P To Microsoft FE Server

Use the *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager Configuration Guide*, for your version of IM and Presence Service, to configure a static route to the Microsoft FE server. Here is the document relating to version 11 of IM&P.

You need the static route towards the Microsoft Server because the outgoing messaging from IM&P goes directly to the Microsoft server.

The difference between this document and the guide cited above is that the incoming messaging / presence does not come directly from the Microsoft Server: it comes from the Gateway Expressway, so you don't need the reverse static route from Microsoft Servers to IM&P nodes.

Update IM&P's TLS Peer Subject List

Add the common names (CN) of other servers to the TLS Peer Subject list as follows:

1. Log on to the publisher node.
2. Go to **System > Security > TLS Peer Subjects**.
3. Add a new TLS Peer Subject.

   The **Peer Subject Name** must match the CN of the peer's server certificate.
4. Repeat for other Gateway Expressway peers that will be connecting to this IM and Presence Service cluster.
5. Repeat for Microsoft servers that will be connecting to this IM and Presence Service cluster.

Configure the TLS Peer Context

Update the publisher node's TLS context as follows:

1. In Cisco Unified CM IM and Presence Administration, go to **System > Security > TLS Context Configuration**.
2. Click **Find**.
3. Choose *Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context*.
4. From the list of available TLS peer subjects, choose the TLS peer subjects that you configured for the Expressways and Microsoft FE servers.
5. Move the chosen entries over to the **Selected TLS Peer Subjects**.
6. [For IM and Presence Service 11.x] In the **TLS Cipher Mapping** pane, remove the ECDHE_ECDSA ciphers from

Configuration

the Selected TLS Ciphers list.

7. Click **Save**.

Update IM&P's Incoming ACL

On each IM and Presence Service cluster's publisher node, you must update the incoming ACL with the IP address and FQDN of all Gateway Expressway peers and all FE Servers.

1. On the publisher node, go to **System > Security > Incoming ACL**.
2. Add a new entry for the IP address of each Gateway peer.
3. Add a new entry for the FQDN of each Gateway peer.
4. Add a new entry for the IP address of each Microsoft server.
5. Add a new entry for the FQDN of each Microsoft server.
6. Save the ACL configuration.

For the detailed procedure, search for "Configure an Incoming Access Control List" in the document *IM and Presence Service Node Configuration for Partitioned Intradomain Federation*. Here is the detail for version 11 of IM and Presence Service.

Restart the SIP Proxy Service

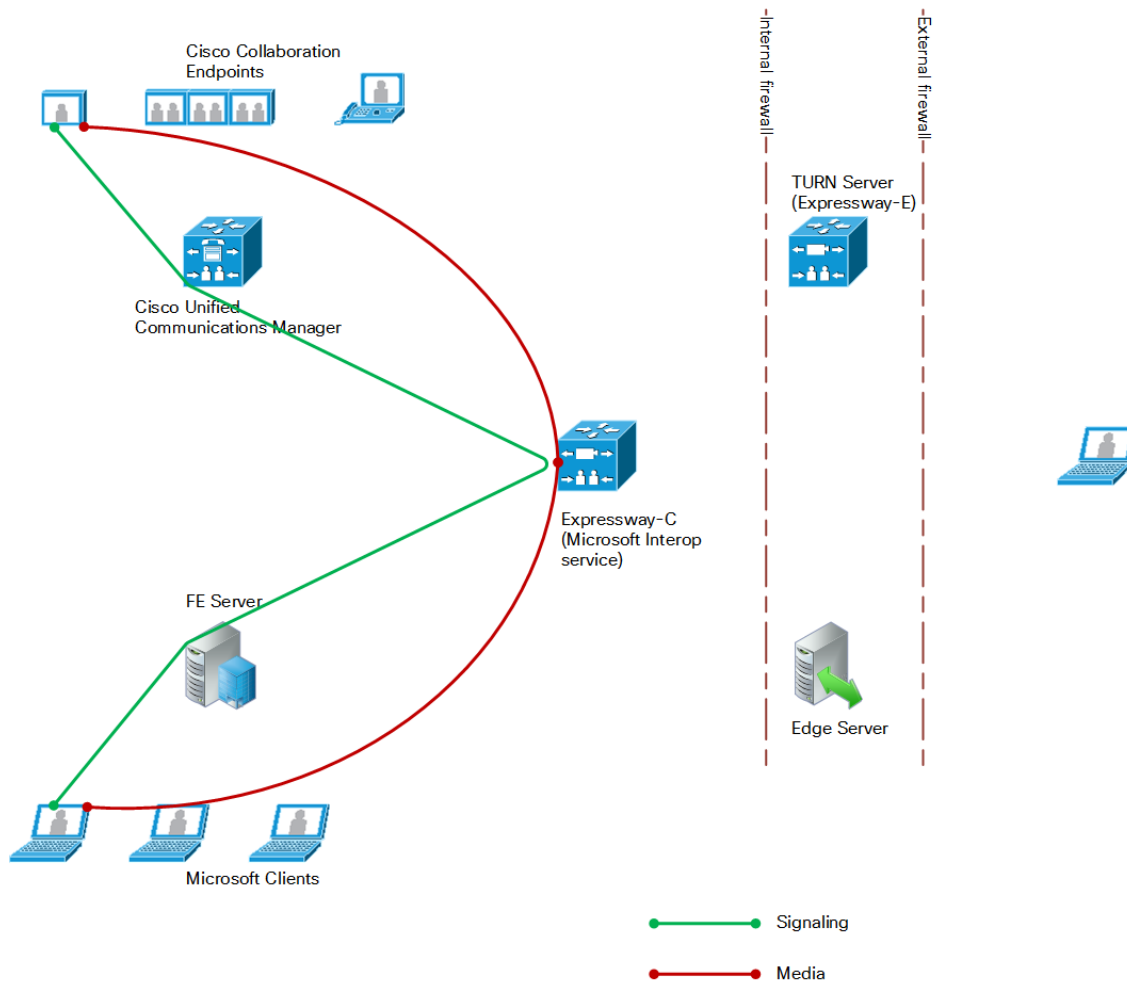On each publisher node, restart the SIP proxy as follows:

1. In Cisco Unified IM and Presence Serviceability, choose **Tools > Service Activation**.
2. Restart the *Cisco SIP Proxy* service.

# Media Paths and License Usage

Microsoft Client Call to SIP Video Endpoint

Figure 4   Call between on-premises Microsoft client and on-premises SIP endpoint

- Licenses consumed by this call:
  - 1 rich media session license on Gateway Expressway
- Signaling flows through FE Server, B2BUA, and Unified CM.
- Media is connected directly between the Microsoft client and the B2BUA.
- Media is connected directly between the internal SIP video endpoint and the B2BUA.
- Calls in both directions use the same signaling and media paths.

Off-premises Microsoft Client Calls On-premises SIP Video Endpoint

Figure 5   Call between off-premises Microsoft client and on-premises SIP endpoint
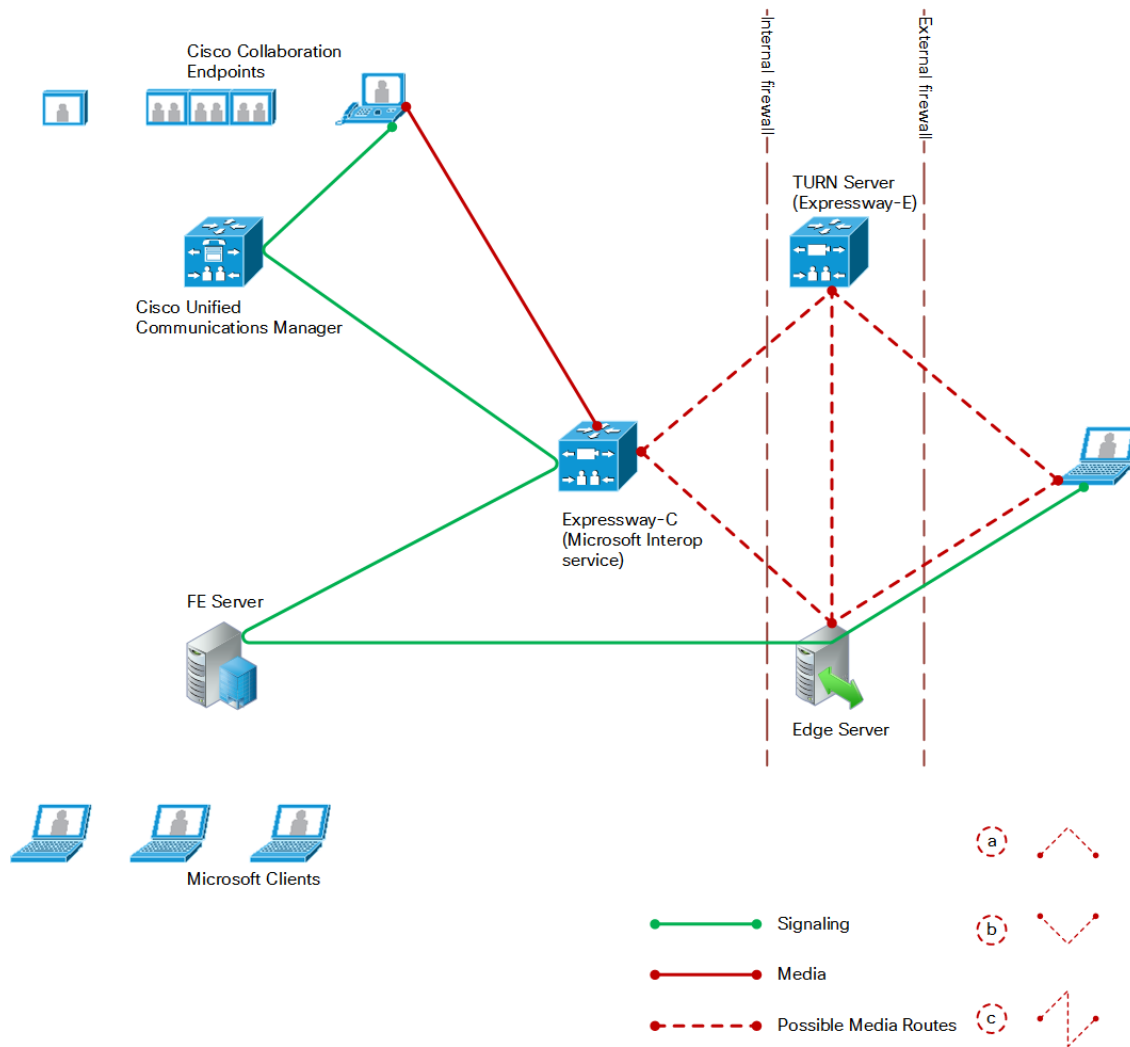
- Licenses consumed by this call:
  - 1 rich media session license on Gateway Expressway
  - A number of TURN licenses on the Expressway-E, which depends on what media streams are relayed
- Signaling flows through the Microsoft Edge Server, Microsoft FE Server, B2BUA, and Unified CM.

- Media between the Microsoft client and the B2BUA can be routed in a number of ways, depending on the ICE (Interactive Connectivity Establishment) negotiation between the Microsoft client and the B2BUA. The options (dotted red lines on the diagram) are:

    a. Microsoft Client – Expressway-E – Gateway Expressway – SIP endpoint
    b. Microsoft Client – Microsoft Edge – Gateway Expressway – SIP endpoint
    c. Microsoft Client – Microsoft Edge – Expressway-E – Gateway Expressway – SIP endpoint

    Note: The exact media path for any particular call is impossible to determine until the call is made. This is because the clients perform the connectivity checks and candidate sorting each time the media path is established, and route selection is based on loosely regulated factors. See RFC 5245 for details.

- Media is connected directly between the internal SIP endpoint and the B2BUA (because the call is SIP to SIP).

- Calls made in the opposite direction, internal video endpoint to external Microsoft client will use the same signaling and media paths.

Port Reference

The port numbers listed below are the default port values. The values used in a real deployment may vary if they have been modified, for example, by changes of registry settings or through group policy, on Microsoft infrastructure or clients, or configuration on Expressway (**Applications > B2BUA**).

Table 15   Between B2BUA and Microsoft Environment

Purpose	Protocol	Expressway port	Microsoft port
Signaling to Microsoft server	TLS	65072	5061 (Server SIP listening port)
Signaling from Microsoft server	TLS	65072	Ephemeral port
Media (The Microsoft interoperability service should run on a separate "Gateway" Expressway and so this range should not conflict with the standard traversal media port range) **Note:** The Expressway does not forward DSCP information that it receives in media streams.	UDP	56000 to 57000 Each call can use up to 18 ports if you **Enable RDP Transcoding for this B2BUA**. Increase this range if you see "Media port pool exhausted" warnings.	Microsoft client media ports
Screen share from Microsoft clients to B2BUA	TCP	56000 to 57000	Microsoft client RDP ports

Table 16   Between B2BUA and Internal Video Network

Purpose	Protocol	Expressway port	Expressway IP port
Internal communications with Expressway application	TLS	65070	SIP TCP outbound port on Expressway
Transcoded screen shares (H.264) from B2BUA to BFCP capable recipients	UDP	56000 to 57000	Recipient of media is dependent on deployment and called alias; eg. endpoint, TelePresence Server, Expressway-C

Table 17   Between B2BUA and Expressway-E Hosting the TURN Server

Purpose	Protocol	B2BUA IP port	Expressway-E IP port
All communications	UDP	56000 to 57000	3478 (media/signaling) *

Ensure that the firewall is opened to allow the data traffic through from B2BUA to Expressway-E.

* On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.

Table 18   External Microsoft Client and Edge Server

Purpose	Protocol	Edge server	Microsoft client
SIP/MTLS used between Microsoft Client and Edge server for signaling (including any ICE messaging to the Edge Server)	TCP	5061	5061
SIP/TLS	TCP	443	443
STUN	UDP	3478	3478
UDP Media	UDP	50000–59999	1024–65535
TCP Media	TCP	50000–59999	1024–65535

Table 19   External Microsoft Client / Edge Server and Expressway-E

Purpose	Protocol	Microsoft client / Edge server	Expressway-E
ICE messaging (STUN/TURN) (Expressway-E must listen on TCP 3478 for screen sharing relay requests from Microsoft clients, and on UDP 3478 for A/V media relay requests)	UDP & TCP	3478	3478
UDP media	UDP	1024–65535	24000–29999

Table 20   Between B2BUA and External Transcoder

Purpose	Protocol	B2BUA IP port	Transcoder
B2BUA communications with transcoder (Cisco AM GW)	TLS	65080	5061

How Many Media Ports are Required on the Gateway Expressway?

The UDP port range of the B2BUA on the Gateway Expressway is set to 1000 ports by default, starting at 56000 and ending at 57000. That is the default destination range for media from Microsoft clients, and may be different in your Microsoft environment.

The B2BUA uses the UDP ports as follows:

Purpose	Call type	Number of ports used
Traversal of audio and video streams	Internal/external Microsoft client to SIP endpoint	8
RDP transcoding	Screen share from Microsoft client	10
Maximum per call	Microsoft client sharing desktop	**18**
Connections from B2BUA to TURN server	Per TURN server connection	2

The number of ports used is one of the reasons why the default maximum number of RDP transcode sessions is set to 20, and why the hard limit for maximum Microsoft Interoperability calls is 100.

For example, if the B2BUA is handling 100 internal Microsoft AV calls, and 20 of those calls are doing RDP:

(80*8) + (20*18) + (0*2)= 1000 ports are required, and no further sharing sessions can be accommodated by the default port range.

(In this example, there are no connections to TURN servers)

If you increase the maximum number of RDP transcode sessions, you should also increase the B2BUA media port range.

Appendix 1: Troubleshooting

Checklist

If you are experiencing a problem with the Microsoft integration, we recommend that you go through the following list when performing the initial faultfinding. It will help to uncover any potential problems with the base configuration and status of the deployment:

- Check the Event Log (**Status > Logs > Event Log**) on Expressway
- Enable logging on FE Server
- Enable debug on Microsoft Client
- Ensure that video endpoints and infrastructure devices are running up-to-date software. Doing so lowers the chances for interoperability issues between the video environment and Microsoft.
- Ensure that all Gateway Expressways can successfully look up all Microsoft Server A-record FQDNs in DNS (this includes both Director and FE Servers). You can use **Maintenance > Tools > Network utilities > DNS lookup** on the Expressway.
- Ensure that all Microsoft servers can successfully look up all Gateway Expressway peer A-record FQDNs and cluster FQDN in DNS. You can use the nslookup command-line utility locally on each Microsoft Server.
- Verify that the B2BUA has connectivity both with the Microsoft environment and the Expressway (on the **Status > Applications > Microsoft interoperability** page, Status = Alive is the desired state for both).

Tracing Calls

Tracing calls at SIP / H.323 level

1. Go to **Maintenance > Diagnostics > Diagnostic logging**.
2. Optionally, select **Take tcpdump while logging**.
3. Click **Start new log**.
4. (Optional) Enter some **Marker** text and click **Add marker**.
   - The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
   - You can add as many markers as required, at any time while the diagnostic logging is in progress.
   - Marker text is added to the log with a "`DEBUG_MARKER`" tag.
5. Reproduce the system issue you want to trace in the diagnostic log.
6. Click **Stop logging**.
7. Click **Collect log**.
8. When the log collection completes, click **Download log** to save the diagnostic log archive to your local file system.

   You are prompted to save the archive (the exact wording depends on your browser).

To download logs again

If you want to download the logs again, you can re-collect them by using the **Collect log** button. If the button is grayed out, first refresh the page in your browser.

Microsoft Problems

Run the Lync Server 'Best Practices Analyzer' to help identify configurations that may be incorrect on Lync Server.

Details and the download for Lync Server 2010 can be found at http://www.microsoft.com/en-us/download/details.aspx?id=4750 and Lync Server 2013 content is at http://www.microsoft.com/en-us/download/details.aspx?id=35455.

Problems with Certificates

If a non-Lync application is used to create certificates to load onto Expressway for use with Lync (for example when purchased from a certificate authority) it is vital that the Subject name and Subject Alternate Name contain the same details as they would if the certificates were created by Lync.

Specifically, if both Subject name and Subject Alternate Name are used, then the name entered in the Subject name must also appear in the Subject Alternative Name list.

See also *Expressway Certificate Creation and Use Deployment Guide*.

Video Endpoint Reports that it does not Support the Microsoft Client SDP

If a video endpoint reports that it does not support the Microsoft client SDP, for example by responding "400 Unable to decode SDP" to a SIP INVITE message containing the Microsoft multi-part mime SDP sent to it:

1. Check whether the Microsoft Server is sending calls to the Expressway incoming IP port, rather than the B2BUA IP port that should be receiving the incoming SIP messages.
2. Reconfigure Microsoft Server to send calls to the B2BUA IP port.

Microsoft Client Cannot Open a TLS Connection to Expressway

Microsoft Debug says Lync Fails to Open a Connection to Expressway, even though the *To Microsoft destination via B2BUA* zone is active and messaging is sent from Expressway to Microsoft infrastructure.

The local host name and domain name fields must be configured in the Expressway **System > DNS** page so that Expressway can use its hostname (rather than IP address) in communications. The Microsoft infrastructure needs to use the Expressway FQDN to open a TLS connection to the Expressway.

Microsoft Responds to INVITE with " 488 Not acceptable here"

There can be two causes for this message:

From IP address

This is normally seen if the B2BUA forwards an INVITE from a standards-based video endpoint where the 'From' header in the SIP INVITE only contains the IP address of the endpoint, e.g. "From: <sip:10.10.2.1>;tag=d29350afae33". This is usually caused by a misconfigured SIP URI in the endpoint. In future versions of B2BUA, the "From"-header will be manipulated if necessary to avoid this issue.

Encryption mismatch

Look for the reason for the 488. If it mentions encryption levels do not match, ensure that you have configured encryption appropriately, either:

- Gateway Expressway has the **Microsoft Interoperability** option key included, or
- (Lync Server 2010 only) Lync is configured such that encryption is supported (or set as "DoNotSupportEncryption") – note that if the encryption support is changed on Lync then a short time must be left for the change to propagate through Lync Server and then the Lync client must be signed off and then signed back in again to pick up the new configuration.

Call Connects but Drops After About 30 Seconds

If a call drops soon after it connects, it is likely that the caller's ACK response to the 200 OK is not being properly routed. Check that the Expressway and FE servers are able to resolve each other's FQDNs in DNS.

Expressway to Microsoft client calls fail – DNS server

Expressway needs to have details about DNS names of Microsoft FE pools and servers, and therefore needs to have one of its DNS entries set to point to a DNS server which can resolve the FQDNs of the FE pools and servers.

Expressway to Microsoft client calls fail – Hardware Load Balancer (HLB)

If the Microsoft environment has FE Servers with a hardware load balancer in front, ensure that the Expressway is neighbored with the HLB. If it is neighbored directly with a FE Server, trust for Expressway will be with the FE Server.

Expressway will send call requests to the FE Server, which record-routes the message such that the ACK response should be sent to the HLB. The ACK sent to the HLB gets rejected by Lync Server, so Lync clears the call after the SIP timeout because the FE Server did not see the ACK.

(Calls from Microsoft client – registered to the FE Server- to Expressway may still work.)

Media Problems in Calls Involving External Microsoft clients Connecting via an Edge Server

RTP over TCP/UDP

The Edge server supports RTP media over both TCP and UDP, whereas the B2BUA and standards based video endpoints only support RTP over UDP. The Edge server and any firewalls that the Edge server may pass media traffic through may need to be reconfigured to allow RTP over UDP as well as RTP over TCP to be passed.

ICE negotiation failure

This can usually be detected by the call clearing with a BYE with reason header "failed to get media connectivity".

Video endpoints only support UDP media. ICE usually offers 3 candidates:

- Host (private IP)
- Server Reflexive (outside IP address of firewall local to the media supplying agent – B2BUA or Microsoft Client)
- TURN server (typically the Edge Server/Expressway-E)

For ICE to work where an endpoint is behind a firewall, the endpoint must offer at least one publicly accessible address (the Server Reflexive address or the TURN server address). This is used both for the B2BUA to try and send media to, but also to validate bind requests sent to the Expressway-E's TURN server – bind requests are only accepted by the TURN server if they come from an IP address that is 'known'.

If a Microsoft INVITE offers only host candidates for UDP, for example:

```
a=candidate:1 1 UDP 2136431 192.168.1.7 30580 typ host
a=candidate:1 2 UDP 2135918 192.168.1.7 30581 typ host
a=candidate:2 1 TCP-ACT 1688975 192.168.1.7 30580 typ srflx raddr 192.168.1.7 rport 30580
a=candidate:2 2 TCP-ACT 1688462 192.168.1.7 30580 typ srflx raddr 192.168.1.7 rport 30580
```

…only one UDP candidate (two lines, one for RTP and one for RTCP) and they are for the host (private, presumably non-routable by Expressway address)

and the B2BUA responds, for example:

```
a=candidate:1 1 UDP 2136431 84.233.149.125 56056 typ host
a=candidate:1 2 UDP 2136430 84.233.149.125 56057 typ host
a=candidate:4 1 UDP 1677215 194.100.47.5 60000 typ relay raddr 84.233.149.125 rport 56056
a=candidate:4 2 UDP 1677214 194.100.47.5 60001 typ relay raddr 84.233.149.125 rport 56057
```

…Host and Relay candidates are both offered.

Neither device will be able to reach the other's private (host) address, and if the Microsoft client tries to bind to the Expressway-E TURN server it will get rejected because the request will come from the server reflexive address rather than private address and Microsoft client has not told the B2BUA what that IP address is.

Thus, FE Server and the Microsoft Edge Server must be configured such that a Microsoft client offers at least one public address with UDP media for this scenario to work.

Note that in the above scenario the B2BUA may not offer the Server Reflexive address if the Server Reflexive address is seen to be the same as the host address.

Call between endpoint and Microsoft client fails with reason 'ice processing failed'

If the search history on Expressway shows calls failing with 'ice processing failed', this means that all ICE connectivity checks between the B2BUA and the remote Microsoft client have failed.

Verify that the TURN server on Expressway-E has been enabled and that the TURN user credentials on Expressway-E and B2BUA configuration match properly. This failure could also indicate a network connectivity issue for STUN/TURN packets between B2BUA, Expressway-E/TURN server and the far end TURN server/Microsoft Edge.

One Way Media: Microsoft Client to Expressway-registered Endpoint

When using Microsoft Edge Server

When Microsoft clients register to Microsoft FE Server through a Microsoft Edge Server, the local IP address and port that the Microsoft client declares is usually private and un-routable (assuming that the Microsoft client is behind a firewall and not registered on a public IP address). To identify alternate addresses to route media to, the Microsoft client uses SDP candidate lines.

Calls traveling through the Microsoft Edge server are supported when using the B2BUA with the **Microsoft Interoperability** option key applied to the Gateway Expressway, and where the video architecture includes a Expressway-E with TURN enabled and the B2BUA is configured to use that TURN server.

When using a Hardware Load Balancer in front of FE Servers

Expressway modifies the application part of INVITEs / OKs received from Microsoft clients to make them compatible with traditional SIP SDP messaging. Expressway only does this when it knows that the call is coming from Microsoft. If there are problems with one-way media (media only going from Microsoft client to the Expressway registered endpoint), check the search history and ensure that the call is seen coming from a Microsoft trusted host. Otherwise, the call may be coming from a FE Server rather than the load balancer. See Enable Calls to Microsoft Environment, page 18 and configure trusted hosts containing the FE Servers' addresses.

Microsoft Clients Try to Register with Expressway-E

SIP video endpoints usually use DNS SRV records in the following order to route calls to Expressway:

1. _sips._tcp.<domain>
2. _sip._tcp.<domain>
3. _sip._udp.<domain>

Microsoft clients use:

- _sipinternaltls._tcp.<domain> - for internal TLS connections
- _sipinternal._tcp. <domain> - for internal TCP connections (only if TCP is allowed)
- _sip._tls. <domain> - for external TLS connections

If Microsoft clients are trying to register with Expressway-E, it could be because the wrong SRV record points to it.

You must make sure that the six DNS records above do not resolve to overlapping addresses.

Microsoft clients only support TLS connection to the Microsoft Edge Server, so use the _sip._tcp.<domain> DNS SRV for the Expressway-E.

Call to PSTN (or Other Devices Requiring Caller to be Authorized) Fails With " 404 not found"

In some Microsoft configurations, especially where Microsoft PSTN gateways are used, calls are only allowed if the calling party is authorized. Thus, the calling party's domain must be the Microsoft Server domain. This means that the

endpoints must register to the video network with a domain that is the same as the Microsoft domain.

Microsoft Rejects Expressway Zone OPTIONS Checks with '401 Unauthorized' and INFO Messages with '400 Missing Correct Via Header'

- A response "400 Missing Correct Via Header" is an indication that Lync does not trust the sender of the message.
- A response "401 Unauthorized" response to OPTIONS is another indication that Lync does not trust the sender of the OPTIONS message.

Ensure that Lync environment has been configured to trust the Expressway which is sending these messages, as described previously in this document.

Note, this can also be seen if a load balancer is used in front of the Lync, and Lync is configured to authorize the Expressway (Lync sees calls coming from the hardware load balancer rather than from the Expressway).

B2BUA Problems

Microsoft Interoperability Service Status Reports Microsoft Server "Unknown" or "Unknown failure"

Check that the Expressway application has been added to the Microsoft trusted application pool and is configured to contact the Expressway B2BUA via port 65072 . See Enable Calls to Microsoft Environment, page 18 for more information.

Microsoft Client

Client Stuck in "Connecting…" State

This could be because the client is not receiving media. The client cannot change into the "Connected" state until it receives RTP (media) from the other party.

Login / Logout Cycling

If your Lync client is not staying signed in, it could be because subscribe is failing, from Lync FE Server via Expressway to IM and Presence Service.

Subscribe can fail because of incorrect security configuration on IM and Presence Service. For example, this issue can be triggered when the Expressway does not trust the server certificates from IM and Presence Service nodes.

Presentation Handover Fails in TelePresence Server Conference

Symptom: A participant cannot share their screen when another participant has been sharing.

Note: This issue was seen in a test of an unsupported Expressway and Microsoft scenario, but the solution applies more generally. You could see this symptom whenever endpoints are sharing in a TelePresence Server conference, or if endpoints that are sharing are registered to Cisco Unified Communications Manager. If you are seeing presentation issues, check the solution shown here (even if your conditions are different).

Conditions:

- Gateway Expressway deployed with Lync 2013 Front End Server and Lync 2013 for Windows clients.
- Gateway Expressway configured for screen sharing.
- The Gateway Expressway is trunked to Cisco Unified Communications Manager.
- TC endpoints are registered to Unified CM.

- TC endpoints and Microsoft clients are in a conference on TelePresence Server.
- The conference is registered to the Gateway Expressway (The TelePresence Server is in locally managed mode – no TelePresence Conductor in this scenario).

Possible Root Causes:

- The TelePresence Server is not configured to allow participants to steal the floor.
- The neighbor zone from Expressway to Unified CM does not support BFCP.
- The SIP profile used by the trunk or endpoints does not support BFCP.

Solution:

1. Sign in to the TelePresence Server and check that **Automatic content handover** is enabled (the check box is on **Configuration > System settings** page).
2. Check the box and save the configuration.
3. Log in to the Expressway, go to **Configuration > Zones > Zones**, and open the neighbor zone toward Unified CM.
4. Check the **Zone profile** (in the **Advanced** section of the zone configuration).

   - BFCP is enabled on the neighbor zone if **Zone profile** is *Cisco Unified Communications Manager (8.6.1 or later)*.
   - BFCP is not enabled on the neighbor zone if **Zone profile** is *Cisco Unified Communications Manager*.

5. Change the zone profile if necessary, then save the configuration.
6. Log in to Unified CM Administration, go to **Device > Trunk**, and open the SIP trunk to Expressway.
7. Find the **SIP Profile** field and click **View Details** to see the configuration of the selected profile.
8. Find the **SDP Information** field, which has a check box to **Allow Presentation Sharing using BFCP**.
9. Go to **Device > Phone**, open the affected phone configuration, and check the details of the SIP profile it's using.
10. If a SIP profile does not allow BFCP, go to **Device > Device Settings > SIP Profile** to modify the SIP profile.

Appendix 2: Chat / Presence Between Jabber and Microsoft Clients

This appendix will help you adapt your on-premises integration between Cisco Collaboration and Microsoft infrastructure to enable calling, messaging (chat), and presence between Cisco Jabber and Microsoft soft clients.

Required versions

- Requires IM and Presence Service 10.x or later
- Requires Lync Server 2010 or Lync Server 2013.
- Requires Expressway X8.8 (with **Microsoft Interoperability** option key)

The following existing scenarios are potential starting points for this integration. The appendix explains at a high level how to simplify them into an integrated chat and video solution.

Existing scenarios

- Scenario 1: Gateway Expressway integration with Microsoft infrastructure; calling, but no chat/presence, page 63
- Scenario 2: CUCM IM and Presence Service integration with Microsoft infrastructure; chat/presence, but no calling, page 64
- Scenario 3: Directory VCS and Gateway Expressway integration with Microsoft infrastructure, page 64

   You have configured calling and chat between Lync and Jabber, using the pre-X8.6 CPL-based integration.

   See "Appendix 1: Federation", in the X8.5 version of *Cisco Expressway and Microsoft Lync Deployment Guide*), listed on the Expressway Configuration Guides page.

Target scenario
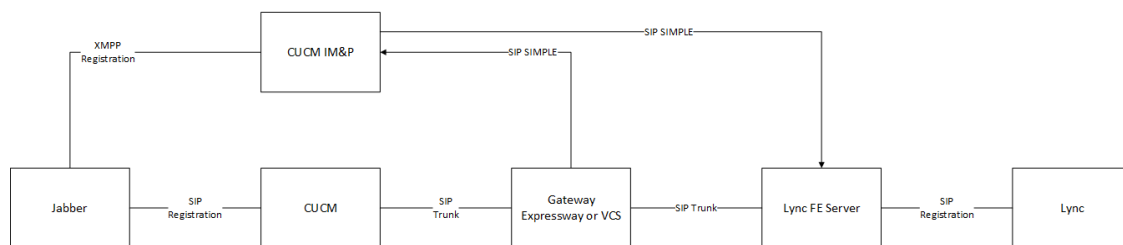
Video calling and chat/presence from Microsoft infrastructure towards Cisco Jabber both go to the Gateway Expressway. The Gateway Expressway sends the messaging and presence towards CUCM IM&P – using the SIP broker instead of CPL – and sends the voice/video calls to the Cisco call control infrastructure.
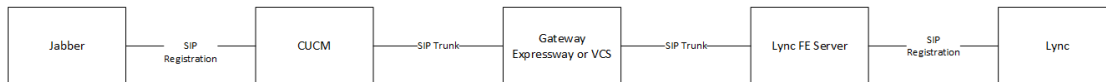
Chat and presence from Jabber go directly from CUCM IM&P to Microsoft infrastructure. Calls from Jabber go through the Gateway Expressway to the Microsoft infrastructure.

Figure 6   Flow Charts Showing Call / Chat Session Establishment in Target Scenario
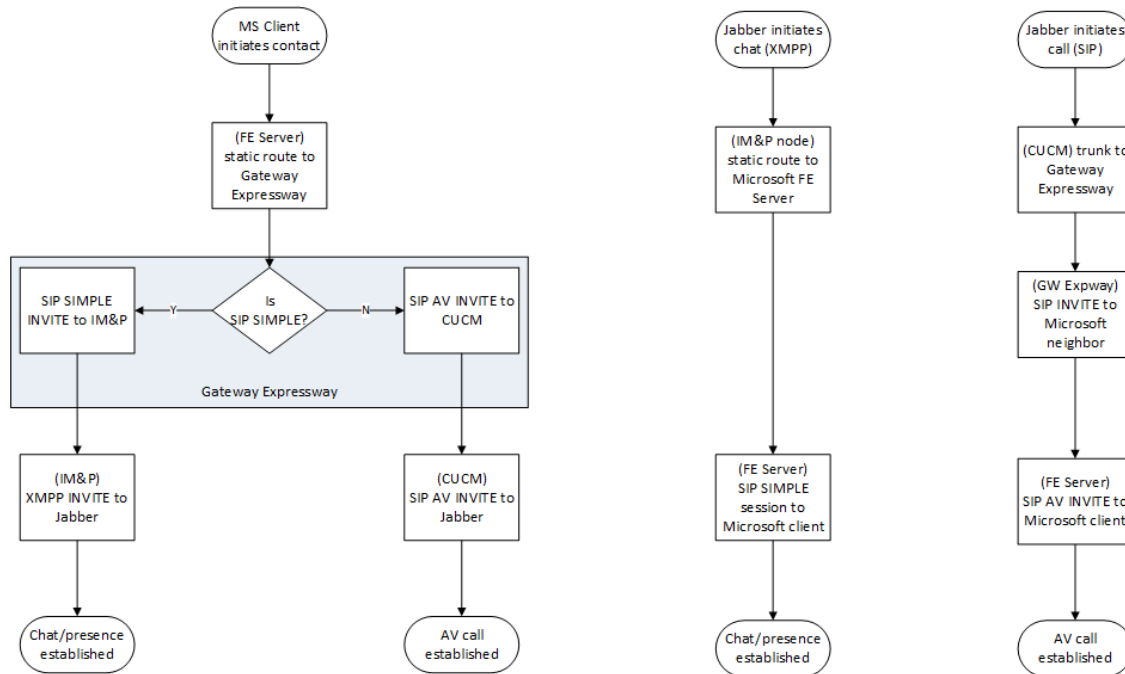
Scenario 1: Gateway Expressway integration with Microsoft infrastructure; calling, but no chat/presence

The voice/video integration is made possible by the "Gateway Expressway" that interoperates between Microsoft video and standard SIP.

The detail of the scenario 1 configuration is in the main body of this document, *Cisco Expressway and Microsoft Infrastructure Deployment Guide*.

Scenario 1 Migration Overview

- Create a SIP direct federation from CUCM IM and Presence Service to Microsoft infrastructure:
  - Enable TLS between IM&P and the Microsoft servers
  - Create cluster-wide static routes from IM&P publisher nodes to the Microsoft servers
  - Create trusted applications (to represent the IM&P nodes) on Microsoft server and put them in trusted application pools
  - **Do not create the reverse static routes**, from MS to IM&P nodes. The intradomain federation guide requires this, but this configuration supersedes that requirement: here, we'll create the static routes from Microsoft servers to the Gateway Expressway instead.
- Enable the SIP broker on the Gateway Expressway, and give it the addresses and port of the listening IM and Presence Service nodes.
- Update the Incoming ACLs (access control lists) and TLS peer context on the IM&P publisher nodes to trust the Gateway Expressways and the Microsoft servers.

Details of the SIP direct federation and the incoming ACL entries are in *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager Configuration Guide*. The different versions of this document are listed at the CUCM Configuration Guides page.

Scenario 2: CUCM IM and Presence Service integration with Microsoft infrastructure; chat/presence, but no calling
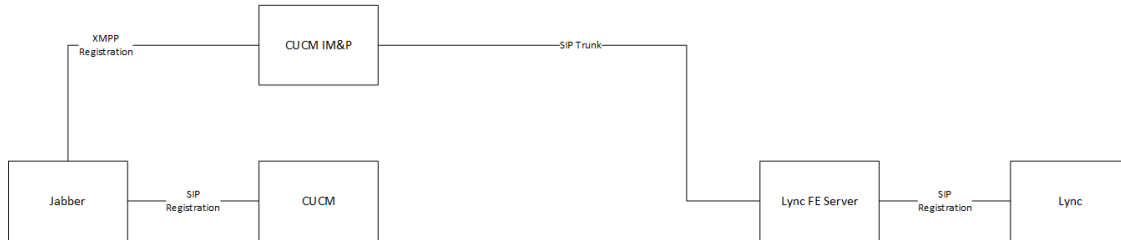
The chat/presence integration is a "SIP direct" federation between CUCM IM and Presence Service and the Microsoft FE servers. You can configure this by following the *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager Configuration Guide*, for your version.

The documents are listed on the CUCM configuration guides page.

Scenario 2 Migration Overview

- Integrate your Cisco collaboration video environment with the Microsoft video environment, using the Gateway Expressway:

    – Enable TLS between the Gateway Expressway and the Microsoft infrastructure.

    – Trunk the CUCM to the Gateway Expressway, neighbor the Gateway Expressway to CUCM.

    – Configure call control on the Gateway Expressway.

    – Add each Microsoft server as a trusted host on the Gateway Expressway.

    – Create a trusted application (to represent the Gateway Expressway peers) on Microsoft server and put them in a trusted application pool (peers as trusted computers).

    – Create static routes from Microsoft server to the Gateway Expressway, remove static routes from Microsoft server to CUCM IM and Presence Service

    Details of the tasks listed above are in the main body of this document (*Cisco Expressway with Microsoft Infrastructure Deployment Guide*).

- Enable the SIP broker on the Gateway Expressway, and give it the addresses and port of the listening IM and Presence Service nodes.

- Update the Incoming ACLs (access control lists) and TLS peer context on the IM&P publisher nodes to trust the Gateway Expressways and the Microsoft servers.

Scenario 3: Directory VCS and Gateway Expressway integration with Microsoft infrastructure
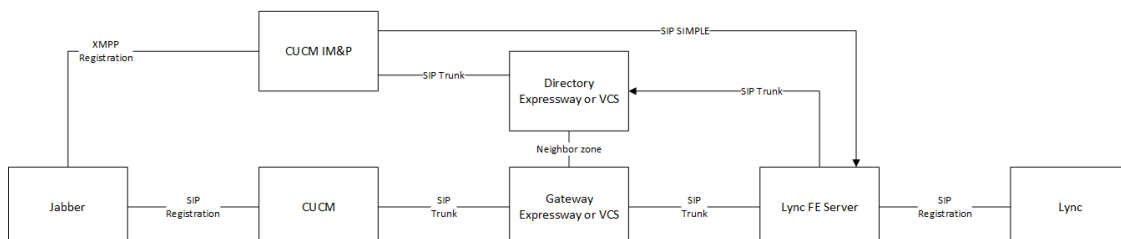
A VCS (or an Expressway) uses CPL to direct SIP SIMPLE SUBSCRIBE and PUBLISH messages towards IM and Presence Service. Other messages are processed by the Gateway Expressway and calls are routed on to the Cisco call control (could be VCS or CUCM).

This deployment scenario stopped working in X8.6 when the Expressway SDP parser was rewritten. You can read about it in *Microsoft Lync and Cisco Expressway Deployment Guide (X8.5)*.

Scenario 3 Migration Overview

- Replace the static route from Microsoft infrastructure to the directory Expressway with a static route to the Gateway Expressway instead.
- Enable the SIP broker on the Gateway Expressway, and give it the addresses and port of the listening IM and Presence Service nodes.
- Update the Incoming ACLs (access control lists) and TLS peer context on the CUCM IM&P nodes to trust the Gateway Expressways and the Microsoft FE Servers.
- Remove the directory Expressway entry from the incoming ACL list and TLS peer context, then decommission the Expressway.

Common Configuration

Before you start: Get the addresses of the IM and Presence Service nodes that you're using for this integration. Check what port they are expecting for messaging and presence. The transport must be TLS.

Configure the SIP Broker

1. Log on to the Gateway Expressway. If it is a cluster, log on to the primary peer.
2. Go to **Applications > B2BUA > Microsoft interoperability > Configuration**.
3. Change **Enable broker for inbound SIP** to *Yes*.
4. Enter the IP addresses, hostnames, or FQDNs of the destination IM and Presence Service nodes.

   If you use hostnames, the Expressway will append the domain from **System > DNS > Domain name**.
5. Change the port number if the IM and Presence Service nodes are listening on a different port.

   Note: There is no transport protocol selection in this configuration. The Expressway sends the traffic out on the same transport protocol that carried the inbound traffic from the Microsoft server (TLS by default). **Changing the port number will not change the transport**.

   For example, entering 5060 will not force the Expressway to interwork inbound TLS to outbound TCP towards IM and Presence Service. The IM and Presence Service does not allow TCP chat federation anyway.
6. Save the configuration.

Create a Static Route From IM&P To Microsoft FE Server

Use the *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager Configuration Guide*, for your version of IM and Presence Service, to configure a static route to the Microsoft FE server. Here is the document relating to version 11 of IM&P.

You need the static route towards the Microsoft Server because the outgoing messaging from IM&P goes directly to the Microsoft server.

The difference between this document and the guide cited above is that the incoming messaging / presence does not come directly from the Microsoft Server: it comes from the Gateway Expressway, so you don't need the reverse static route from Microsoft Servers to IM&P nodes.

Create a Static Route From Microsoft FE Server To Gateway Expressway

The route is needed for calling, and for chat / presence, initiated by the Microsoft soft client. The routing configuration may already have routes from scenarios 2 and 3. You must remove them.

If you're updating from scenario 1, the static route was already configured for calling; this is described in more detail in the body of this document (Configure Static Routes from Microsoft FE Server to Gateway Expressway, page 43).

1. Find existing static routes with this command:

   ```
   Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty Route
   ```

2. Remove existing routes with this command:

   ```
   Remove-CsStaticRoutingConfiguration -Identity <Identity>
   ```

   - If you were in scenario 2, you must remove the route(s) that pointed to the IM&P node(s)
   - If you were in scenario 3, you must remove the route that pointed to the directory Expressway

3. Create the new static route to the Gateway Expressway with this command:

   ```
   $NewRoute=New-CsStaticRoute -TLSRoute -Destination "gatewayexpressway.example.com" -MatchUri
   "example.com" -Port 65072 -UseDefaultCertificate $true
   ```

4. Add the new route to the global routing configuration with this command:

   ```
   Set-CsStaticRoutingConfiguration -Identity global -Route @ {Add=$NewRoute}
   ```

Configure IM and Presence Service to Trust the Gateway and Microsoft FE Server

You must configure each IM and Presence Service cluster to trust the Gateway Expressway peers and Microsoft FE Servers that are interacting with IM and Presence Service.

You need to repeat the following tasks on all publisher nodes used in this deployment.

Update IM&P's TLS Peer Subject List

Add the common names (CN) of other servers to the TLS Peer Subject list as follows:

1. Log on to the publisher node.
2. Go to **System > Security > TLS Peer Subjects**.
3. Add a new TLS Peer Subject.

   The **Peer Subject Name** must match the CN of the peer's server certificate.
4. Repeat for other Gateway Expressway peers that will be connecting to this IM and Presence Service cluster.
5. Repeat for Microsoft servers that will be connecting to this IM and Presence Service cluster.

Configure the TLS Peer Context

Update the publisher node's TLS context as follows:

1. In Cisco Unified CM IM and Presence Administration, go to **System > Security > TLS Context Configuration**.
2. Click **Find**.
3. Choose *Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context*.
4. From the list of available TLS peer subjects, choose the TLS peer subjects that you configured for the Expressways and Microsoft FE servers.
5. Move the chosen entries over to the **Selected TLS Peer Subjects**.
6. [For IM and Presence Service 11.x] In the **TLS Cipher Mapping** pane, remove the ECDHE_ECDSA ciphers from the Selected TLS Ciphers list.
7. Click **Save**.

Update IM&P's Incoming ACL

On each IM and Presence Service cluster's publisher node, you must update the incoming ACL with the IP address and FQDN of all Gateway Expressway peers and all FE Servers.

1. On the publisher node, go to **System > Security > Incoming ACL**.
2. Add a new entry for the IP address of each Gateway peer.
3. Add a new entry for the FQDN of each Gateway peer.
4. Add a new entry for the IP address of each Microsoft server.
5. Add a new entry for the FQDN of each Microsoft server.
6. Save the ACL configuration.

For the detailed procedure, search for "Configure an Incoming Access Control List" in the document *IM and Presence Service Node Configuration for Partitioned Intradomain Federation*. Here is the detail for version 11 of IM and Presence Service.

Restart the SIP Proxy Service

On each publisher node, restart the SIP proxy as follows:

1. In Cisco Unified IM and Presence Serviceability, choose **Tools > Service Activation**.
2. Restart the *Cisco SIP Proxy* service.

Troubleshoot Chat Between Jabber and Microsoft Clients

Diagnostic Information

Wireshark and rejected certificates

The Microsoft FE Server logs can be ambiguous when TLS connections are failing. You can use Wireshark to see exactly which server is rejecting the certificate.

Trust configuration

Connections could also be failing because the servers do not trust each other. You need to configure incoming ACL entries on IM&P, trusted hosts on Expressway, and trusted applications on Microsoft FE Servers.

Asymmetric deployment

If you get chat/presence partially working, it could be because of the asymmetry in the deployment.

Also, if you get presence working but not chat, this could be because chat is a three-way handshake across the asymmetrical link: subscribe > 200 OK > ACK but the ACK fails as it is trying to go direct from Microsoft FE to IM&P. That link is the one that is not trusted.

Appendix 2: Chat / Presence Between Jabber and Microsoft Clients
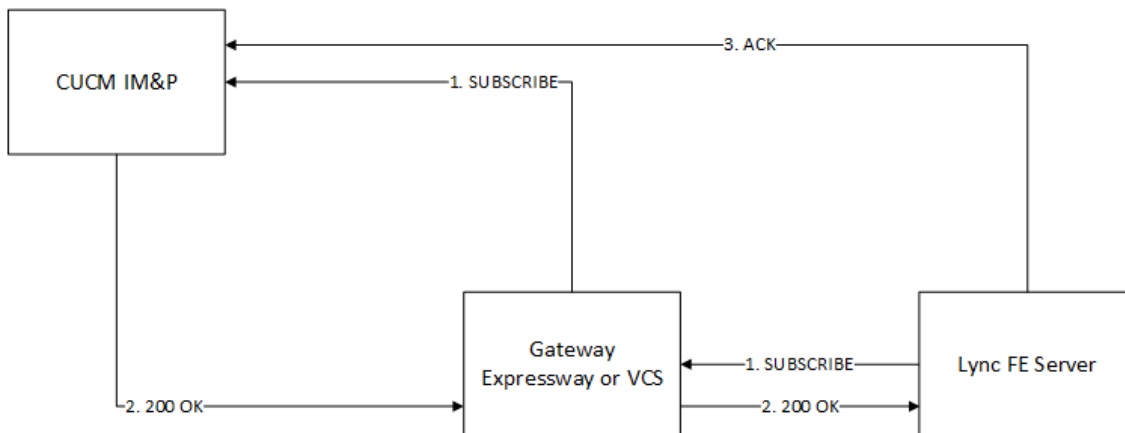
Known Symptoms, Causes, and Fixes

TLS connections are failing

Possible Causes: Each server's certificate must be able to authenticate that server as a web client or as a web server.

Fix: The Microsoft FE, Expressway, and IM&P servers must have certificates that have entries for TLS Web Server Authentication and TLS Web Client Authentication in the Extended Key Usage section.

IM&P is not allowing connections from Expressway or Microsoft server

Possible Cause 1: The IM&P Access Control Lists (ACLs) are not configured properly.

Fix: Check the IM&P ACLs.

In Cisco Unified CM IM and Presence Administration, go to System > Security > Incoming ACL. This list needs to have entries for all Expressways and all Microsoft FE Servers.

Go to System > Security > Outgoing ACL. This list needs to have entries for all the Microsoft FE servers.

Possible Cause 2: The Expressway and Microsoft FE are not TLS peers on IM&P.

Fix: From Cisco Unified CM IM and Presence Administration, go to System > Security > TLS Peer Subjects and add entries for all the Expressway and MS FE servers. Go to System > Security > TLS Context Configuration and click the links for "Peer Auth." Make sure that all Expressway and MS peers are selected, and that all the ciphers are selected.

Calls or chats are not working.

Possible Cause: The IM&P peer auth listener is on the wrong port.

Fix: Go to System > Application Listeners and check that SIP peer auth is listening on port 5061. If SIP server auth is on 5061, you need to change them around as documented in the IM&P documentation.

Jabber presence, as seen by Microsoft client, does not update when the Jabber user is on a call

Possible Cause: A misconfiguration has occurred between IM&P and CUCM.

Fix: On IM&P, go to Presence > Routing > Settings and switch Method/Event Routing Status to On.

You need to restart the proxy service for this to take effect.

Jabber-to-Jabber chat and presence are not working (nothing to do with Expressway)

Possible Cause: Some proxy services need a restart.

Fix: If you tried restarting the proxy services you received notifications about, but it did not fix the issue, ¬ restart the whole of IM&P. This force restarts all the services.

Initializing chat works one way, but not the other.

Possible Cause: Someone does not trust someone else.

Fix: Check the certificates and the ACL lists.

Appendix 3: Extended Microsoft Deployments

Clustered Gateway

When this document refers to a Gateway Expressway, a cluster of Expressways can also be used. The operation is functionally the same, but there is more capacity available.

Calls from Microsoft FE will typically arrive at a single Expressway in the cluster because the Microsoft infrastructure uses a static route; the route resolves to a single FQDN for TLS connectivity, or to a single IP address for TCP connectivity.

If you use a DNS A record to to map the peers' addresses to the FQDN of the cluster, the DNS server typically returns the addresses in a different order each time the FE Server queries DNS (round-robin). The FE server chooses one of the returned addresses, based on its own logic (outside of this document's scope).

Microsoft Environments

Microsoft environments have a number of building blocks, and so they may be constructed in many ways. A full scale Microsoft deployment is likely to use Director, Hardware Load Balancers (HLBs), Front End Servers in enterprise pools, and a redundant AD server.
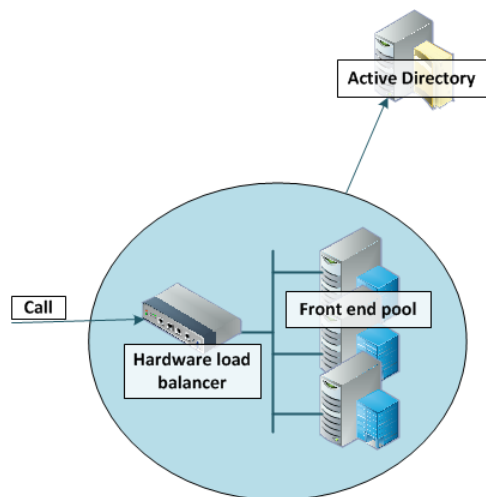
Microsoft recommend that DNS may be used in place of hardware load balancing for routing SIP traffic. Microsoft guidance can be found at http://technet.microsoft.com/en-us/library/gg398634.aspx.

An example architecture is shown below:
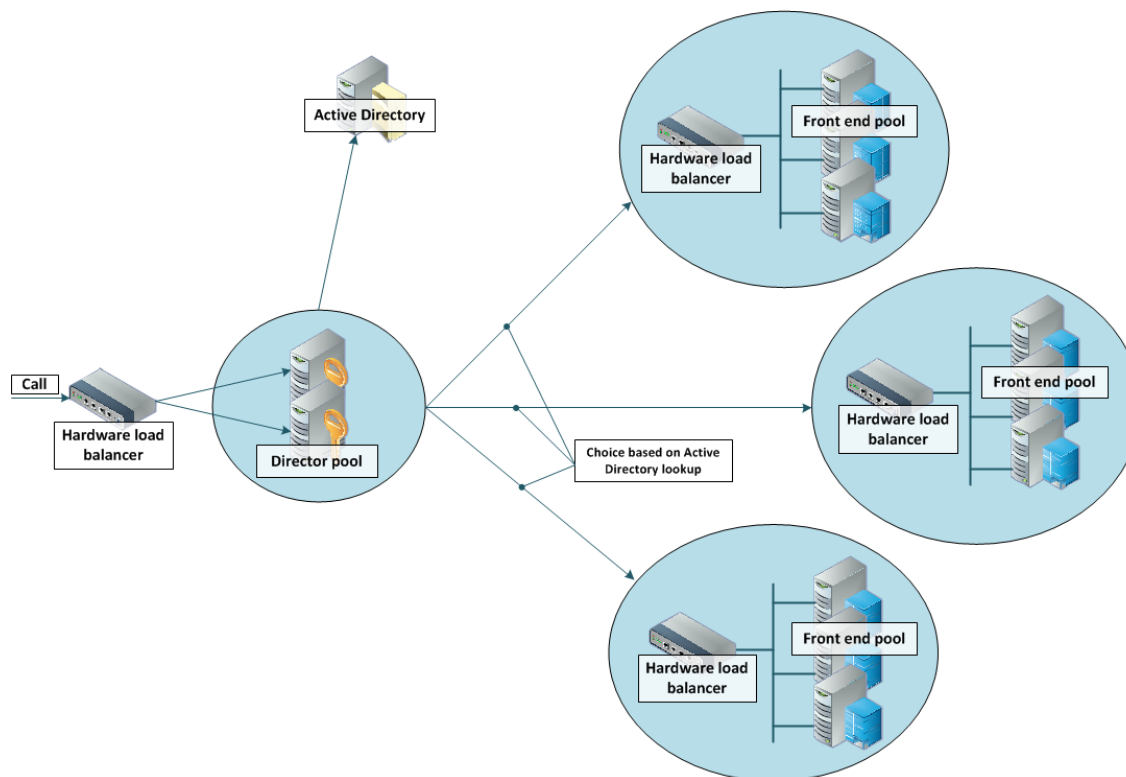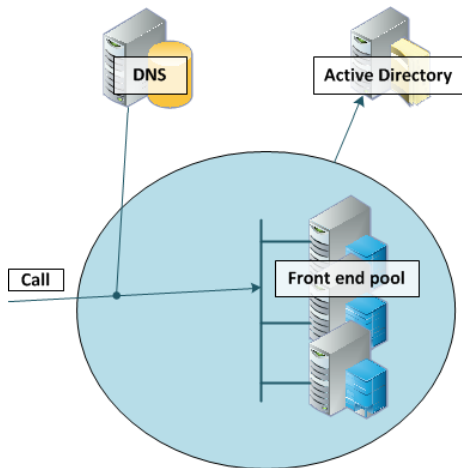

A smaller deployment may not use Director servers, but may just use a Hardware Load Balancer in front of a set of Front End Servers.

A Microsoft environment may use DNS instead of the Hardware Load Balancer, for example:

Note that Microsoft requires that the AD server and the FE Server are on separate machines.

Microsoft deployments may also contain Edge servers to allow Microsoft clients to register from outside the local network through the Edge server to the Front End Server. Communicating with Microsoft devices outside the edge server requires both the Edge Server and the Expressway-E connecting to the public Internet. (Calls involving a Microsoft Edge server require the Expressway to have the **Microsoft Interoperability** option key installed, as this key allows for ICE to be used for media connectivity, which is required in the following scenario.)
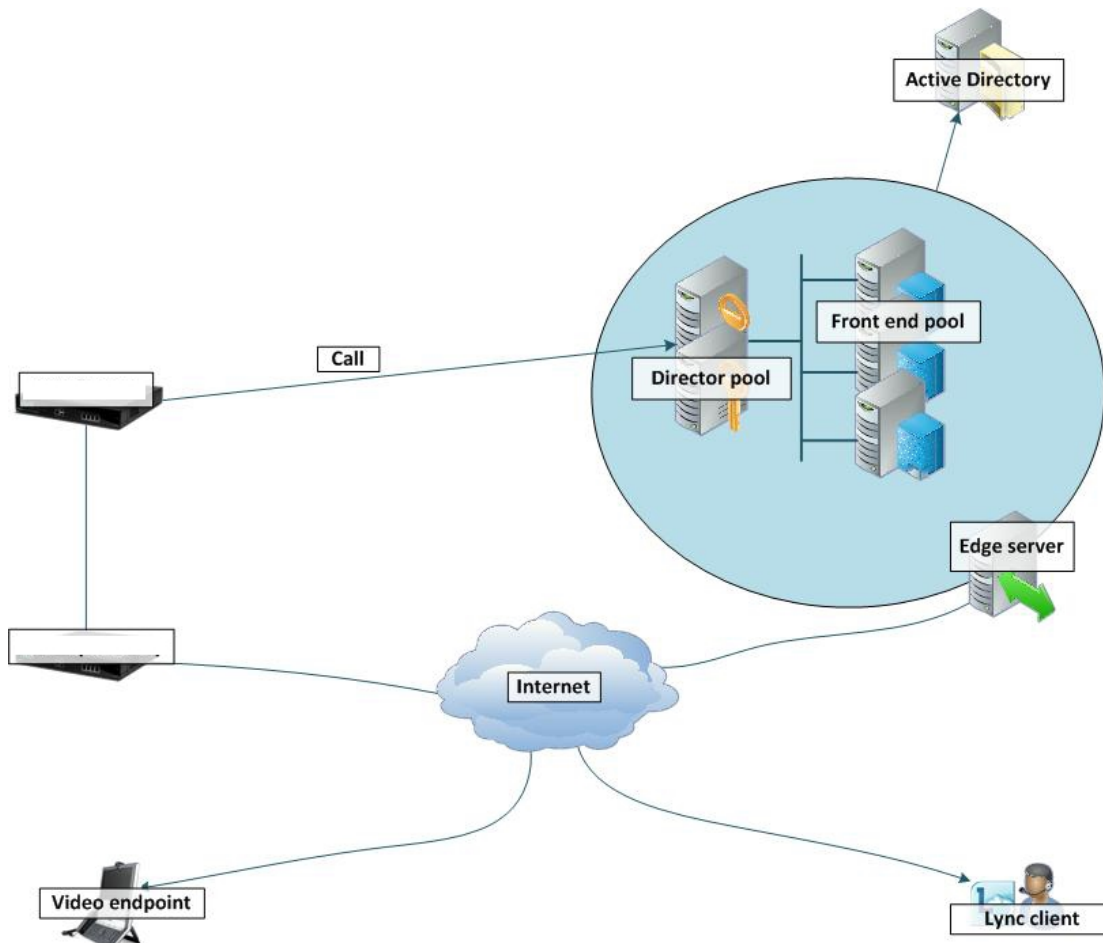
In any deployment with Expressway and Microsoft infrastructure:

- Traffic is sent via a static SIP route form the Microsoft infrastructure to the Expressway. The flow is either directly from a Front End Server, or from the FE Server via a Director, to the Expressway.
- If the Microsoft environment is fronted by a Hardware Load Balancer in front of Directors then calls to and from the video network will go via the Directors; they will not be routed directly to or from the FE Servers:
  - Directors should trust the Gateway Expressway(s).
  - Directors should route the video network domain (video.example.com) to the Gateway Expressway cluster FQDN.
  - Depending on Microsoft environment, FE Servers may route SIP traffic directly to the Expressway, or they may route the traffic through a Director pool.
- If the Microsoft environment is fronted by a single Director then calls to and from the video network will go via that Director; they will not be routed directly to or from the FE Servers:
  - Directors should trust the Gateway Expressway(s).
  - Directors should route the video network domain (video.example.com) to the Gateway Expressway cluster FQDN.
  - Depending on Microsoft environment, FE Servers may route SIP traffic directly to the Expressway, or they may route the traffic through a Director pool.
- If the Microsoft environment has no Director but a Hardware Load Balancer in front of Front End Server pool(s) then configure the pool(s) (not each FE Server):
  - The FE Server pools should trust the Gateway Expressway(s).
  - All FE Server pools should route the video network domain (video.example.com) to the Gateway Expressway cluster FQDN.

  Configuring the pool ensures that the same configuration is applied to every FE Server in the pool.
- If the Microsoft environment is a single Front End Server, then configure that server:
  - The FE Server should trust the Gateway Expressway(s).
  - It should route the video network domain (video.example.com) to the Gateway Expressway cluster FQDN.

We recommend that you use a Expressway cluster FQDN (e.g. lyncexp.example.com) rather than an individual Expressway peer (even if it is a "cluster of one"). If you configure a Trusted Application Pool (Cluster FQDN), you can always add peer FQDNs (Expressway peers) to the Application pool later without requiring to remove the existing search rules, static routes or Trusted Applications in the Microsoft Server.

Gateway Expressway should be configured such that:

- If the Microsoft environment is fronted by a Hardware Load Balancer in front of Directors, then the B2BUA should be configured to route calls for Microsoft users to the Hardware Load Balancer, and receive calls from either of the Directors:
  - The Gateway B2BUA needs to specify the Hardware Load Balancer as the Microsoft signaling destination address.
  - The Gateway B2BUA needs to include the addresses of both Directors as trusted hosts (and any FE Servers which might send traffic directly to the B2BUA).
  - Search rules that route calls to Microsoft users will target the B2BUA neighbor zone.
- If the Microsoft environment is fronted by a Director or a pool of directors, then the B2BUA should be configured to route calls for Microsoft users to the Director, and receive calls from the Director:
  - The Gateway B2BUA needs to specify the Director (pool) as the Microsoft signaling destination address.
  - The Gateway B2BUA needs to include the address of each individual Director as a trusted host (and any FE Servers which might send traffic directly to the B2BUA).
  - Search rules that route calls to Microsoft users will target the B2BUA neighbor zone.

■ If the Microsoft environment has no Director but a Hardware Load Balancer in front of Front End Servers, then the B2BUA should be configured to route calls for Microsoft users to the Hardware Load Balancer, and receive calls from any of the FE Servers:

– The Gateway B2BUA needs to specify the Hardware Load Balancer as the Microsoft signaling destination address.

– The Gateway B2BUA needs to include the addresses all of the Microsoft FE Servers as trusted hosts.

– Search rules that route calls to Microsoft will target the B2BUA neighbor zone.

■ If the Microsoft environment is a single FE Server, then the B2BUA should be configured to route calls for Microsoft users directly to that FE Server, and to receive calls from that FE Server:

– The Gateway B2BUA needs to specify the FE Server as the Microsoft signaling destination address.

– The Gateway B2BUA needs to include the address of the FE Server as a trusted host.

– Search rules that route calls to Microsoft will target the B2BUA neighbor zone.

## Multiple Microsoft Domains and Multiple Gateway Expressways

You can integrate Cisco collaboration infrastructure with more than one Microsoft domain if required. Wherever you put a single Expressway as a gateway, you could use a cluster instead.

The diagram below shows the following different options:

1. This option is used in this document; there is one gateway Expressway (or cluster) into a single Microsoft domain.

2. One gateway or gateway cluster serving multiple Microsoft domains. Requires multiple search rules to route the calls to and from Microsoft infrastructure correctly.

3. It is possible to configure multiple Microsoft domains with an independent gateway serving each. This option is not exhaustively tested, nor is it described in this document.

4. You should avoid configuring multiple gateways to serve one Microsoft domain.

   With this deployment, calls from one video endpoint to another video endpoint that is called via its Microsoft domain will get routed via Microsoft infrastructure rather than directly through the collaboration infrastructure; users could lose duo video, far end camera control, and possibly encryption and video quality.

Appendix 3: Extended Microsoft Deployments

Figure 7   Gateway Expressway Deployment Options, Showing Potential Misconfiguration
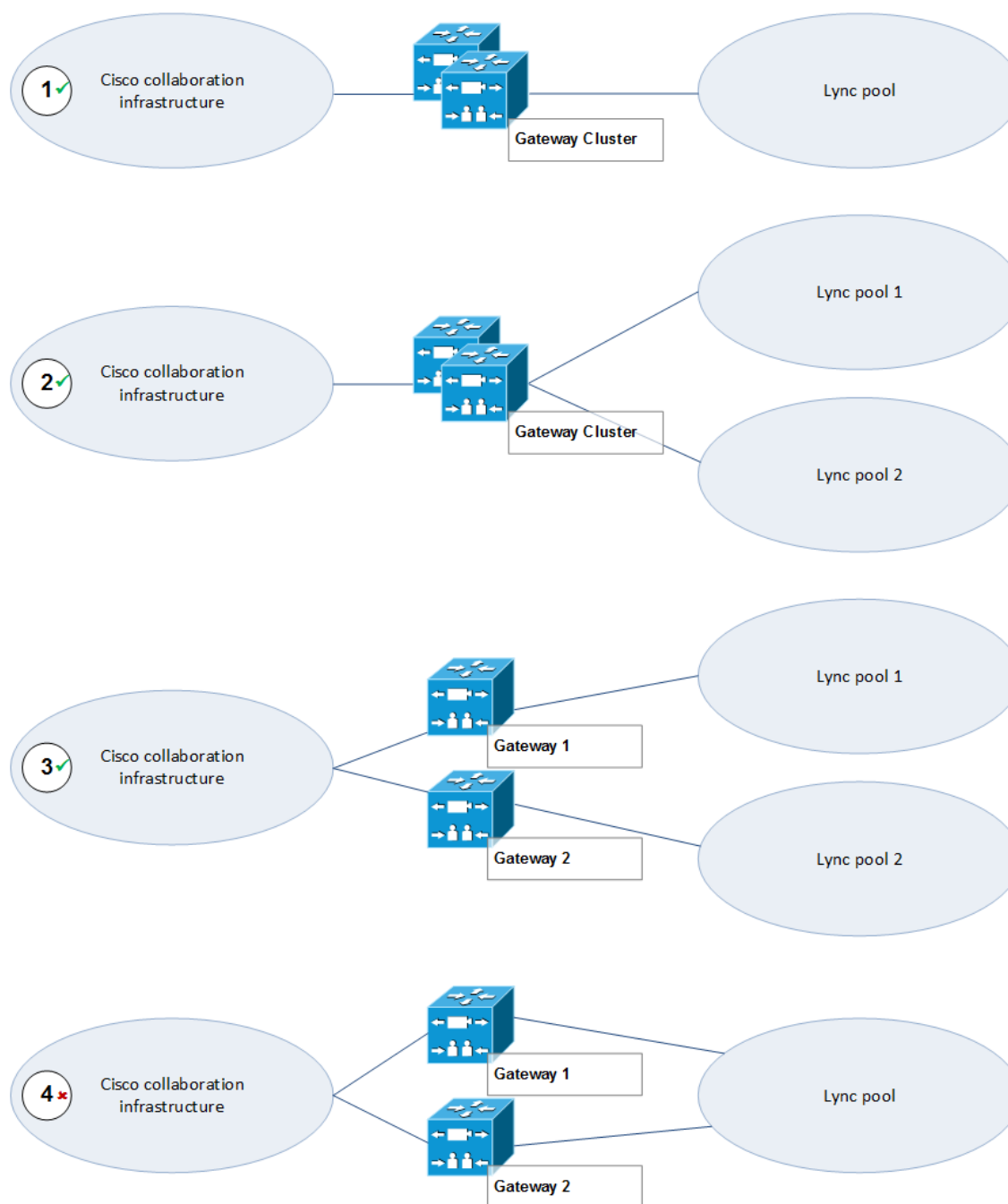
Appendix 4: Assistance with Prerequisite Tasks

Verify Calls Between Microsoft Clients

This is a prerequisite to integrating Expressway with your Microsoft environment. The simplified procedures are listed here but you should refer to the Microsoft documentation for your products.

Enable Users for Microsoft Clients

By default, Active Directory users are not enabled for Lync/Skype for Business. Check that users are enabled to use these clients in the FE Server Control Panel or through Windows PowerShell commands.

Using the Lync Server Control Panel (Lync Server 2010/2013):

1. Open the Lync Server Control Panel and find the Users section.
2. Find the control to enable users, which allows you to search for and add existing AD users.
3. Assign the selected users to the appropriate Lync Server pool.
4. Select which AD user properties are used to generate the users' SIP URIs.

To enable AD users for Lync, using Management Shell:

Use the command `enable-csuser`. For example:

```
enable-csuser -identity "example\alice.parkes" -registrarpool "fepool.example.com" -sipaddress
sip:alice.parkes@example.com
```

See https://technet.microsoft.com/en-us/library/gg398711(v=ocs.16).aspx (Enable-CsUser documentation for Skype for Business Server 2015).

Register Microsoft Clients to Microsoft Server

1. Install and run the Microsoft client.
2. Enter the SIP URI as the sign-in address.
3. Point the client to the FQDN of the correct Microsoft FE pool.
4. Save the configuration and verify log in.

Test Calls

1. Select a contact in the Microsoft client
2. Start a video call
3. Answer the call with the contact's Microsoft client

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark