Cisco VCS and Microsoft Infrastructure

Deployment Guide

First Published: October 2008

Last Updated: February 2018

Cisco VCS X8.9

Microsoft Lync 2010, Lync 2013

Skype for Business Server 2015

Preface

Change History

Table 1   Deployment Guide Change History

Date	Change	Reason
February 2018	Updated Features and Limitations section to describe issue with Microsoft calls if a clustered VCS Expressway is placed in Maintenance Mode.	New information
July 2017	Republished with corrections.	Updated port reference table.
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	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	Updated for VCS X8.1 and Lync 2013. Modified the guide to first describe static route-based deployments, and to place FindMe-based deployment configuration into a separate section.	
April 2013	Removed Appendix 12 Federation.	

Table 1   Deployment Guide Change History (continued)

Date	Change	Reason
December 2012	Revised B2BUA and AM GW integration appendix to refer to external document.	
August 2012	Updated for VCS X7.2.	
June 2012	Updated for VCS X7.1.	
November 2011	Updated for VCS X7.0, OCS 2007 R2 and Lync 2010.	
May 2011	Updated for VCS X6.1 and Lync 2010.	
November 2010	Updated for VCS X5.2.	
December 2009	Updated for VCS X5.	
August 2009	Updated for VCS X3 and X4, OCS 2007 R1 and R2.	
October 2008	Initial release: VCS X3.0, OCS 2007v3.0.	

Contents

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 TelePresence Video Communication Server ("Gateway" VCS).

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

To enable video calling, screen sharing, and presence between VCS-registered video endpoints and Microsoft clients, you need to configure:

- A neighbor zone between the Gateway VCS and the VCS Control
- The Microsoft Interoperability service on the Gateway VCS to route calls to Microsoft
- Static routes from Microsoft FE Servers to the Gateway VCS
- The Presence Server and Presence User Agent on the VCS Control

Note: Previous versions of this guide recommended an extended deployment, using FindMe to enhance presence and provide what we term Single Number Reach (SNR). We consider that to be a legacy deployment, preferring Cisco Unified Communications Manager products for SNR and presence, but we included the details in Appendix 2: Extended Deployment Using FindMe, page 53.

Deployment Scope

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

- Mobile and Remote Access
- Microsoft Interoperability
- Jabber Guest
- Hybrid Services (connector host)

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

A Gateway VCS is a VCS Control (or cluster of VCS Controls) that provides interoperability between a Cisco Collaboration network and the Microsoft environment.

We require that you dedicate a VCS Control to this role so that you:

- Minimize the impact of adding Microsoft interoperability to your existing Cisco Collaboration network.
- Limit the number of VCSs 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 VCSs.

- 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 VCS (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 VCS, 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 between Microsoft clients and your VCS-registered endpoints, screen sharing from Microsoft clients, and presence sharing from the video endpoints.

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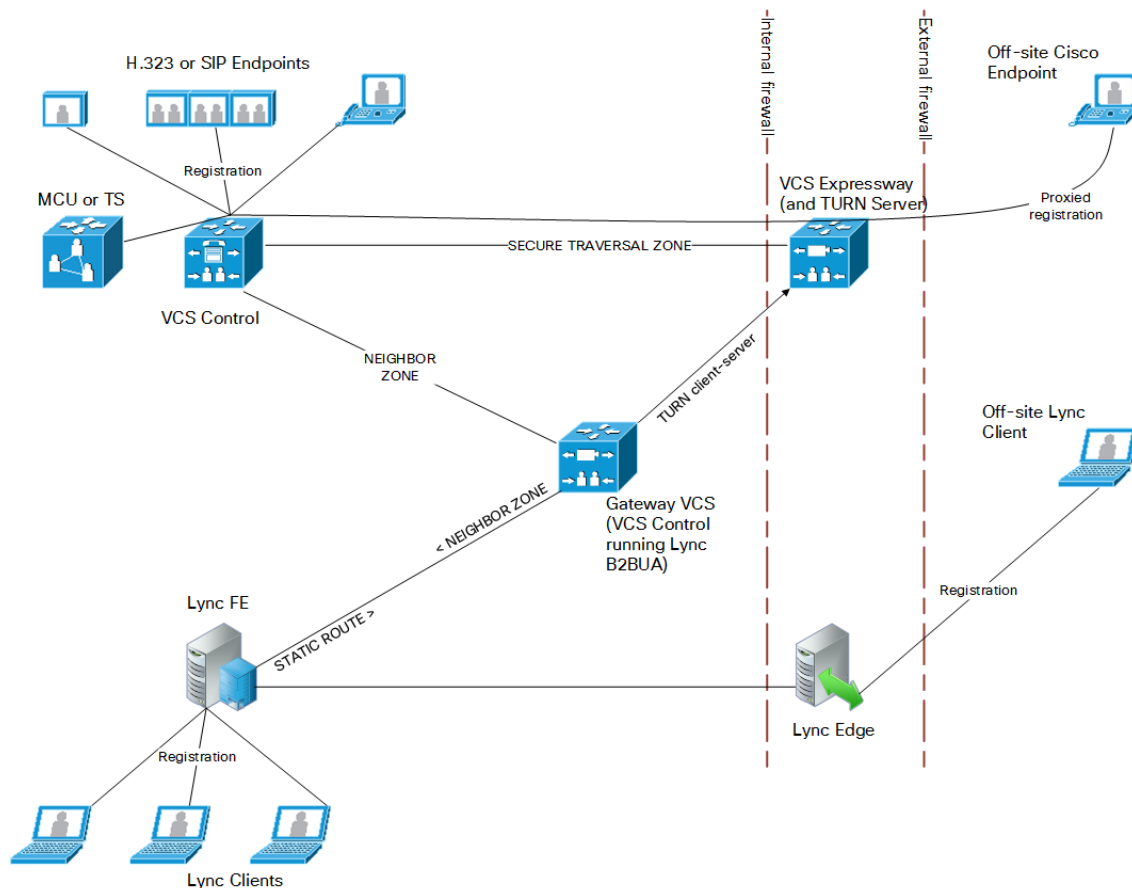
What's in the diagram?

This deployment uses separate registration domains for Microsoft clients and for VCS endpoints. It is possible to use one domain for both sets of endpoints, if you take care to avoid routing loops. If you want to use one domain for both, we recommend using Cisco Unified Communications Manager for your call control.

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:

- VCS Control for primary call control of the Cisco Collaboration video network.
- On-premises and off-premises video endpoints registered to VCS Control.
- A dedicated VCS Control for interoperability with the Microsoft environment (referred to as Gateway VCS).
- VCS Expressway in the DMZ to provide TURN services and to proxy connections from off-premises endpoints to the on-premises VCS Control.
- MCU or TelePresence Server registered to the video network VCS Control.

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 may be SIP or H.323 endpoints; they must register with an ID in the format alias@domain, where domain is a domain hosted on the video network (for example firstname.lastname.device_type@video.example.com).

  We recommend that any H.323 to SIP and IPv4 to IPv6 protocol interworking is performed on the VCS Control.

- 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`
- Endpoints registered to the video network are identified by URIs, frequently including the location or type of the endpoint, for example:
  - Alice's internal video endpoint with an alias of `alice.parkes.office@video.example.com`
  - Alice's home office video endpoint with an alias of `alice.parkes.home@video.example.com`
  - David's internal video endpoint with an alias of `david.jones.office@video.example.com`
  - David's home office video endpoint with an alias of `david.jones.home@video.example.com`
- Microsoft Front End Server is configured with a static domain route which routes URIs with the VCS's video network domain (`video.example.com`) to the Gateway VCS. Take care when using domain static routes; any traffic for that domain that Microsoft cannot handle locally will be routed to VCS.
- The Presence Server on the VCS Control publishes presence information into the Microsoft environment through the Microsoft Interoperability service on the Gateway VCS. The Presence Server must be authoritative for the video domain (`video.example.com`).

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 63 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 VCS 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 VCS deployment.

Table 2   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	Not supported
Lync 2013 for Windows (Windows desktop) that has the option to use the Skype for Business UI[2]	Not applicable	Supported	Not 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 VCS Expressway Cluster Node Placed in Maintenance Mode

This applies if you have clustered VCS Expressway 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 VCS domain and caches the result. If the DNS query resolves to the VCS Expressway that is in Maintenance Mode, call requests will fail until either the Microsoft server cache expires, or the VCS Expressway 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 VCS, 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. X7.2 or earlier software will work with Lync 2013 only if calls are routed through a Cisco AM GW transcoder.

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 VCS does not interoperate with any versions of Microsoft Office Communications Server or Live Communications Server.

Voice and Video Calling

SIP and H.323 Calls

- SIP and H.323 endpoints can make calls via VCS Control to Microsoft clients registered to a Microsoft Server.
- Microsoft clients registered to a Microsoft Server can make calls to SIP and H.323 endpoints registered to VCS Control.
- SIP signaling and RTP media is always routed through the Microsoft Interoperability B2BUA for calls involving Microsoft clients. Each B2BUA instance (one per VCS) can handle 100 simultaneous calls between Microsoft and the VCS video environment.
- Media encryption (SRTP) is supported when TLS is used between VCS and Microsoft and the **Microsoft Interoperability** option key is added to the Gateway VCS.
- 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).

Introduction

- 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.
- If a call from VCS is made to a Microsoft client which has a forward to another VCS-registered endpoint or a FindMe, then VCS sees this as a "loop detected" call.

Upspeeding a Voice Call to Video

- If a voice call is made from a Microsoft client to a VCS-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.
- Interworking a Microsoft client to an H.323 endpoint, the call will only upspeed from voice to video if the upspeed request occurs before the endpoint sends a BRQ lowering the connection bandwidth.

MXP Endpoints

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

Screen Sharing

- Microsoft clients can share their screen with standards-based endpoints in the video network, because the Gateway VCS 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 VCS:

  - 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.

  The VCS Control requires the *Interworking* option key if interworking to H.323 endpoints.

- 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 3   Recommended Number of Desktop Transcode Sessions by Platform

On this platform:	Set **Maximum RDP transcode sessions** to:
1st generation VCS appliance	1
CE500, CE1100‡, or Medium OVA	10
CE1000, CE1100‡, or Large OVA	20 **Note:** This recommendation requires an active 10 Gbps network connection.
Clusters	Same as the individual platform setting. The **Maximum RDP transcode sessions** you enter on the primary applies to each peer in the cluster.

‡ The CE1100 appliance operates with Medium capacity if you install 1 Gbps NICs, or with Large capacity if you install 10 Gbps NICs.

These numbers were chosen conservatively. They are based on the additional CPU load caused by transcoding 1920 by 1080 screens while the Gateway VCS 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 VCS 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:

Figure 2   Lync environment to conference registered to VCS

| Microsoft client | → | Front End Server | —RDP→ | Cisco VCS (MS Interop) | —H.264→ | Cisco TelePresence VCS | → | Cisco MCU or TelePresence Server | → | BFCP- or H.239-capable endpoint |

Figure 3   Lync environment to conference managed by TelePresence Conductor neighbored to VCS

| Microsoft client | → | Front End Server | —RDP→ | Cisco VCS (MS Interop) | —H.264→ | Cisco TelePresence VCS | → | Cisco TelePresence Conductor[1] | → | Cisco MCU or TelePresence Server[2] | → | BFCP- or H.239-capable endpoint |
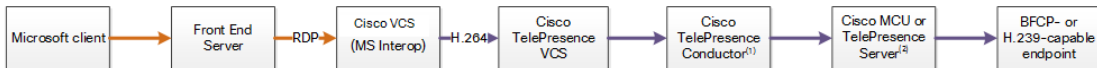
Figure 4   Lync environment to SIP or H.323 endpoint registered to VCS

| Microsoft client | → | Front End Server | —RDP→ | Cisco VCS (MS Interop) | —H.264→ | Cisco TelePresence VCS[3] | → | BFCP- or H.239-capable endpoint |
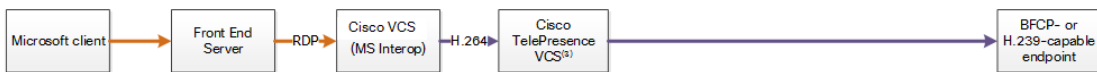
Notes:

1. If you are using the Optimize Resources feature with Microsoft client screen sharing, you need TelePresence Conductor version XC4.0 or later.
2. If you are using the Optimize Resources feature with Microsoft client screen sharing, you need TelePresence Server version 4.2 or later.
3. Requires *Interworking* option key.

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.

Endpoint Presence From VCS

These are the features and limitations of the Presence feature on VCS when used with the Microsoft Interoperability service.

- Use of "Available" for registered endpoints is optional via Presence User Agent (PUA) configuration.
- "Off-line" and "Available" status are reported for users (for up to 100 subscribers).
- "In-call" status is not reported unless you are using FindMe-based configuration.
- The feature does not pass the presence from Microsoft clients to VCS-registered devices.

13

Conferencing

Protocols

In this deployment, we do not support H.323 between VCS 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 registered to the VCS Control.

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 registered to the VCS Control.

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 VCS and the standards-based endpoints do not support endpoints joining Lync conferences.

Multiway

Endpoints can join Microsoft clients into an ad hoc conference using the Multiway feature.

When a Microsoft client is transferred into a Multiway conference, the client will connect using audio only. The Microsoft user will then manually have to enable video on the client after connecting to the conference.

Neither VCS Control nor standards-based video endpoints support the Microsoft proprietary signaling. Note, however use of Multiway on endpoints can join Microsoft clients into an ad hoc conference (see *Cisco TelePresence Multiway Deployment Guide* on the VCS Configuration Guides page).

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 70).

Cisco Collaboration Environment

- Minimum versions: The dedicated Gateway VCS(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 VCS.

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

- The Gateway VCS cluster must have at least Non-traversal call licenses. For H.323 interworking they also need Traversal call licenses.

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

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

- Video network endpoints should be able to call each other (there is more detail on setting this up in Verify Calls Between VCS-registered Endpoints, page 69).

DNS Records

- The FQDNs of all Microsoft FE servers are resolvable by the DNS server used by the Gateway VCS (Gateway VCS and FE Servers should use the same DNS server).

- The FQDNs of each Gateway VCS is resolvable by DNS. If the Gateway VCS 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 VCS in B2BUA mode to enable:

1. VCS-registered SIP and H.323 endpoints to call internal or external Lync clients registered to Lync (Enable Calls to Microsoft Environment, page 17)

2. Internal or external Lync clients registered on Lync Server to call SIP and H.323 video endpoints registered in the video network (Enable Calls from Microsoft Environment, page 28 and Enable Calls from External Microsoft Clients, page 32)

3. Screen sharing from Lync clients to SIP endpoints registered to the video network (Enable Screen Sharing from Microsoft, page 34)

4. Lync clients to see the presence status of endpoints registered in the video network

    This option uses the Presence User Agent on the VCS (Show Presence of VCS-registered Endpoints to Microsoft Clients, page 35).

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

Command or Action	Purpose
Configure the Gateway VCS, page 17	Prepare the Gateway VCS to work in your environment: configure DNS and NTP, and enter a cluster name
Neighbor the VCS Control to the Gateway, page 19	To route calls destined for Microsoft domains towards the Gateway VCS
Configure Microsoft Server Environment , page 21	Enable SIP TLS, trust the Gateway VCS, and configure media encryption
Configure the Microsoft Interoperability Service and Search Rules on the Gateway VCS, page 24	To route calls destined for Microsoft domains towards the internal Microsoft environment
Test Calls from Internal Endpoint to Internal Microsoft Client, page 27	To verify this part of the configuration.

Configure the Gateway VCS

Table 5   Prepare the Gateway VCS for the Network

Command or Action	Purpose
Task 1: Load CA Certificate and Server Certificate to Gateway VCS, page 17	To enable TLS to the Microsoft Server environment
Task 2: Configure DNS and Local Hostname, page 18	So that the Gateway VCS can resolve trusted Microsoft Servers (B2BUA hosts)
Task 3: Enter a Cluster Name, page 19	So that Microsoft Server static routes can resolve the Gateway VCScluster
Task 4: Configure an NTP Server, page 19	To synchronize the Gateway VCS with the Microsoft Server environment
Task 5: Enable SIP TLS, page 19	To enable TLS to the Microsoft Server environment

Task 1: Load CA Certificate and Server Certificate to Gateway VCS

Obtain and load the CA certificate, server certificate, and private key onto each Gateway VCS.

Specify and Request the Certificate

- For mutual TLS authentication, the server certificate must also be able to authenticate the VCS as a client.
- The server certificate for the Gateway VCS must contain its FQDN as the Common Name. If the Gateway VCS is part of a cluster, the FQDN of the cluster and the peer in the cluster must be included as SANs.

  For example, the certificate signing request fields should be:
  - **Subject Name**: Enter the VCS peer's FQDN e.g. vcs01.example.com
  - **Subject Alternate Name**: Enter the VCS cluster's FQDN and the VCS peer's routable FQDN as a comma-separated list, e.g. lyncvcs.example.com, vcs01.example.com

Configuration

Load the Certificates and Private Key

- Go to **Maintenance > Security certificates > Trusted CA certificate** to load the VCS's trusted CA certificate.
- Go to **Maintenance > Security certificates > Server certificate** to load the VCS's server certificate and private key.

See *VCS Certificate Creation and Use Deployment Guide* for more details about creating certificates for VCS.

Task 2: Configure DNS and Local Hostname

Configure the DNS Server Details

If possible, you should configure the Gateway VCS 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:

   `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 VCS, use the IP address of the FE Server platform instead.

On each Gateway VCS peer:

1. Go to **System > DNS**.
2. If the DNS server that the FE Server uses can provide all DNS lookups needed by VCS:
   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 VCS 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 VCS 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 VCS.
   b. **Domain name** to the domain name for this VCS.
2. Click **Save**.

Configuration

> **Note:**
>
> - Concatenate **System host name** with **Domain name** to get the routable FQDN of this VCS
> - These items must be configured to properly enable TLS between VCS and the Microsoft environment.
>
>   If they are not, the neighbor zone may go active and VCS may send messaging to the FE Server, but the FE Server will never open a TLS connection back to VCS.

Task 3: Enter a Cluster Name

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

For each Gateway VCS 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 *VCS Cluster Creation and Maintenance Deployment Guide* if you need to change the cluster name.

Task 4: Configure an NTP Server

On each Gateway VCS peer:

1. Go to **System > Time**.
2. Set **NTP server 1** to the IP address of an NTP server.
3. (Optional) Enter the details of additional NTP servers.
4. Set **Time zone** as appropriate to the location of the VCS.

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

Task 5: Enable SIP TLS

1. Go to **Configuration > Protocols > SIP**.
2. Set **TLS mode** to *On*.

Neighbor the VCS Control to the Gateway

The video network must have a link to the Gateway; to configure this:

1. Set up a neighbor zone from the VCS Control to the Gateway VCS (cluster).
2. Set up a search rule, on the VCS Control, to route calls to the Microsoft domain to the Gateway VCS (cluster).
3. [Only if required] Set up search rules on the VCS Control to route calls to any other domains supported on Microsoft (but not in the video network) to the Gateway VCS (cluster). You don't need to do this if there are no other domains.

Task 1: Create a Neighbor Zone from VCS Control to the Gateway VCS

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.

Configuration

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

Name	An appropriate name, for example "To Gateway"
Type	*Neighbor*
H.323 mode	*Off*
SIP mode	*On*
Port	5061 (or the value that matches SIP port on the Gateway VCS for TLS mode SIP)
Transport	*TLS*
In the Location section: **Peer 1 address**	IP address or FQDN of the Gateway VCS (or the 1st VCS in the Gateway VCS cluster)
In the Location section: **Peer 2** to **Peer 6 address**	IP address or FQDN of the 2nd to 6th Gateway cluster peers (if any)
In the Advanced section: **Zone profile**	*Default*

4. Click **Create zone**.

Task 2: Create a Search Rule to Route Calls for the Microsoft Domain to the Gateway VCS

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the following fields (leave all other fields with default values):

Rule name	An appropriate name, for example "Route to Gateway"
Description	(optional) Describe the search rule to help you distinguish it from others
Priority	Leave as default, for example 100
Source	*Any*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	`.+@example\.com.*`
Pattern behavior	*Leave*
On successful match	*Continue*
Target	Select the Gateway zone, for example "To Gateway"

4. Click **Create search rule**.

Task 3: Create Search Rules to Route Calls for Other Microsoft Domains to the Gateway VCS

If there are any other domains supported by Microsoft (but not in the video network), you will also need to routes calls destined for these domains to the Gateway VCS. This example uses "domain.name":

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

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

Rule name	An appropriate name, for example "Route domain xxx to Gateway"
Description	(optional) Describe the search rule to help you distinguish it from others
Priority	Leave as default, for example 100
Source	*Any*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	`.+@domain\.name.*`
Pattern behavior	*Leave*
On successful match	*Stop*
Target	Select the Gateway zone, for example "To Gateway"

4. Click **Create search rule**.

5. Repeat the process if additional search rules are needed.

Configure Microsoft Server Environment

Task 1: Trust the Gateway VCS

You must create a trusted application pool for each VCS 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:

- If a Director is in use, then configure the Director (pool) to trust the Gateway VCS 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 VCS to the AD domain.

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

   Example Command

   ```
   C:\Users\Administrator.example>New-CsTrustedApplicationPool -Identity lyncvcs.video.example.com -
   ComputerFqdn vcs01.video.example.com -Registrar fepool.example.com -site 1 -RequiresReplication $false
   -ThrottleAsServer $true -TreatAsAuthenticated $true
   ```

   Table 6 Parameter Reference

`-Identity`	The Gateway VCS **cluster** FQDN, which must match the Common Name or a Subject Alternate Name on the VCS server certificate
`-ComputerFqdn`	The Gateway VCS **peer** FQDN (or the primary's FQDN if running a cluster), which must match the Common Name on the VCS 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.

3. If the Gateway VCS 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 vcs02.video.example.com -
   Pool lyncvcs.video.example.com
   ```

   Table 7 Parameter Reference

`-Identity`	The FQDN of the VCS peer you're adding, eg. vcs02.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 VCSApplication1 -
TrustedApplicationPoolFqdn lyncvcs.video.example.com -Port 65072
```

Table 8   Parameter Reference

`-ApplicationID`	Names the Gateway VCS application (this is only used by the Microsoft FE server, it is not a DNS name).
`-TrustedApplicationPoolFQDN`	Specifies the FQDN of the Gateway VCS.
`-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 VCS B2BUA can modify these headers if the Gateway VCS 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 VCS 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.

- **Does the Gateway VCS 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 VCS, then mandatory encryption is possible.

  The Gateway VCS 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.

  However, you can use a zone on the VCS Control to encrypt the media on behalf of those endpoints. Set up your search rules on the VCS Control to route calls to/from those endpoints through a zone that has **Media encryption policy** set to *Force encrypted*.

  Important: If you choose this option, make sure that **Media encryption policy**, on the neighbor zones of the *Gateway* VCS, is set to *Auto*. Do not force encryption on behalf of endpoints on the Gateway VCS.

  If encrypting media on behalf of the endpoints is not practical or possible, then you must change the default media encryption on the FE Server.

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 VCS 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 VCS

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

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

Configuration

If the Microsoft environment...	Configure the signaling destination address and port to be that of the...
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*
Register FindMe users as clients to Microsoft server	*No*
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	If no Cisco AM GW is to be used, set to *No*. If an Cisco AM GW is to be used, see *Microsoft Lync 2010, VCS and Cisco AM GW Deployment Guide*
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, such as user=phone (see for further information about user=phone).

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. (To handle presence messaging a .* is included at the end of the domain to allow any parameters following the domain to be retained in the SIP messaging.)

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, presence etc 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*

Configuration

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 / H.323 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 both SIP and H.323 endpoints registered on VCS Control.

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 9   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 28	Provide the Microsoft Interoperability service on the Gateway VCS with a list of sources of Microsoft calls. The addresses you need depends on how the Microsoft environment is structured.
Neighbor the Gateway VCS to the VCS Control, page 29	Route Microsoft-originated calls from the Gateway VCS to the VCS Control.
Configure Static Routes from Microsoft FE Server to Gateway VCS, page 30	Enable FE Server to route calls for unrecognized destination aliases to the Gateway VCS.
Test Calls from Internal Microsoft Client to Internal Endpoint, page 31	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 VCS 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 VCSs
the Microsoft environment is fronted by a Hardware Load Balancer in front of Directors (see Appendix 3: Extended Microsoft Deployments, page 63)	Hardware Load Balancer and the Directors
the Microsoft environment is fronted by a Director (see Appendix 3: Extended Microsoft Deployments, page 63)	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 63)	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*

Configuration

4. Click **Save**.

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

Notes:

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

- The VCS currently has a nominal limit of 25 trusted hosts. If there are more than 25 trusted hosts, the VCS 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 VCS.

Neighbor the Gateway VCS to the VCS Control

Note: In earlier versions of this document, this step was optional, depending on whether you hosted the Microsoft Interoperability service on the VCS that was acting as registrar. We now require that you use a dedicated VCS for the Microsoft Interoperability service.

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

2. Click **New**.

   We recommend that the connection to the Gateway VCS uses SIP over TLS to communicate so that encrypted calls can be handled.

3. Configure the following fields, leaving others with their default values:

Name	"To video network"
Type	*Neighbor*
H.323 mode	*Off*
SIP mode	*On*
Port	5061 (or the value that matches the SIP TLS port configured on the VCS Control)
Transport	*TLS*
Accept proxied registrations	*Deny*
Location: Peer 1 address	IP address or FQDN of the VCS Control (or the primary peer if it is a cluster)
Location: Peer 2 to Peer 6 address	IP addresses or FQDNs of the subordinate video network cluster peers (if required)

4. Click **Save**.

Create Search Rules to Route Calls with Video Network Domains to the Video Network

Note: In earlier versions of this document, this step was optional, depending on whether you hosted the Microsoft Interoperability service on the VCS that was acting as registrar. We now require that you use a dedicated VCS for the Microsoft Interoperability service.

1. Go to **Configuration > Dial plan > Search rules**.

2. Click **New**.

3. Configure the following fields:

4. Configure the search rule to match the domain supported in the video network (leave other fields with their default values):

Rule name	An appropriate name, for example "Route to Video network"
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	`.+@video\.example\.com.*` (matches anything for the "video.example.com" domain)
Pattern behavior	*Leave*
On successful match	*Continue*
Target	Select the video network zone, for example "To Video network"

5. Click **Create search rule**.

6. Repeat these steps to add a rule for each video network domain.

Configure Static Routes from Microsoft FE Server to Gateway VCS

This involves configuring domain static routes that route calls to the video domains to the Gateway VCS.

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 VCS. 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 VCS Cluster FQDN. Use the IP Address in case of TCP routes.

   `-MatchUri`: the SIP domain in which the Gateway VCS 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 VCS, 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
   "lyncvcs.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. Add and assign other static routes for any other domains in the video network.

5. 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, VCS 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 VCS Control. For example, call `david.jones.office@video.example.com` from a Microsoft client.

Enable Calls from External Microsoft Clients

Table 10   Configure TURN in the Cisco Collaboration network

Command or Action	Purpose
Activate the TURN Server on the VCS Expressway, page 32	Enable the VCS Expressway 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 33	To tell Microsoft clients the addresses of the TURN servers when they are establishing connectivity (ICE)

Activate the TURN Server on the VCS Expressway

Prerequisites

- VCS Expressway is configured as required in Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide on Cisco VCS Configuration Guides page.
- VCS Expressway cluster has TURN Relay licenses.

Create a Local Account for the Gateway VCS and Enable TURN Services

1. Sign in to the VCS Expressway 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:

    a. Make your changes and set **TURN services** to *Off*.

    b. Click **Save** and then set **TURN services** to *On*.

    c. Click **Save**.

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

Prerequisites

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

Configure TURN Services on the Gateway VCS

To enable call connectivity with Microsoft clients calling via an Edge server, you must configure the Gateway VCS 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 VCS Expressway which has TURN enabled. (Just a single VCS; it may be just one peer from a cluster.)
TURN server port	3478 The default TURN listening port on the VCS Expressway. 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 VCS 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 VCS-registered endpoints
- The **Microsoft Interoperability** key is installed on the Gateway VCS
- Read and

Enable RDP Transcoding on the Gateway VCS

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 11   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 VCS-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.

Show Presence of VCS-registered Endpoints to Microsoft Clients

The VCS has a Presence application that you can use to publish the presence of VCS-registered endpoints to Microsoft clients, with limitations as shown in the following table.

Note: This option builds on the VCS and Microsoft deployment described in this document, but we recommend using Cisco Unified Communications Manager IM and Presence Service for presence and Unified CM for SIP registrations and call control.

Table 12   The Presence Information Shared Between Microsoft FE Server and the VCS

	... to VCS	... to FE Server
VCS to ...	Full presence available [1]	Presence = Available only[2]
FE Server to ...	No presence information available[3]	Full presence available [4]

1. Endpoints registered to VCS Control can see the presence status of other endpoints registered to VCS Control.
2. Using SIP-SIMPLE, FE Server only supports the reception of the "Available" status, so presence is limited to "not available" or "available". "In-call" and other rich presence states are not handled. VCS only supports a maximum of 100 subscriptions per presentity.

   Note: Configure your system to register FindMe IDs to the FE Server if you want to publish "In-call" states to Microsoft environment. See Appendix 2: Extended Deployment Using FindMe, page 53
3. FE Server does not supply presence status information about its registered endpoints using SIP-SIMPLE and so no presence information can be supplied to endpoints registered on VCS about endpoints registered on FE Server.
4. Microsoft clients registered to Microsoft FE Server can see the presence status of other Microsoft clients registered to FE Server.

Enable Presence User Agent on VCS Control

We recommend that you enable the Presence Server on the VCS Control and disable it on the Gateway VCS.

We also recommend that you enable the PUA (Presence User Agent) on the VCS Control, which can generate presence information for registered endpoints that don't generate their own presence information.

The PUA generates presence according to the following rules:

- Presence Server uses the endpoint's own presence information (in preference to the PUA generated information) if possible
- PUA generates *In-call* if the endpoint is in a call
- PUA generates *Online* (by default) if the endpoint is registered but not in a call. This presence appears to Microsoft users as *Available*
- PUA can generate presence for H.323 devices if the registered H.323 IDs resemble SIP URIs (eg. name@domain)

See the Presence application topics in the VCS help for more details.

To configure presence in this deployment:

1. On the VCS Control, go to **Applications > Presence** and configure the following:

SIP SIMPLE Presence User Agent	*On* (if VCS Control is to generate presence information for registered endpoints)
Default published status for registered endpoints	*Online*
SIP SIMPLE Presence Server	*On*

2. Click **Save**.
3. On the Gateway VCS, go to **Applications > Presence** and configure the following:

SIP SIMPLE Presence User Agent	*Off*
SIP SIMPLE Presence Server	*Off*

4. Click **Save**.

Test Presence

Set up the endpoints registered on VCS as buddies in Microsoft clients, and then:

- Check the status of the Microsoft-registered users on the Gateway VCS by looking at **Status > Applications > Microsoft-registered FindMe users**. Check that:
  - Registration state = Registered
  - Subscription state = Subscribed
  - Presence state = offline or online
- Check the icon on Microsoft client changes from gray to green when an endpoint is registered on VCS
- Check the icon on Microsoft client changes from green to gray if the endpoint is de-registered from VCS

Media Paths and License Usage

Microsoft Client Call to SIP Video Endpoint

Figure 5   Call between on-premises Microsoft client and on-premises SIP endpoint
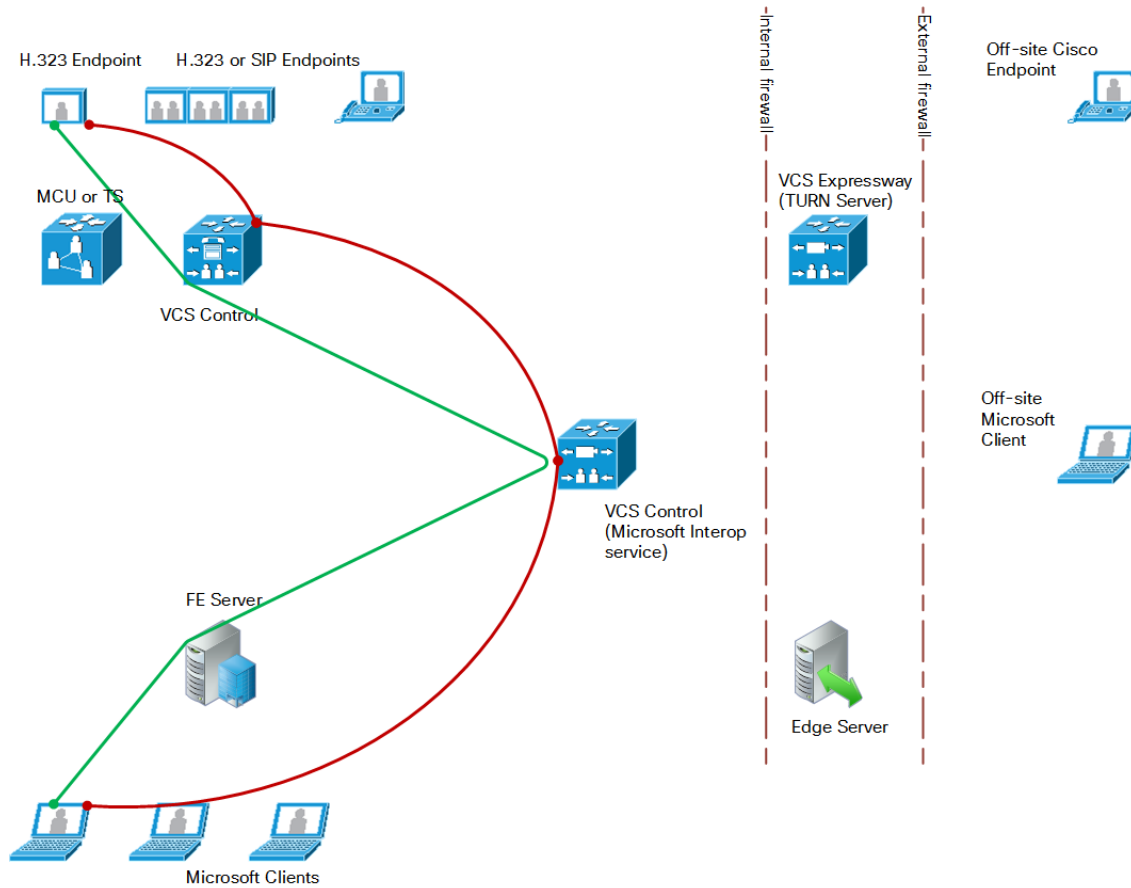

- Licenses consumed by this call:
    - 1 non-traversal call license on VCS Control
    - 1 non-traversal call license on Gateway VCS
- Signaling flows through FE Server, B2BUA, and VCS Control.

37

- 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.

Microsoft Client Call to H.323 Video Endpoint

Figure 6   Call between internal Microsoft client and internal H.323 endpoint

- Licenses consumed by this call:
    - 1 traversal call license on VCS Control
    - 1 non-traversal call license on Gateway VCS
- Signaling flows through FE server, B2BUA, and VCS Control.
- Media is connected directly between the Microsoft client and the B2BUA.
- Media from the H.323 endpoint flows through the VCS Control and then to the B2BUA on the Gateway VCS.
- Calls made in the opposite direction (H.323 endpoint to Microsoft client) use the same signaling and media paths.

Off-premises Microsoft Client Calls Off-premises Video Endpoint

Figure 7   Call between off-site Microsoft client and off-site Cisco endpoint
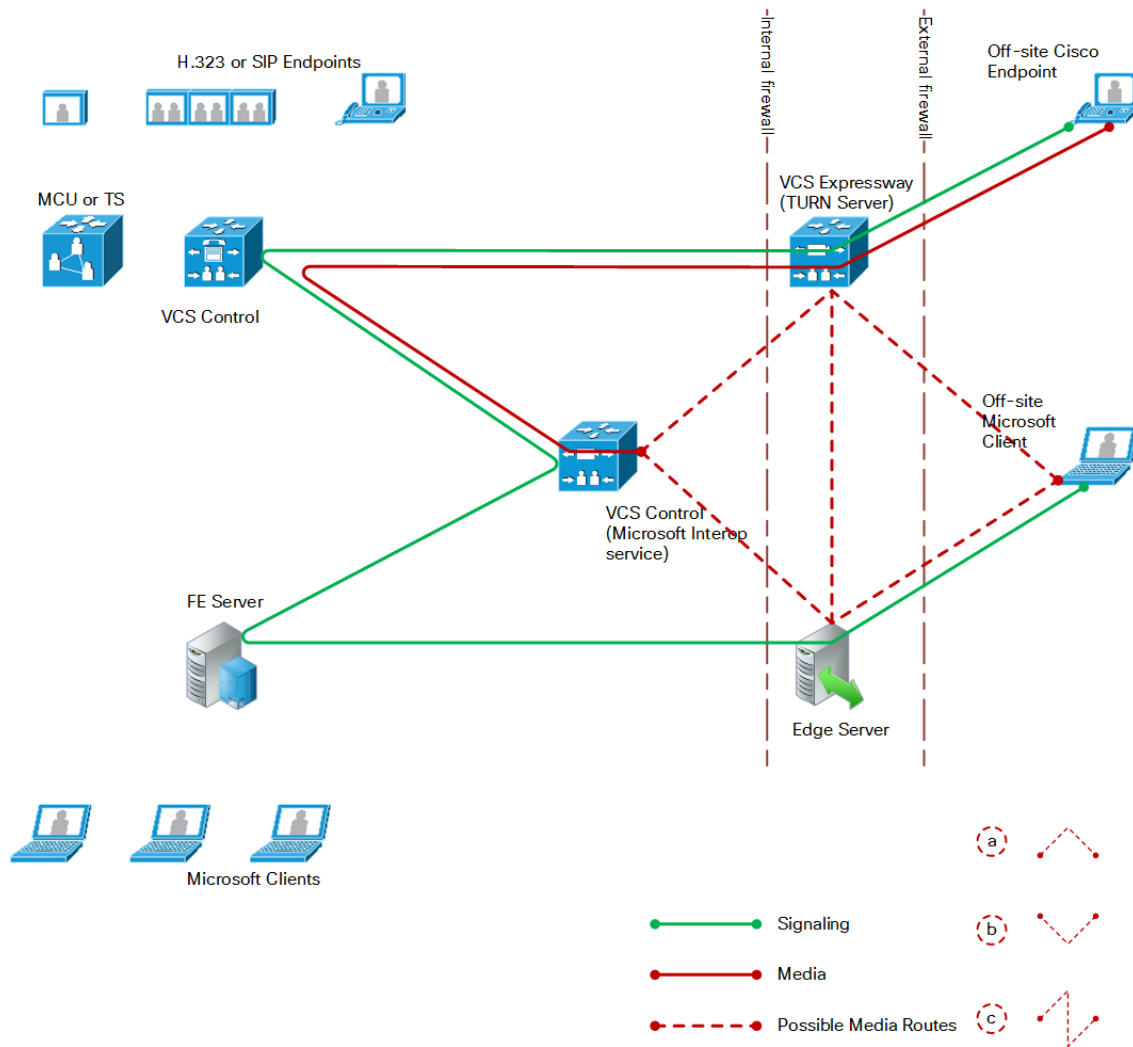
- Licenses consumed by this call:
    - 1 traversal call license and up to 18 TURN licenses on the VCS Expressway
    - 1 traversal call license on the VCS Control
    - 1 non-traversal call license on the Gateway VCS
- Signaling flows through the Microsoft Edge Server, FE Server, MS interop B2BUA, VCS Control and VCS Expressway.

- 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 – VCS Expressway – Gateway VCS – VCS Control – VCS Expressway – External endpoint

  b. Microsoft Client – Microsoft Edge – Gateway VCS – VCS Control – VCS Expressway – External endpoint

  c. Microsoft Client – Microsoft Edge – VCS Expressway – Gateway VCS – VCS Control – VCS Expressway – External 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 between the external Cisco endpoint and the B2BUA flows through the secure traversal zone between VCS Control and VCS Expressway.

- Calls made in the opposite direction (external Cisco endpoint to external Microsoft client) use the same signaling and media paths.

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

Figure 8   Call between off-premises Microsoft client and on-premises SIP endpoint
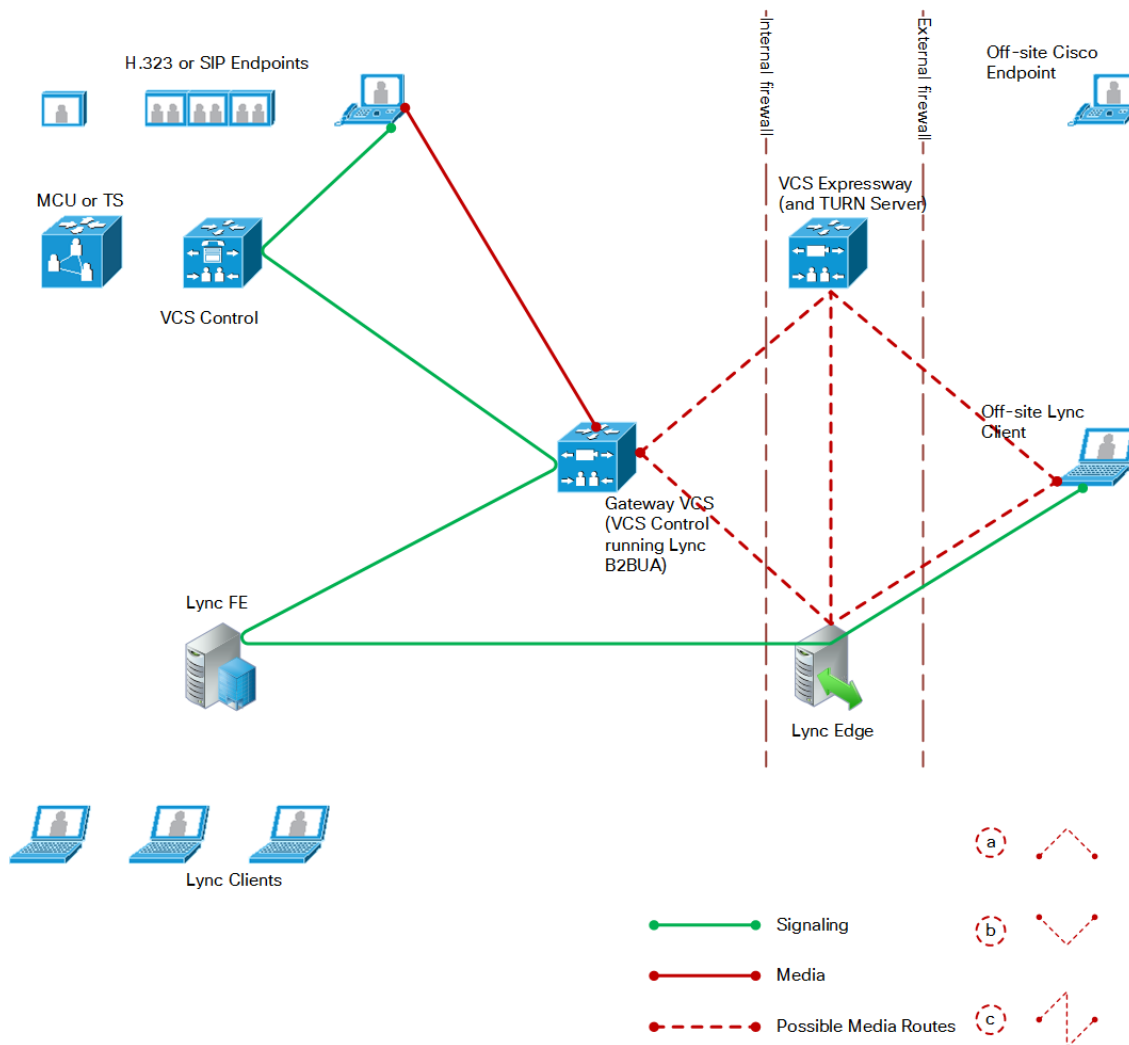
- Licenses consumed by this call:
  - 1 non-traversal call license on the VCS Control, as it is a SIP endpoint
    (an H.323.endpoint would use 1 traversal call license on the VCS Control)
  - 1 non-traversal call license on the Gateway VCS
  - A number of TURN licenses on the VCS Expressway, which depends on what media streams are relayed
- Signaling flows through the Microsoft Edge Server, Microsoft FE Server, B2BUA, and VCS Control.
- 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 – VCS Expressway – Gateway VCS – SIP endpoint

  b. Microsoft Client – Microsoft Edge – Gateway VCS – SIP endpoint

  c. Microsoft Client – Microsoft Edge – VCS Expressway – Gateway VCS – 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 VCS (**Applications > B2BUA**).

Table 13   Between B2BUA and Microsoft Environment

Purpose	Protocol	VCS port	Microsoft port
Signaling to Microsoft server	TLS	65072	5061 (Server SIP listening port)
Signaling from Microsoft server	TLS	65072	Ephemeral port
Presence to Microsoft server	TLS	10011	5061 (Server SIP listening port)
Presence from Microsoft Server	TLS	10011	Ephemeral port
Media (The Microsoft interoperability service should run on a separate "Gateway" VCS and so this range should not conflict with the standard traversal media port range) **Note:** The VCS does not forward DSCP information that it receives in media streams.	UDP & TCP	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 14   Between B2BUA and Internal Video Network

Purpose	Protocol	VCS port	VCS IP port
Internal communications with VCS application	TLS	65070	SIP TCP outbound port on VCS
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, VCS Control

Table 15   Between B2BUA and VCS Expressway Hosting the TURN Server

Purpose	Protocol	B2BUA IP port	VCS Expressway IP port
All communications	UDP & TCP	56000 to 57000	3478 (media/signaling) *

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

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

Table 16   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 17   External Microsoft Client / Edge Server and VCS Expressway

Purpose	Protocol	Microsoft client / Edge server	VCS Expressway
ICE messaging (STUN/TURN) (VCS Expressway 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 18   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 VCS?

The UDP port range of the B2BUA on the Gateway VCS 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 VCS
- 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 VCSs 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 VCS.
- Ensure that all Microsoft servers can successfully look up all Gateway VCS 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 VCS (on the **Status > Applications > Microsoft interoperability** page, Status = Alive is the desired state for both), and, if using FindMe, that the B2BUA has successfully registered FindMe accounts to Microsoft (on the **Status > Applications > Microsoft-registered FindMe users** page **Registration state** = *Registered* and **Subscription state** = *Subscribed* are the desired states).

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 **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).

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 VCS 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 *VCS Certificate Creation and Use Deployment Guide*.

Problems Connecting VCS Control Local Calls

Look at search history to check the applied transforms

1. In VCS, go to **Status > Search history**.

   Search history entries report on any searches initiated from a SETUP/ARQ /LRQ in H323 and from an INVITE/OPTIONS in SIP. The summary shows the source and destination call aliases, and whether the destination alias was found.

2. Select the relevant search attempt. The search history for that search attempt shows:

   - the incoming call's details
   - any transforms applied by pre-search transforms or CPL or FindMe
   - in priority order, zones which matched the required (transformed) destination, reporting on:
     - any transforms the zone may apply
     - found or not found status
     - if not found, the error code as seen in the zone's search response

     repeated until a zone is found that can accept the call, or all matches have been attempted

   (The search may be 'not found' due to lack of bandwidth or because the search from the zone resulted in an H.323 rejection reason or a non 2xx response to a SIP request.)

3. If the search indicates:

   - Found: False
   - Reason: 480 Temporarily Not Available

   this could be because the VCS's zone links are not correctly set up. From the command line execute:

   `xcommand DefaultLinksAdd`

   to set up the links for the default zones. Also check that the links for other zones that have been created.

Note that each H.323 call will have 2 entries in the search history:

- An ARQ to see if the endpoint can be found.
- The SETUP to actually route the call.

The ARQ search does not worry about links or link bandwidth, and so if links do not exist or link bandwidth is insufficient it may still pass, even though the SETUP search will subsequently fail.

Each SIP call will usually only have a single search history entry for the SIP INVITE.

Look at 'Call History' to check how the call progressed

1. Go to **Status > Calls > History**.

   The summary shows the source and destination call aliases, the call duration and whether the call is a SIP, H.323 or SIP< -- >H.323 interworking call.

2. Select the relevant call attempt.

    The entry shows the incoming and outgoing call leg details, the call's status and the zones that the VCS Control used to route the call.

Presence Not Observed as Expected

Presence Server status

- Go to **Status > Applications > Presence > Publishers** to check who is providing presence information to the VCS Presence Server.
- Go to **Status > Applications > Presence > Presentities** to check whose presence is being watched for (on domains handled by VCS Presence Server).
- Go to **Status > Applications > Presence > Subscribers** to check who is watching for presence (of one or more entities in domains handled by VCS Presence Server):

No presence being observed

Check that there is no transform that may be inadvertently corrupting the presence Publication, Subscription or Notify, for example that there is no transform modifying the presence URI. (Notifies are sent to the subscription contact ID, typically <name>@<IP address>:<IP port>;transport=xxx. Any transforms that modify this are likely to stop the presence Notify being routed appropriately.)

Microsoft client fails to update status information

If a Microsoft client is started before the Presence Server is enabled, the Microsoft client may need to be signed out and signed back in again before it will display the correct presence information.

Check for errors

Checking for presence problems should be carried out in the same way as checking for errors with calls: check the Event Log and the logging facilities mentioned in the 'Check for errors' section above.

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 VCS 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 VCS

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

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

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 VCS 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 VCS and FE servers are able to resolve each other's FQDNs in DNS.

VCS to Microsoft client calls fail – DNS server

VCS 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.

VCS 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 VCS is neighbored with the HLB. If it is neighbored directly with a FE Server, trust for VCS will be with the FE Server.

VCS 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 VCS 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/VCS Expressway)

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

One Way Media: Microsoft Client to VCS-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 VCS, and where the video architecture includes a VCS Expressway with TURN enabled and the B2BUA is configured to use that TURN server.

When using a Hardware Load Balancer in front of FE Servers

VCS modifies the application part of INVITEs / OKs received from Microsoft clients to make them compatible with traditional SIP SDP messaging. VCS 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 VCS 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 17 and configure trusted hosts containing the FE Servers' addresses.

Microsoft Clients Try to Register with VCS Expressway

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

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 VCS Expressway, 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 VCS Expressway.

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 shared domain.

- For calls from endpoints that are not part of a FindMe, this means that the endpoints must register to the video network with a domain that is the same as the Microsoft domain.
- For calls from endpoints that are part of a FindMe, the endpoints can register with any domain so long as the FindMe ID has the same domain as the shared Microsoft domain and in the FindMe configuration **Caller ID** is set to *FindMe ID* (instead of *Incoming ID*).

Microsoft Rejects VCS 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 VCS 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 VCS (Lync sees calls coming from the hardware load balancer rather than from the VCS).

B2BUA Problems

B2BUA Users Fail to Register

If B2BUA registration fails to register FindMe users (Registration status = failed), check:

1. The FindMe name is correctly entered into Active Directory.
2. A Microsoft client can register as the FindMe name – you need to log in first from a Microsoft client before the B2BUA can properly control the Microsoft user.

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

Check that the VCS application has been added to the Microsoft trusted application pool and is configured to contact the VCS B2BUA via port 65072 . See Enable Calls to Microsoft Environment, page 17 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 VCS 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 VCS does not trust the server certificates from IM and Presence Service nodes.

Microsoft Mediation Server

Calls to Microsoft Mediation Servers work from endpoints in the VCS video network for SIP initiated calls, but do not work for interworked H.323 initiated calls (the mediation server does not respond to the VCS INFO message, sent to check availability of the destination number).

A workaround is possible if the format of the numbers that will be routed to the mediation server can be configured in VCS.

The workaround is to send some calls through a different zone from the Gateway VCS to the Lync Server, as follows:

1. Create a new neighbor zone and select *Custom* in the **Zone profile** field.
2. Configure the zone with the values shown in Table 19   Custom neighbor zone attributes to work around Mediation Server limitation, page 51
3. Configure one or more search rules, with the correct priority, such that the appropriate subset of calls destined for the Mediation Server are routed through the new zone rather than the standard "To Microsoft Lync Server via B2BUA" zone.
4. You may also need to change the **On successful match** action from *Stop* to *Continue* on the search rule in the "To Microsoft Lync Server via B2BUA" zone. See Enable Calls to Microsoft Environment, page 17.

Table 19   Custom neighbor zone attributes to work around Mediation Server limitation

Setting	Lync Server zone configuration
Monitor peer status	Yes
Call signaling routed mode	Auto
Automatically respond to H.323 searches	Off
Automatically respond to SIP searches	On
Send empty INVITE for interworked calls	Off
SIP poison mode	On
SIP encryption mode	Microsoft
SIP multipart MIME strip mode	On
SIP UPDATE strip mode	On
Interworking SIP search strategy	Info

Table 19   Custom neighbor zone attributes to work around Mediation Server limitation (continued)

Setting	Lync Server zone configuration
SIP UDP/BFCP filter mode	Off
SIP record route address type	Hostname
SIP Proxy-Require header strip list	<blank>

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 VCS 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 VCS deployed with Lync 2013 Front End Server and Lync 2013 for Windows clients.
- Gateway VCS configured for screen sharing.
- The Gateway VCS 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 VCS (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 VCS 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 VCS, 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 VCS.
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: Extended Deployment Using FindMe

You can optionally extend the deployment described in this guide by configuring your video network deployment to use FindMe. This provides richer presence and a more integrated environment. It uses the example deployment depicted below:
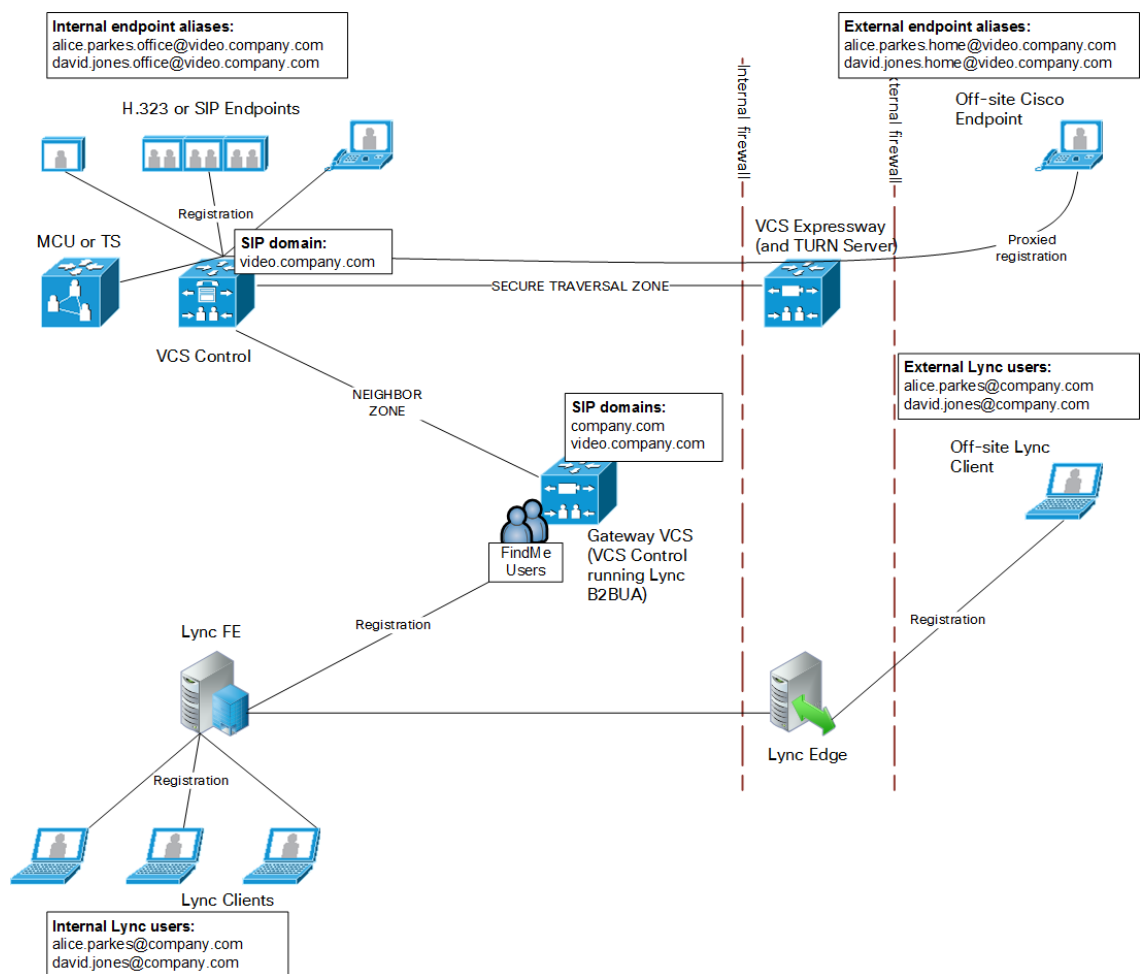
Deployment Information

This deployment configuration consists of:

- FindMe accounts (also known as FindMe users) on the Gateway VCS that use the Lync network's domain (example.com in this example). The B2BUA registers these FindMe accounts into Lync so that Lync sees them as though they were Lync client registrations, for example:
  - David with a URI david.jones@example.com, containing devices david.jones.office@video.example.com and david.jones.home@video.example.com

– Alice with a URI alice.parkes@example.com, containing devices alice.parkes.office@video.example.com and alice.parkes.home@video.example.com

These FindMe accounts specify single or multiple endpoints as primary devices to call; the primary devices can be located anywhere in the video network or anywhere accessible via the video network.

When Lync 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 a registration is to a B2BUA registered FindMe account, Lync Server will send the call to the B2BUA.

– If there is no registration, Lync Server will then check the static domain routes and if there is one for this domain then Lync Server will route the call to the destination specified.

If a corresponding Lync client also exists from a PC, the Lync client on the PC and the video endpoints specified in the FindMe will ring simultaneously when called, whether called from an endpoint communicating with VCS, or whether called from an endpoint communicating with Lync.

For calls into Lync (from whichever video endpoint the user wants to call from) to have a Caller ID / call back ID that works, FindMe must re-write the caller ID of calls to Lync with the relevant Lync SIP user ID. For FindMe to be able to do this, calls must be routed through the VCS holding the relevant FindMe; having a Gateway helps funnel all calls through the correct place.

■ The Lync static routes defined in Configure Static Routes from Microsoft FE Server to Gateway VCS, page 30 are no longer required.

■ MCUs that will receive calls from Lync can register conferences to the video network and make these available to Lync users via a FindMe account (suitable for static conference aliases).

■ The Presence Server must be enabled on the Gateway VCS (and disabled on the VCS Control).

■ The Gateway VCS must be authoritative for the domain shared by Lync and the VCS (example.com), and all of the other domains used in the video network (video.example.com).

■ The Gateway VCS must hold the presence status of endpoints specified in the FindMe accounts in the Lync domain existing on this Gateway VCS (cluster), as FindMe presence only represents the presence of devices whose presence is known on that VCS (cluster). FindMe will only aggregate presence data for devices where their presence state is known on the same VCS that holds the FindMe account.

■ "Available", "off-line" and "in-call" presence may be observed by Lync clients for users and any MCU conferences that are associated with a FindMe account on the Gateway VCS. Note: this requires that the primary video devices within the FindMe account have a URI-based alias, for example firstname.lastname@domain and that their presence is also held on the Presence Server on the Gateway VCS.

Clustered Gateway VCS

To provide enhanced load balancing, the Gateway VCS peers will distribute the shared domain FindMe users between themselves, and register their set with Lync Server. When Lync Server makes a call to one of these user IDs, the call will be presented to the VCS that made the registration – hence the calls are statically load-shared across the cluster.

If any peers go out of service, the remaining active peers take over the registrations of the unavailable peers.

Gateway VCS and Multiple Lync Domains

If Lync supports multiple domains, and the video network is to support these domains as well, we recommend that you use one Gateway VCS (or cluster) to handle each domain. This is because the Lync B2BUA only supports registering FindMe users from a single domain into Lync Server.

If some domains are not used in the video network, but need calls to be routed to them, there does not need to be a Gateway VCS for those domains. Search rules can be added to support routing to these domains.

If different Lync SIP domains are handled by different Gateway VCSs or VCS clusters, take care to ensure that each Gateway VCS or VCS cluster is authoritative for the presence information that is required for the B2BUA registered FindMe users for that one shared domain and all endpoints that are referenced by those FindMe entries.

MCU Configuration for Ad Hoc Conferences from Lync

We recommend that you create FindMe accounts for static/permanent conferences, where the FindMe account contains the SIP URI of the conference as a device. For FindMe-based permanent conferences, presence will show as:

- *Available* if conference does not have participants
- *In-Call* if conference has participants

Optionally, a FindMe account can be created which contains the SIP URI of the MCU's auto attendant. This will allow Lync users to join any conference via the auto attendant. However, this method will not utilize the '*In-call*' presence status available for individual FindMe-based conferences.

Configuration Overview

Prerequisites

The FindMe option key must be installed on the Gateway VCS.

Task List

Table 20   Tasks required to prepare the Gateway VCS for the FindMe deployment

	Command or Action	Purpose
Step 1	Configure the Gateway VCS, page 56	Make the Gateway VCS authoritative for the Microsoft domain and video domain(s) so its Presence Server can aggregate presence information
Step 2	Configure the Microsoft Interoperability Service to Register FindMe Users to Microsoft Server, page 56	Enable Microsoft FE Server to see the FindMe users as if they were Microsoft clients
Step 3	Configure FindMe and Create FindMe User Accounts for Users of Microsoft Clients and VCS-registered Endpoints, page 57	Group video endpoints and Microsoft clients into one alias for each user, so that calls to that user will ring on all of the user's endpoints
Step 4	Configure Active Directory for FindMe Users, page 58	Allow FindMe users to sign in to Microsoft client
Step 5	Configure the VCS Control to Use the Gateway VCS for Presence, page 59	Disable Presence Server on the VCS Control and route PUBLISH messages to the Gateway VCS
Step 6	Configure the Presence Server on the Gateway VCS , page 60	Enable Presence Server on the Gateway VCS and trust PUBLISH messages from the VCS Control
Step 7	Configure the Microsoft Clients, page 61	Enable Microsoft users to sign in and see presence of FindMe users
Step 8	Test Calls and Presence with Microsoft Clients, page 61	Verify that the deployment is working as expected

Configure the Gateway VCS

Create the Required SIP Domains on the Gateway VCS

B2BUA-registered FindMe users need the Gateway VCS to be authoritative for the FE server's shared domain (example.com). It also needs to be authoritative for any other domains in the video network (to support the Presence Server, and to aggregate presence information for devices associated to the FindMe accounts).

1. Go to **Configuration > Domains**.
2. Click **New**.
3. Set **Name** to *example.com*.
4. Click **Create domain**.
5. Repeat for all the other domains in the video network, including video.example.com.

Domains   You are here: Configuration ▸ Domains ▸ Edit

Configuration	
Domain name	✱ example.com ⓘ

Configure the Microsoft Interoperability Service to Register FindMe Users to Microsoft Server

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

Register FindMe users as clients to Microsoft server	*Yes*
Microsoft domain	Select the shared Microsoft domain, e.g. example.com

3. Click **Save**

Configure FindMe and Create FindMe User Accounts for Users of Microsoft Clients and VCS-registered Endpoints

1. Go to **Maintenance > Option keys** and ensure that the **FindMe** key is listed.
2. Go to **Applications > FindMe**.
   a. Set **Mode** to *On*.
   b. Set **Caller ID** to *FindMe ID*.

   Setting FindMe to present the FindMe ID (rather than the endpoint ID) means that any device in the primary list of FindMe devices will provide the FindMe ID as the Caller ID. Thus, if a called party rings the caller ID back, all FindMe endpoints will ring, not just the endpoint that made the initial call.

   c. Click **Save**.

3. For each user that is to share Microsoft client and VCS endpoints, create a FindMe user account on the VCS with the same URI as the Microsoft client:

   a. Go to **Users > FindMe accounts**.

   (If you are using Cisco TMSPE you must set up the accounts via Cisco TMS instead.)

   b. Click **New**.

   c. Configure the following fields:

Username	Username used by the FindMe user to log in to VCS to administer this account.
Display name	Full name of this user.
Phone number	E164 number to use when outdialing to a gateway.
FindMe ID (dialable address)	URI with Microsoft's domain that will register to Microsoft infrastructure as though it were a Microsoft client.
Principal device address	Routable endpoint URI / E164 or H.323 ID to call when this FindMe is called.
Initial password and **Confirm** password	Password needed by the FindMe user to log in to VCS to administer this account. (Not configurable if using remote authentication (**Users > LDAP configuration > FindMe authentication source** = *Remote*)
FindMe type	*Individual*

4. Ensure that the domain shared with Microsoft is resolvable by the VCS's DNS server; we recommend that you use the same DNS server as the Microsoft FE servers use. See Enable Calls to Microsoft Environment, page 17.

Configure Active Directory for FindMe Users

Ensure that Active Directory user accounts exist for all FindMe accounts on the Gateway VCS(s) that will register to Microsoft infrastructure.

On the server running the Active Directory for the Microsoft client users:

Create Users

1. Run **Active Directory Users and Computers**
2. Open the **Users** folder under the required domain (example.com in our example)
3. Click **Create new user**
4. Enter the user's first name, last name, and logon name
5. Click **Next**
6. Configure the following fields:

Password	The user's password
Confirm password	Retype the password
Password never expires	Select this check box.

7. Click **Next**.
8. Click **Finish**.
9. Repeat for all FindMe accounts.

Enable Users

1. Enable the users for Lync/Skype for Business:

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

   a. Open the Lync Server Control Panel and find the Users section.

   b. Find the control to enable users, which allows you to search for and add existing AD users.

   c. Assign the selected users to the appropriate Lync Server pool.

   d. 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).

2. Repeat for all AD users that are named after FindMe accounts

Configure the VCS Control to Use the Gateway VCS for Presence

Disable the Presence Server on the VCS Control

1. Go to **Applications > Presence**.

2. Configure the following fields:

SIP SIMPLE Presence User Agent	*On* (if VCS Control is to generate presence information for registered endpoints)
Default published status for registered endpoints	*Online*
SIP SIMPLE Presence Server	*Off* (the Gateway VCS will be the Presence Server)

Create a Search Rule to Route Messages to the Presence Server on the Gateway VCS

The PUA on the VCS Control needs to be able to route PUBLISH messages from its domain endpoints to the Presence Server running on the Gateway VCS. To do this, a search rule is required:

1. Go to **Configuration > Dial plan > Search rules**.

2. Click **New**.

3. Configure the following fields:

Rule name	An appropriate name, for example "Route PUBLISH messages to Gateway"
Priority	Leave as default, for example 100. Note that this should be a lower priority (a larger number) than the priority configured for the LocalZoneMatch.
Source	*Any*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	Configure the pattern to match the domain supported in the video network, for example: .*@video\.example\.com
Pattern behavior	*Leave*
On successful match	*Continue*
Target	Select the Gateway zone, for example "To Gateway"

4. Click **Create search rule**.

   Note that this search rule does not conflict with Local Zone searches (which may contain the same pattern match string) because the PUA is not treated as a Local Zone registered device.

5. Create additional search rules for any other SIP domains supported by this VCS (i.e. for endpoints that are registered to the VCS Control) otherwise Presence will not work (messages will not get forwarded).

Configure the Presence Server on the Gateway VCS

Enable the Presence Server

On the Gateway VCS:

1. Go to **Applications > Presence**.
2. Configure the following fields:

SIP SIMPLE Presence User Agent	*Off*
Default published status for registered endpoints	*Online*
SIP SIMPLE Presence Server	*On*

Treat Presence Messages as Authenticated on the Neighbor Zone to the VCS Control

Ensure that the zone to the video network has an authentication policy of *Treat as authenticated* (the Presence Server accepts PUBLISH messages only if they have been authenticated):

1. Go to **Configuration > Zones > Zones**.
2. Select the "To Video network" zone.
3. Find the **Authentication policy** control and select *Treat as authenticated*.
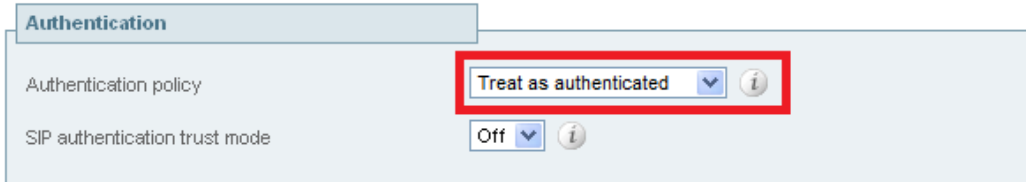
4. Click **Save**.

Notes:

- The Gateway VCS that connects to the Microsoft Server must be the presence server for any SIP domains that Microsoft Server might want to look at for presence; this limits the number of VCSs that Microsoft server's presence requests will travel through.
- Presence requests use up SIP resources and with typically thousands of Microsoft clients connected that may be requesting presence, it is best to limit the range of where the presence requests can go, especially not letting them reach VCSs that may already be heavily used for taking calls.

Configure the Microsoft Clients

1. Set up **Sign-in address** as required. This is the SIP URI of the Microsoft user.

   If the Microsoft user also has video endpoints on the video network, the Sign-in address is the same URI you entered as the B2BUA registered FindMe user ID, for example david.jones@example.com.

2. Log in to the Microsoft Client.

   The FE Server will not provide presence for FindMe users to other Microsoft clients until the user associated with a FindMe has signed into a Microsoft client.

3. Repeat for each FindMe user that has not already signed in.

Test Calls and Presence with Microsoft Clients

Verify FindMe Registrations

After the FindMe accounts have been configured for at least 60 seconds:

1. On the Gateway VCS, go to **Status > Applications > Microsoft-registered FindMe users**.
2. Verify the following for each FindMe user:
   - Registrations state is Registered
   - Presence state is Online (if **Default published status for registered endpoints** is set to *Online*, otherwise expect to see Offline)
   - Subscription state is Subscribed
3. If the states are not as expected, check that the FindMe and Active Directory registered names are identical.

Test from Microsoft Clients

Test calls from Microsoft clients registered on Microsoft FE Server to endpoints registered on VCS Control. For example, call david.jones@example.com or alice.parkes@example.com from a Microsoft client.

1. Open the Microsoft client and verify that you can see presence of VCS-registered endpoints
2. Make a video call from the Microsoft client to a VCS-registered endpoint

Test Call-forking from the Microsoft Client and From a VCS-registered Endpoint

1. Make a video call from a VCS-registered endpoint to a Microsoft-registered FindMe user.
2. Verify that the call forks to the user's other VCS-registered endpoint(s) and Microsoft client , as listed in the FindMe entry for the called user.
3. Make a video call from a Microsoft client to a Microsoft-registered FindMe user.
4. Verify that the call forks to the Microsoft client and to any VCS-registered endpoint(s), as listed in the FindMe entry for the called user.

Limitations of the FindMe Deployment

Microsoft Interoperability Service Only Registers to One Lync Domain

Gateway VCS can route to multiple Microsoft domains. However, if you are using the FindMe deployment, be aware that the B2BUA can only proxy registrations from one FindMe domain to Microsoft. If you need users from multiple FindMe domains to register to Microsoft FE server, you must use multiple Gateway VCSs.

FindMe Caller ID set to FindMe ID Causes Calls from Microsoft Client to Fail

If all of the following are true:

- FindMe Caller ID is set to *FindMe ID*
- a Microsoft client's URI is in the active location of a FindMe
- a call is made from that Microsoft client to a SIP destination

Then the call will fail because Microsoft does not expect the caller ID (From: header) to be modified.

If the call is interworked on the Gateway VCS, the call will work as required.

Best practice is that a Microsoft client should never be included as a FindMe device. Microsoft clients and video endpoints are related to one another using B2BUA registration of FindMe IDs where the FindMe URI is the same as the Microsoft client URI.

Need to log in to Microsoft client before FindMe presence shown to other Microsoft users

Microsoft FE Server will not provide presence for FindMe users to other Microsoft clients until the user associated with a FindMe has signed into the Microsoft client.

Appendix 3: Extended Microsoft Deployments

Clustered Gateway

When this document refers to a Gateway VCS, a cluster of VCSs 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 VCS 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.

Appendix 3: Extended Microsoft Deployments

An example architecture is shown below:
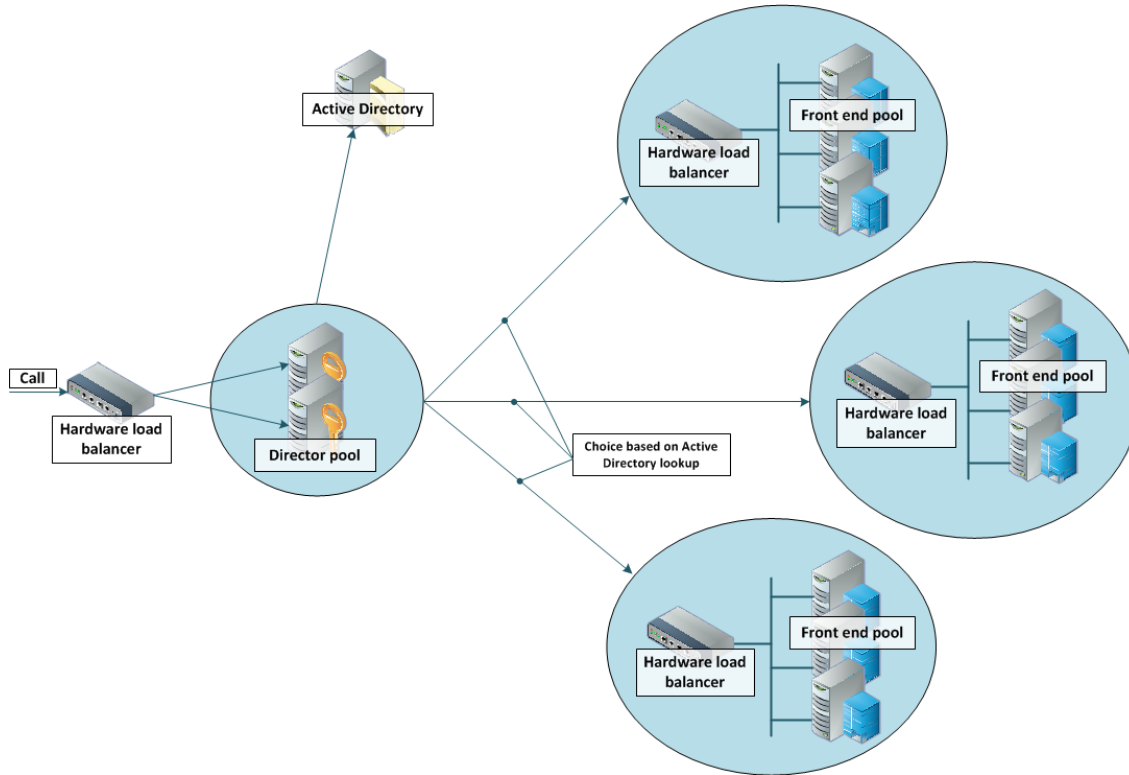
A smaller deployment may not use Director servers, but may just use a Hardware Load Balancer in front of a set of Front End Servers.
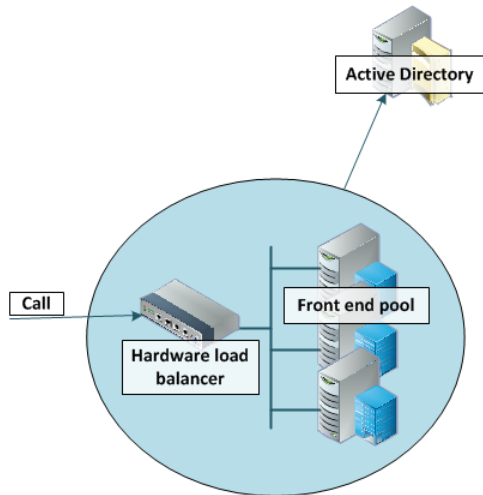
Appendix 3: Extended Microsoft Deployments

A Microsoft environment may use DNS instead of the Hardware Load Balancer, for example:
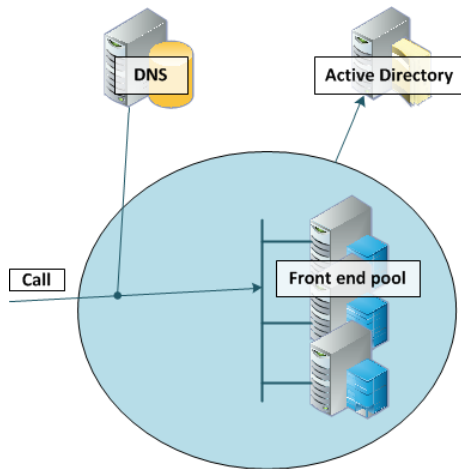
Note that Microsoft requires that the AD server and the FE Server are on separate machines.

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 VCS Expressway connecting to the public Internet. (Calls involving a Microsoft Edge server require the VCS 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.)
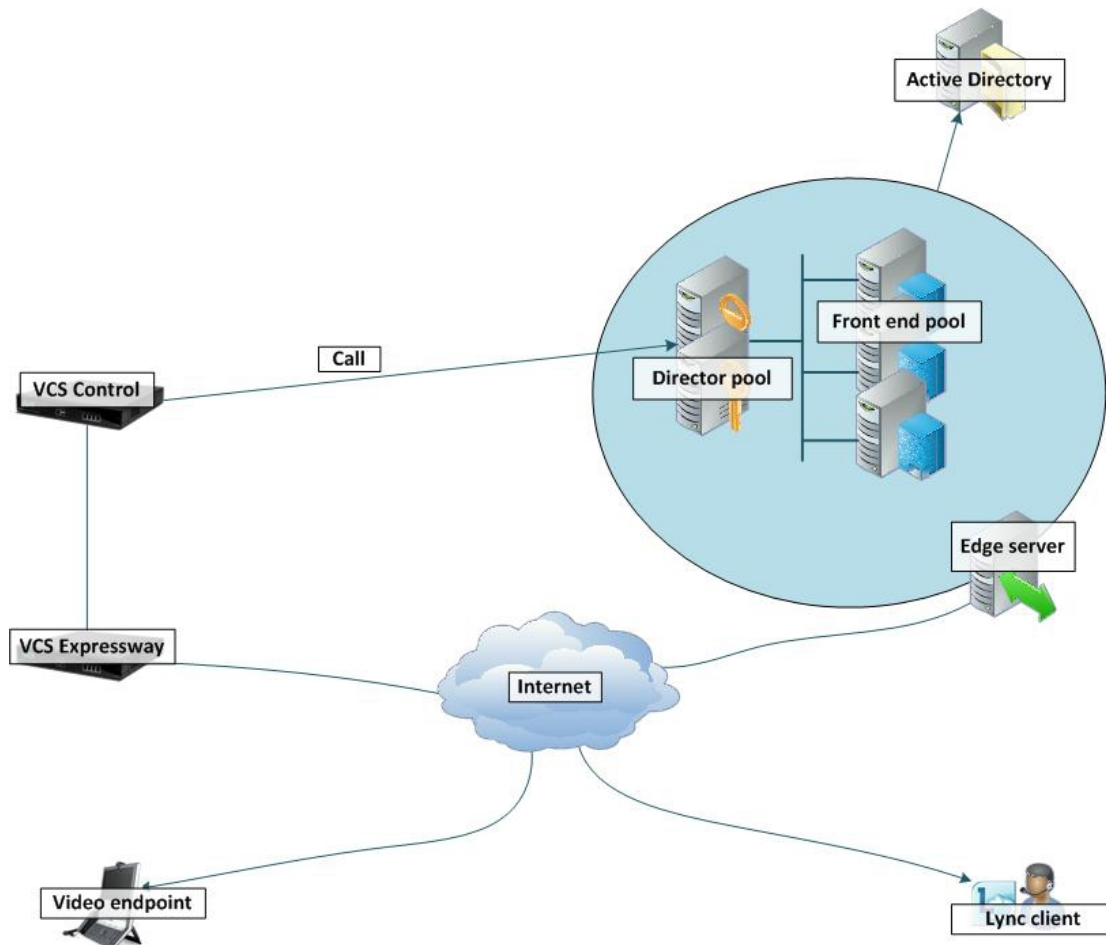
In any deployment with VCS and Microsoft infrastructure:

- Traffic is sent via a static SIP route form the Microsoft infrastructure to the VCS. The flow is either directly from a Front End Server, or from the FE Server via a Director, to the VCS.
- 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 VCS(s).
  - Directors should route the video network domain (video.example.com) to the Gateway VCS cluster FQDN.
  - Depending on Microsoft environment, FE Servers may route SIP traffic directly to the VCS, 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 VCS(s).
  - Directors should route the video network domain (video.example.com) to the Gateway VCS cluster FQDN.
  - Depending on Microsoft environment, FE Servers may route SIP traffic directly to the VCS, 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 VCS(s).
  - All FE Server pools should route the video network domain (video.example.com) to the Gateway VCS 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 VCS(s).
  - It should route the video network domain (video.example.com) to the Gateway VCS cluster FQDN.

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

Gateway VCS 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.

Appendix 3: Extended Microsoft Deployments

Figure 9   Gateway VCS Deployment Options, Showing Potential Misconfiguration
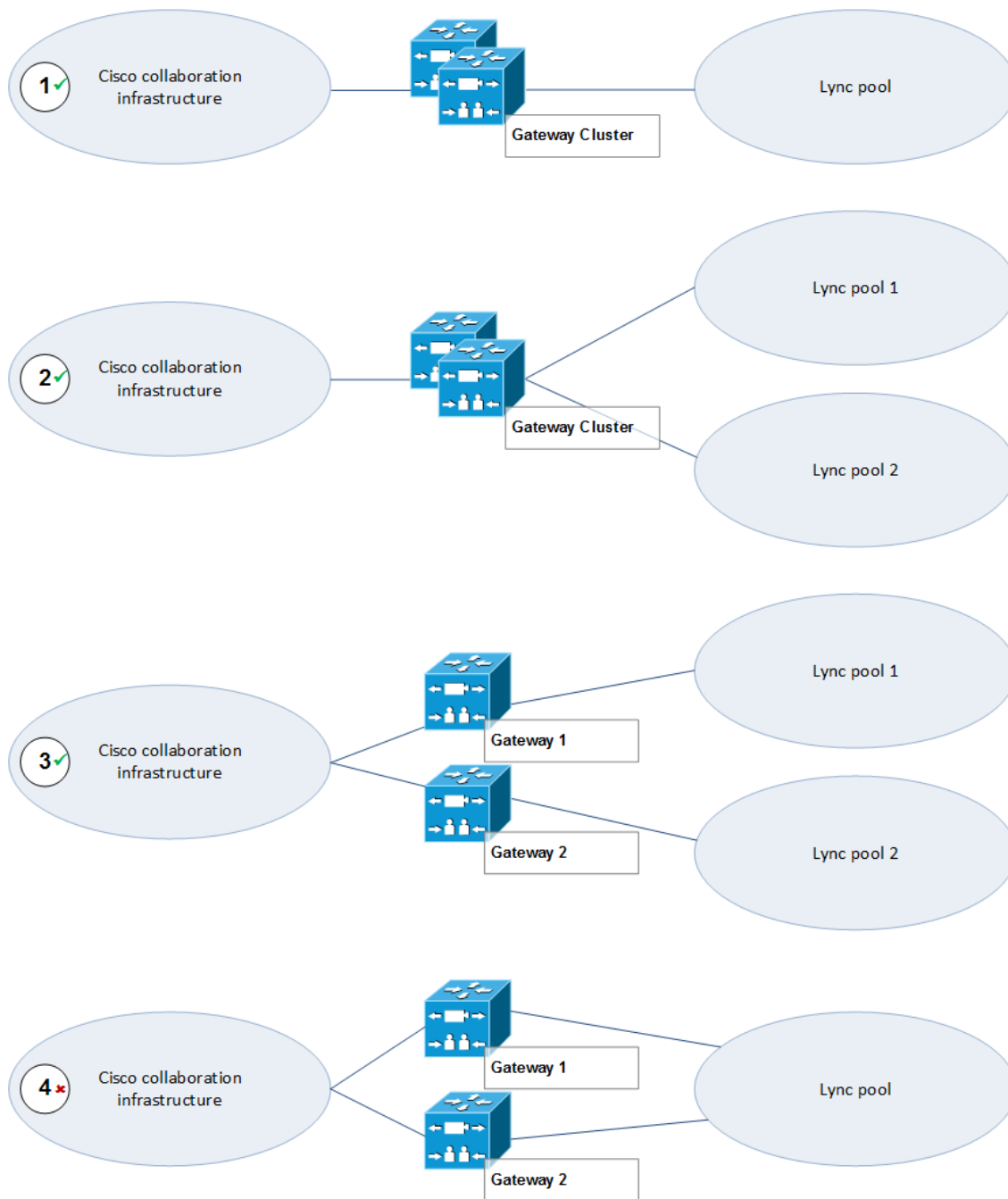
Appendix 4: Assistance with Prerequisite Tasks

Verify Calls Between VCS-registered Endpoints

The configuration described in this section should already be in place and operational.

VCS Control Configuration Summary

The configuration of the VCS Control in the video network to allow calls to be made between endpoints that register to them should already have been carried out. Ensure that the SIP domain of the video network, which is needed for SIP registration and presence handling, is configured.

If appropriate, you may also want to configure interworking to handle calls with any H.323 endpoints that are registered to other systems in the video network.

Ensure SIP Domain of Video Network Endpoints is Configured in the VCS Control

SIP endpoints register with the VCS Control with a URI in the format user-id@sip-domain. The VCS Controls accepting these registrations must be configured with the SIP domain information so that it will accept these registrations.

1. Go to **Configuration > Domains**.
2. Check that the domain is listed; if it is not listed:
   a. Click **New**.
   b. Set **Name** to, for example, video.example.com.
   c. Click **Create domain**.
3. Repeat for any other domains being used.

Configure Interworking for H.323 Endpoints Registered to Other Systems

By default the VCS Control will perform H.323 to SIP protocol interworking between H.323 endpoints registered to the VCS Control and any SIP devices also registered to the VCS Control or to Microsoft devices.

If you have any H.323 endpoints that are registered to other systems in the video network, you will need change the interworking configuration from the default of *Registered only* to *On*:

1. Go to **Configuration > Protocols > Interworking**.
2. Set **H.323 <-> SIP interworking mode** to *On*.
3. Click **Save**.

Register Video Endpoints to the Video Network

Endpoint Configuration

For H.323, configure the endpoints as follows:

- H.323 ID (for example, david.jones.office@video.example.com)
- H.323 Call Setup Mode = Gatekeeper

- Gatekeeper IP address = IP address or FQDN of VCS Control (cluster)

For SIP, configure the endpoints as follows:

- SIP Address (URI) (for example, alice.parkes.office@video.example.com)
- Server Address (Proxy address) = IP address or FQDN of VCS Control (cluster)

Confirm Registrations

Registration status can be confirmed on the **Registrations** page (**Status > Registrations**).

By default the VCS Control accepts all registrations to SIP domains configured in the VCS Control. You can limit registrations by explicitly allowing or denying individual registrations (see *VCS Administrator Guide* for further details).

Calls can now be made between endpoints registered on VCS Control.

Test Calls

To test the configuration:

1. Make some test calls between the endpoints.
2. Clear the calls.
3. Check the **Call history** page on the VCS Control (**Status > Calls > History**).

Verify Calls Between Microsoft Clients

This is a prerequisite to integrating VCS 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

Appendix 5: Additional Information

B2BUA Registration on Gateway VCSs

The B2BUA FindMe registration function allows personal video endpoints to appear in a similar manner to an endpoint registered directly to Microsoft FE Server with the same credentials as an existing Microsoft user, but still maintain the benefits of having the endpoint register to the VCS which is designed to support video calling.

The B2BUA registration function also means that the user credentials are no longer needed on each individual video endpoint. This is possible because the VCS B2BUA is configured as a trusted host to Microsoft FE Server. This simplifies the long term endpoint management since passwords do not need to be regularly updated on the video endpoints.

What Does Register FindMe users as clients to Microsoft server do?

When enabled, FindMe users that are in the shared domain with Microsoft are registered to the Microsoft Server so that they appear like Microsoft clients.

This means that if a Microsoft client registers to a Microsoft Server, and a FindMe user is registered as that same user to a Microsoft Server, when the user is called by another Microsoft client, the call will be forked to both the registered Microsoft client and also to the VCS's FindMe. This means that Microsoft clients and all video endpoints configured as primary devices in the FindMe will ring when called at the Microsoft client address.

Without registering the shared domain FindMe user, the Microsoft Server will not fork the call to VCS, but:

- if a Microsoft client is registered with the called address then just that Microsoft client will ring.
- if there is no Microsoft client registered but there is a static domain route to the VCS for that domain, the call will be routed to VCS to handle.
- if there is no Microsoft client registered and there is no static domain route for this call then the call will just fail.

The Microsoft Server only allows FindMe users to register if the FindMe ID being registered is a valid user in the Lync Active Directory (in the same way that Microsoft clients can only register if they have a valid account enabled in the Lync AD).

Registering FindMe users also allows the presence of these users to be provided to the Microsoft Server and for "in-call" as well as "available" and "off-line" status to be provided. Endpoint devices and FindMe entries that are not registered to a Microsoft Server can only communicate "available" and "off-line" status to the Microsoft Server. The Gateway VCS (or VCSs) must host the presence server for the domain shared with Microsoft (example.com) in order for presence to be provided to the Microsoft Server.

The Gateway VCS must also host the presence server for the domain of the video network (video.example.com). This is because presence of a FindMe entry can only be provided if the presence status of the device(s) in the active location of the FindMe entry are hosted on the Gateway VCS. If FindMe entries contain multiple devices in the active location, VCS will aggregate the presence of those devices whose presence is hosted on the Gateway VCS and present the appropriate overall presence status.

Use of FindMe also allows any endpoint that is referred to in the FindMe to take on the caller ID of that FindMe entry. This means that whichever video endpoint makes the call, the receiving Microsoft client and video endpoints will see the call as having come from the FindMe ID. This is especially useful when the called party wants to return the call; the return call calls the FindMe ID resulting in all endpoints relating to this FindMe and any Microsoft clients registered with this ID all ringing simultaneously – rather than the return call being addressed directly to the single endpoint that made the call.

Configuring Domains

It is best practice to keep the video endpoints in their own domain, and just have the FindMe users on the Gateway VCS with the same domain as the Microsoft Server. This avoids any confusion as to what functionality will be received for each entity. When a call arrives for the FindMe user, FindMe will forward calls appropriately to the defined endpoints, whichever domain they are in.

For example, when alice.parkes@example.com is called, the call will fork to the Microsoft client with the same name, and also to alice.parkes.office@video.example.com and alice.parkes.home@example.com (assuming that these two devices are listed as primary devices in Alice Parkes' FindMe.)

We strongly recommend that you create the Microsoft client users first and have them sign in at least once from a Microsoft client. You can create the FindMe accounts 5 to 10 minutes later on the Gateway VCS (when the user is fully available on Microsoft FE).

B2BUA and Cisco AM GW Integration

For full instructions about how to configure the Microsoft Interoperability service with a Cisco TelePresence Advanced Media Gateway (Cisco AM GW), see *Microsoft Lync 2010, VCS and Cisco AM GW Deployment Guide*.

Previous versions of that document are also available for earlier, non-B2BUA VCS and Cisco AM GW deployments.

TEL URI Handling for VCS to Microsoft Calls

If an endpoint wants to dial a telephone number rather than selecting a user from a directory, the VCS Control must format the telephone number appropriately for the Microsoft Server to be able to look it up. The Microsoft environment expects to see telephone numbers (known as TEL: URIs) in the form: `+<country code><full dialed number>`

VCS Control can use transforms to appropriately format the telephone numbers. These transforms can either be implemented globally using **Configuration > Dial plan > Transforms** or just for the Microsoft neighbor zone by configuring the transform in the appropriate search rules.

For example, for 4 digit extension number dialing to be expanded to a full telephone number for a company in the UK whose telephone number is 781xxx, an extension number 1008 would need to be expanded to +441344781008. This can be implemented by configuring a transform as follows:

Priority	80 (match in preference to the no transform needed rule - 80 is higher priority than 100)
Source	*Any*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	(1...)@example\.com(.*)
Patter behavior	*Replace*
Replace string	+44134478\1;@example.com;user=phone\2
On successful match	*Continue*
Target Zone	*To Microsoft destination via B2BUA*

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.

© 2008-2018 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)