Core Applications

Revised: January 22, 2015

This chapter describes the core applications included in the Preferred Architecture for Enterprise Collaboration. While many additional applications from Cisco and our Ecosystem partners are available, this chapter focuses on a subset of core applications that are necessary for most collaboration environments. The Preferred Architecture is built with all of the available applications in mind to simplify the deployment of these applications and avoid unnecessary configuration changes.

The two main sections of this chapter explain how to implement Unified Messaging with Cisco Unity Connection and Conference Scheduling with Cisco TelePresence Management Suite (TMS). Each of those sections contains a description of the core architecture as well as details about the deployment process.

A third section of this chapter describes Tools for Application Deployment, namely: Cisco Prime Collaboration Deployment (PCD) and Cisco Prime License Manager (PLM). There is also a list of Additional Applications at the end of this chapter.

What's New in This Chapter

Table 5-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 5-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:	Revision Date
Cisco TelePresence Conductor	Conference Scheduling with Cisco TelePresence Management Suite (TMS), page 5-33	January 22, 2015

Prerequisites

Before deploying the core applications for the Preferred Architecture, ensure that:

- Cisco Unified Communications Manager (Unified CM) is deployed and functioning.
- Microsoft Active Directory is installed, and the integration for each application is understood.
- The Call Control chapter of this document is understood and implemented.
- The Conferencing chapter of this document is understood and the necessary components for scheduled conferencing are deployed.
- Sizing and licensing for the conferencing solution is understood.

List of Core Applications

The core applications of the Preferred Architecture included these elements:

- Cisco Unity Connection to provide unified messaging (See the section on Unified Messaging with Cisco Unity Connection.)
- Cisco TelePresence Management Suite to provide Collaboration Meeting Room (CMR) provisioning and conference scheduling (See the section on Conference Scheduling with Cisco TelePresence Management Suite (TMS).)

List of Tools Used in a Collaboration Deployment

These software tools are useful to administrators in deploying the Enterprise Collaboration Preferred Architecture:

- Cisco Prime License Manager (PLM)
- Cisco Prime Collaboration Deployment (PCD)

Key Benefits

- Unified messaging available on multiple end-user platforms
- Creation and provisioning for individual end-user Collaboration Meeting Rooms (CMRs)
- Conference scheduling and One Button to Push feature deployment
- Eases deployment of new infrastructure components
- A single tool to manage licenses for various products

Unified Messaging with Cisco Unity Connection

Cisco Unity Connection enables unified messaging for the Cisco Preferred Architecture for Enterprise Collaboration. This section provides the information and instructions for deploying Unity Connection for voice messaging and unified messaging along with features such as single inbox and visual voicemail. This section also covers networking between two Unity Connection clusters.

Core Components

The core architecture contains these elements:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unity Connection
- Microsoft Exchange

Key Benefits

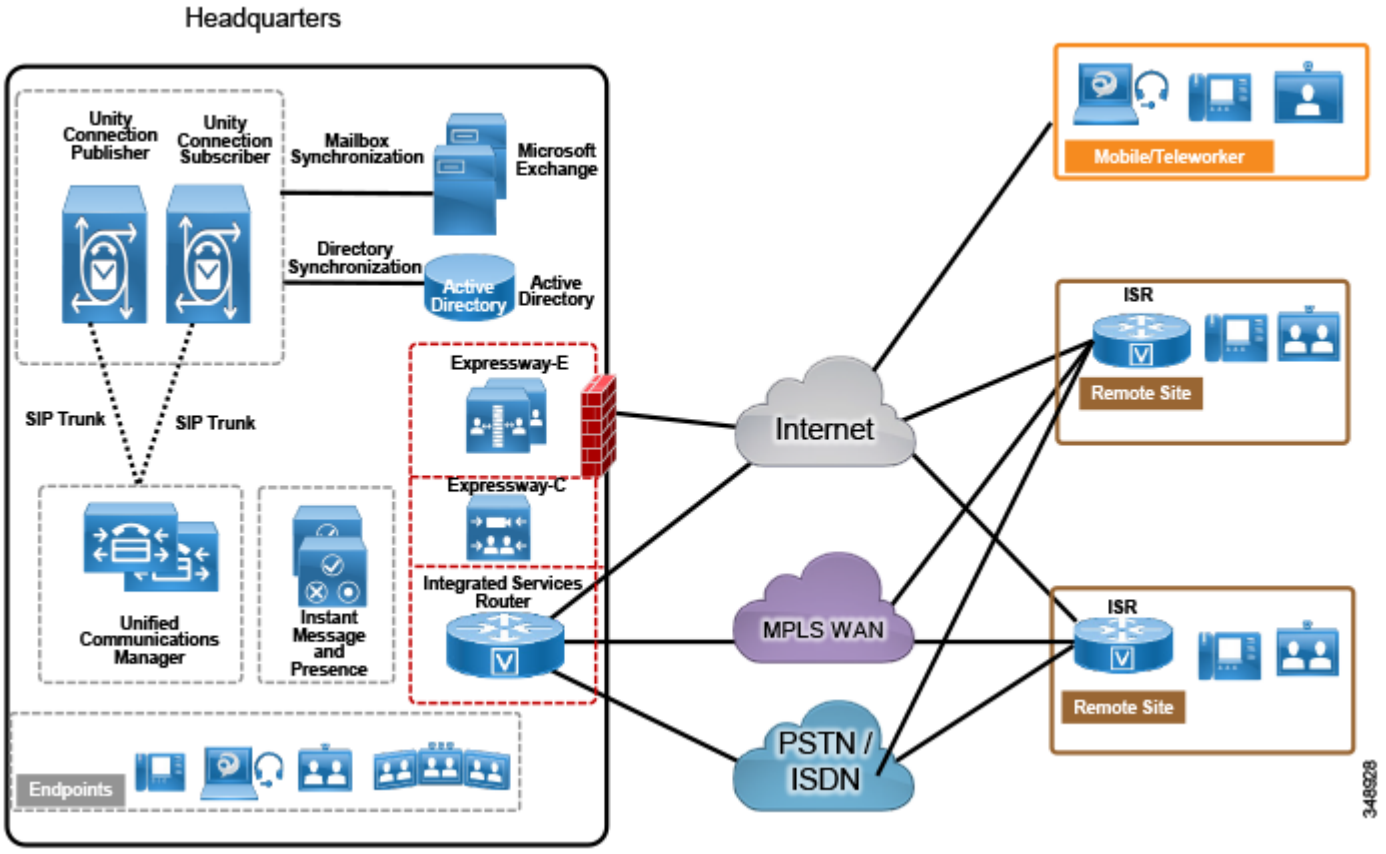
- Users can access the voicemail system and retrieve their voice messages by using:
  - Cisco Unified IP Phones, TelePresence endpoints, Jabber, and mobile devices
  - Web interface with PCs or Mac
  - Email client applications such as Microsoft Outlook
- Visual voicemail provides secure access to a visual display of voice messages on a Jabber client, listed with sender name, date, and message duration.

Core Architecture

Centralized Messaging and Centralized Call Processing

As shown in Figure 5-1, with centralized messaging Unity Connection is located in the same site as the Unified CM cluster. Remote branch sites located over the WAN from the central site rely on the centralized Unity Connection for unified messaging services. Unity Connection integrates with Unified CM using SIP for call control and RTP for the media path. Each Unity Connection cluster consists of two server nodes providing high availability and redundancy.

Figure 5-1 Architecture Overview



At the remote branch site, Cisco Unified Survivable Remote Site Telephony (SRST) is installed as a backup call agent, which is integrated with the central Unity Connection server. In the event of an IP WAN outage, all the phones at the remote branch register with SRST, which is preconfigured to send all the unanswered and busy calls to the central Unity Connection server via the PSTN.

Role of Unified CM

Unified CM provides call control capabilities and forwards calls to Unity Connection in the event that a called phone is either busy or unanswered. If a user presses the message button on the phone or dials the voicemail pilot number from an outside network, then Unified CM routes the call to Unity Connection.

Role of Unity Connection

In a centralized messaging deployment, Unity Connection provides users with the ability to store and retrieve voicemails. Typically calls forwarded to Unity Connection are direct calls or are due to a called extension that is either busy or unanswered. Message Waiting Indicator (MWI) is displayed on the endpoint for any new messages stored for the user. With each call, the following call information is typically passed between the phone system and Unity Connection:

- The extension of the called party
- The extension of the calling party (for internal calls) or the phone number of the calling party (if it is an external call and the phone system supports caller ID)
- The reason for the forward (the extension is busy, does not answer, or is set to forward all calls)

If the call is forwarded because the called party did not answer the call, Unity Connection plays the called user's standard greeting. If the call was forwarded because the called phone was busy, Unity Connection plays the called user's busy greeting.

Unity Connection handles direct calls differently than forwarded calls. When Unity Connection receives a call, it first attempts to determine whether the caller is a user. It does this by identifying whether the caller ID matches a user's primary or alternate extension. If Unity Connection finds a match, it assumes that a user is calling and it asks for that user's voicemail PIN. If Unity Connection determines that the caller ID is not associated with a user, then the call is sent to the opening greeting. An opening greeting is the main greeting that outside callers hear when they reach the Unity Connection auto-attendant.

Role of Microsoft Exchange

Unity Connection is integrated with Microsoft Exchange to enable the Single Inbox feature. Single Inbox in Unity Connection enables unified messaging and synchronizes voice messages between Unity Connection and Microsoft Exchange.This enables users to retrieve voicemail using their email client.

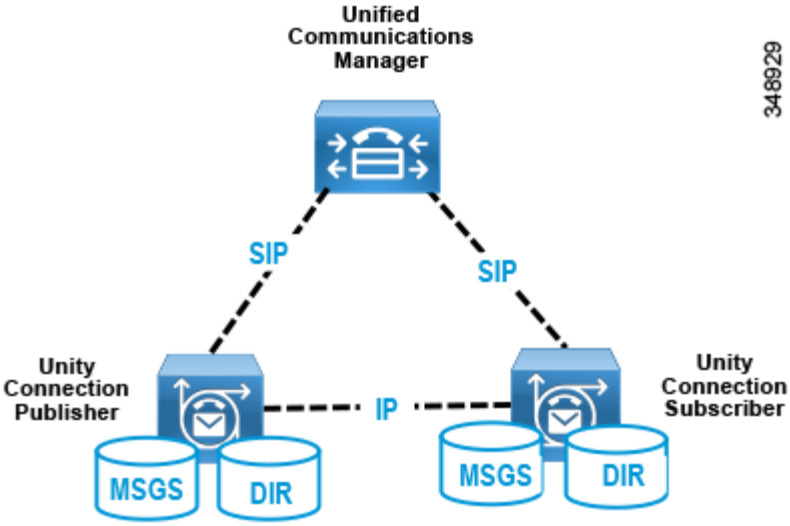
This chapter focuses on Unified Messaging with Microsoft Exchange. Unity Connection can also be integrated with IBM Lotus Sametime instant messaging application, allowing users to play their voice messages using Lotus Sametime. For more information on this topic, refer to the Unity Connection documentation available at

http://www.cisco.com/en/US/products/ps6509/index.html

High Availability for Unified Messaging

Figure 5-2 shows Unity Connection in an active/active pair, allowing the Unity Connection servers to be installed in the same or separate buildings to provide high availability and redundancy. Both servers in the active/active pair are running Unity Connection, both accept calls and HTTP requests, and both servers store user information and messages. In the event that only one server in the clustered pair is active, Unity Connection preserves the complete end-user functionality, including voice calls and HTTP requests. However, Unity Connection port capacity for calls will be reduced by half, to that of a single server.

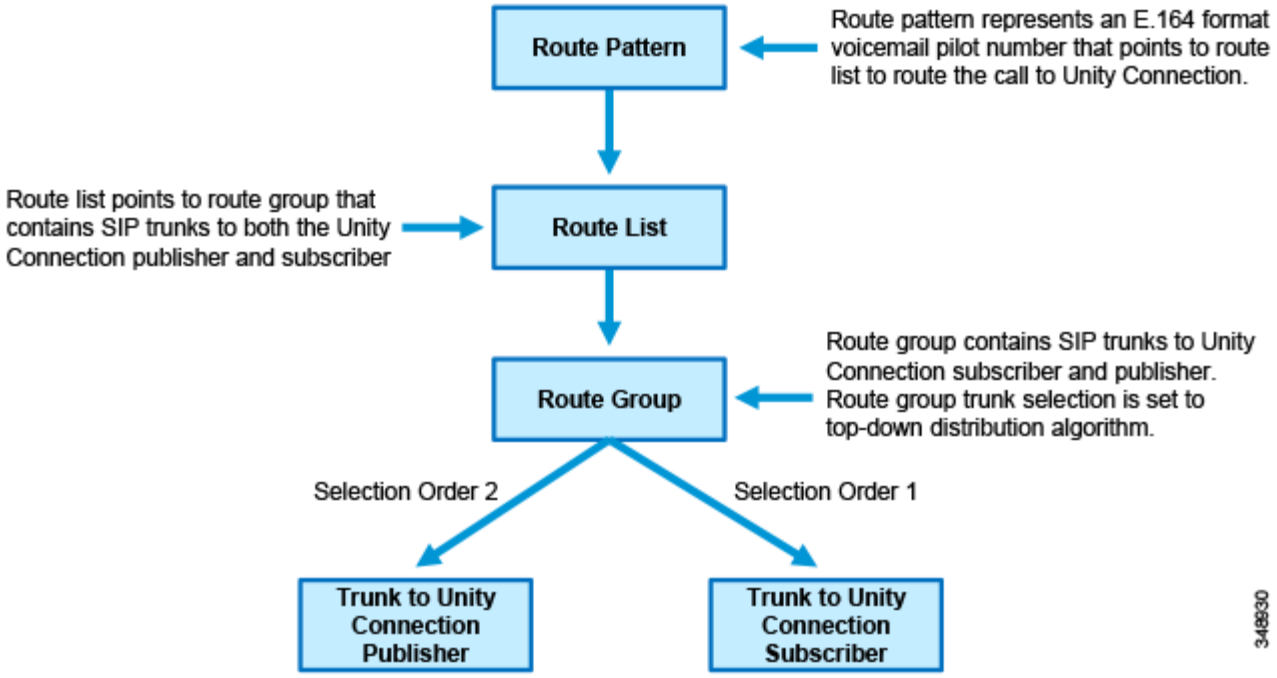
Figure 5-2 Unity Connection Cluster



All user client and administrator sessions (for example, IMAP and Cisco Personal Communications Assistant) and administration traffic (for example, Cisco Unity Connection Administration, the Bulk Administration Tool, and backup operations) connect to the Unity Connection publisher server. If the publisher server stops functioning, the user client and administrator sessions can connect to the Unity Connection subscriber server.

This topology requires two separate Unified CM SIP trunks pointing to each Unity Connection server node in the cluster. This configuration provides both high availability and redundancy. Unified CM should be configured to route all calls to the Unity Connection subscriber node first. If the subscriber server is unavailable or all the ports of the subscriber are busy, then calls are routed to the publisher node. Given the SIP integration between Unified CM and Unity Connection, trunk selection is achieved via Unified CM route pattern, route list, and route group constructs (see Figure 5-3). Both trunks are part of the same route group and assigned to the same route list, and the trunks within the route group are ordered using a top-down trunk distribution algorithm. This approach allows Unified CM to control the preference of the Unity Connection server node selection during both normal and failover operation.

Figure 5-3 Unity Connection SIP Trunk Selection



Unity Connection supports using Single Inbox with Microsoft Exchange 2010 or Exchange 2013 Database Availability Groups (DAGs) for high availability. The DAGs are deployed according to Microsoft recommendations. Unity Connection also supports connecting to a client access server (CAS) array for high availability. This section does not cover Microsoft Exchange high availability deployment. For more information about Exchange high availability deployments, refer to the Microsoft Exchange product information available at http://www.microsoft.com/.

Licensing Requirements

The licenses for Unity Connection are managed by the Cisco Prime License Manager (PLM). To use the licensed features on Unity Connection, the valid licenses for the features must be installed on the PLM server and Unity Connection must communicate with the PLM server to obtain the license. The PLM server provides centralized, simplified, and enterprise-wide management of user-based licensing.

Unified Messaging Requirements

- Unity Connection supports Microsoft Exchange 2003, 2007, 2010, and 2013 Server for Single Inbox. Unity Connection also supports interoperability with the Microsoft Business Productivity Online Suite (BPOS) Dedicated Services and Microsoft Office 365 cloud-based exchange server.
- Exchange servers and Active Directory domain controllers/global catalog servers (DC/GCs) can be installed in any hardware virtualization environment supported by Microsoft. Refer to Microsoft Exchange product information available at http://www.microsoft.com/ for more information about supported hardware platforms.
- The Microsoft Exchange message store can be stored in any storage area network configuration supported by Microsoft. Refer to Microsoft Exchange product information available at http://www.microsoft.com/ for more information about supported storage area network.
- For every 50 voice messaging ports on each server, 7 Mbps of bandwidth is required between Unity Connection and Microsoft Exchange for message synchronization.
- The default Unity Connection configuration is sufficient for a maximum of 2,000 users and 80 milliseconds of round-trip latency between Unity Connection and the Exchange servers. For more than 2,000 users and/or more than 80 milliseconds of latency, you can change the default configuration. For more information, see the information on latency in the *Design Guide for Cisco Unity Connection*, available at

  http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

Scaling Unity Connection

A Unity Connection cluster consists of a maximum of two nodes, one publisher and one subscriber in an active/active deployment. Under normal operation, call processing load balancing does not occur in an active/active deployment. Unified CM is configured to route all calls to the Unity Connection subscriber server first. If all ports are busy or if the subscriber server is unavailable, then calls are routed to the publisher. When sizing Unity Connection, consider the following parameters:

- Total number of current and future users.
- Required Voice messaging storage capacity.
- Number of voicemail ports supported with each platform.

For more information on Unity Connection scaling, see the Sizing chapter.

Cisco Unity Connection Deployment Process

Prerequisites

Before deploying the unified messaging architecture, ensure that:

- Unified CM is installed and configured for call control (see the Call Control chapter).
- Microsoft Exchange is installed and configured as an email server. For more information about supported exchange versions, refer to the section on Unified Messaging Requirements.

Deployment Overview

For the purposes of this Preferred Architecture, we assume a centralized messaging deployment model serving three sites in the US: SJC, RCD, and RTP. The deployment of centralized messaging starts with the Unity Connection cluster installation followed by further provisioning and configuration. To deploy centralized unified messaging with Cisco Unity Connection, perform the following tasks in the order listed here:

1. Provision the Unity Connection Cluster
2. Configure Unified CM for Unity Connection Integration
3. Unity Connection Base Configuration
4. Enable Single Inbox
5. Enable Visual Voicemail
6. Voice Mail in SRST Mode
7. HTTPS Internetworking of Two Unity Connection Clusters

Note Only non-default and other configuration field values are specified in this document. If a field configuration value is not mentioned, then the default value should be assumed.

1. Provision the Unity Connection Cluster

When clustering Unity Connection server nodes, one server is designated as the publisher server in the server pair while the other server is designated as the subscriber server.

Publisher

In Unity Connection only two servers are supported in a cluster for active/active high availability. The publisher server is the first to be installed, and it publishes the database and message store, replicating this information to the other subscriber server in the cluster.

Subscriber

Once the software is installed, the subscriber server node subscribes to the publisher to obtain a copy of the database and message store.

Unity Connection Mailbox Stores

During installation, Unity Connection automatically creates:

- A directory database for system configuration information (user data, templates, classes of service, and so forth).
- A mailbox store database for information on voice messages (who each message was sent to, when it was sent, the location of the WAV file on the hard disk, and so forth).
- An operating system directory for voice message WAV files.

Prerequisite for Unity Connection Cluster Deployment When the Servers Are to Be Installed in the Same Building

- For inbound and outbound calls to Unity Connection, the TCP and UDP ports of the firewall must be open as listed in the chapter on *IP Communications Required by Cisco Unity Connection* in the *Security Guide for Cisco Unity Connection*.
- For a cluster with two virtual machines, both must have the same virtual platform overlay.
- The servers must not be separated by a firewall.
- Both Unity Connection servers must be in the same time zone.
- Both Unity Connection server nodes must integrate to the same phone system.
- Both Unity Connection servers must have the same enabled features and configurations.

Prerequisite for Unity Connection Cluster Deployment When the Servers Are to Be Installed in Separate Buildings

- For inbound and outbound calls to Unity Connection, the TCP and UDP ports of the firewall must be open as listed in the chapter on *IP Communications Required by Cisco Unity Connection* in the *Security Guide for Cisco Unity Connection*.
- For a cluster with two virtual machines, both must have the same virtual platform overlay.
- Both Unity Connection server nodes must integrate to the same phone system.
- Both Unity Connection servers must have the same enabled features and configurations.
- Depending on the number of voice messaging ports on each Unity Connection server node, the connectivity between the server nodes must have the following guaranteed bandwidth with no steady-state congestion:
  - For every 50 voice messaging ports on each server, 7 Mbps of bandwidth is required.
  - Maximum round-trip latency must be no more than 150 milliseconds (ms).

To Deploy Unity Connection Cluster

- Determine which VMware Open Virtual Archive (OVA) template you want to deploy for the Unity Connection node based on the maximum number of ports and the maximum number of users. Refer the section on Scaling Unity Connection.
- Add both the Unity Connection nodes as host A records in the enterprise domain name service (DNS) server. For example, set the publisher Unity Connection hostname as US-CUC1.ent-pa.com and the subscriber hostname as US-CUC2.ent-pa.com.
- Determine the network parameters required for the installation:
  - Time zone for the server
  - Host name, IP address, network mask, and default gateway. Ensure that the hostname and IP address match the previous DNS configuration.
  - DNS IP addresses
  - Network Time Protocol (NTP) server IP addresses
- Download the above noted OVA file from the Cisco website.
- Deploy the Unity Connection publisher server node using the VMware vSphere Client.
- After installing the Unity Connection publisher, add the subscriber details in the cluster configuration of the primary server.
- Deploy the Unity Connection subscriber server node using the VMware vSphere Client.

2. Configure Unified CM for Unity Connection Integration

Before Unity Connection communicates with Unified CM, certain tasks must be performed on Unified CM. Unity Connection communicates to Unified CM over a SIP trunk. This section provides an overview of the tasks required to integrate Unified CM with Unity Connection.

SIP Trunk Security Profile

As far as media and signaling encryption is concerned, this guide assumes they are not used and instead non-secure SIP trunks are implemented between Unified CM and Unity Connection server nodes. Create a new SIP Trunk Security Profile for Unity Connection with device security mode set to **Non Secure**. Table 5-2 lists the SIP trunk security profile settings.

Table 5-2 SIP Trunk Security Profile Settings

Parameter	Value	Comments
Name	Unity Connection SIP Trunk Security Profile	Enter the name of the security profile.
Description	Unity Connection SIP Trunk Security Profile	Enter the description for profile.
Device Security Mode	Non Secure	Security mode for SIP trunk.
Accept out-of-dialog refer	Checked	Ensures that Unified CM accepts incoming non-INVITE, out-of-dialog refer messages that come via the SIP trunk.
Accept unsolicited notification	Checked	Ensures that Unified CM accepts incoming non-INVITE, unsolicited notification messages that come via the SIP trunk. This parameter must be checked to accept MWI messages from Unity Connection.
Accept replaces header	Checked	Ensures that Unified CM accepts new SIP dialogs, which replace existing SIP dialogs. This allows "REFER w/replaces" to be passed, which is used for Cisco Unity Connection initiated supervised transfers.

SIP Profile

Configure a SIP profile for the SIP trunk to Unity Connection. Copy the standard SIP profile and rename it to **Unity Connection SIP Profile**. Select the checkbox **Use Fully Qualified Domain Name in SIP Requests** to prevent the IP address of the Unified CM server from showing up in SIP calling party information sent by Unified CM. Ensure that the checkbox **Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"** is checked so that the system tracks the status of connectivity to the Unity Connection node.

When the OPTIONS Ping is enabled, each node running the trunk's SIP daemon will periodically send an OPTIONS Request to each of the trunk's destination IP addresses to determine its reachability and will send calls only to reachable nodes. A destination address is considered to be "out of service" if it fails to respond to an OPTIONS Request, if it sends a Service Unavailable (503) response or Request Timeout (408) response, or if a TCP connection cannot be established. The overall trunk state is considered to be "in service" when at least one node receives a response (other than a 408 or 503) from a least one destination address. SIP trunk nodes can send OPTIONS Requests to the trunk's configured

destination IP addresses or to the resolved IP addresses of the trunk's DNS SRV entry. Enabling SIP OPTIONS Ping is recommended for all SIP trunks because it allows Unified CM to track the trunk state dynamically rather than determining trunk destination state on a per-node, per-call, and time-out basis.

SIP Trunk

Create two separate SIP trunks, one for each Unity Connection server node in the cluster. Table 5-3 lists the SIP trunk settings.

Table 5-3 Parameter Settings for SIP Trunk to Unity Connection Server

Parameter	Value	Description
Name	US_CUC1_SIP_Trunk	Enter the unique name for SIP trunk to Unity Connection.
Description	Unity Connection Publisher	Enter the description for the SIP trunk.
Device Pool	Trunks_and_Apps	Enter the device pool for Unity Connection. (See the Call Control chapter.)
Run On All Active Unified CM Nodes	Checked	This ensures that outbound calls using the SIP trunk do not require intra-cluster control signaling between Unified CM call processing subscribers.
Call Routing Information – Inbound Calls		
Calling Search Space (CSS)	VoiceMail (Refer to the Call Control chapter for more about CSS configuration.)	CSS assigned contains all the on-net destinations such as DIDs, non-DID numbers, and URI partitions. If the CSS does not include all these partitions, then the MWI Unsolicited Notify messages from Unity Connection will not reach user phones.
Redirecting Diversion Header Delivery - Inbound	Checked	This ensures that the redirecting Information Element, the first redirecting number, and the call forward reason are sent and accepted as a part of incoming messages. Unity Connection uses the first redirecting number to answer the call.
Call Routing Information – Outbound Calls		
Calling and Connected Party Info Format	Deliver URI and DN in connected party, if available	This option determines whether Unified CM inserts a directory number, a directory URI, or a blended address that includes both the directory number and directory URI, in the SIP identity headers for outgoing SIP messages.
Redirecting Diversion Header Delivery - Outbound	Checked	This ensures that the redirecting Information Element, the first redirecting number, and the call forward reason are sent and accepted as a part of outgoing messages. Unity Connection uses the first redirecting number to answer the call.
SIP Destination Information		
Destination Address	10.195.100.20	Enter the IP address of Unity Connection server.

Table 5-3 Parameter Settings for SIP Trunk to Unity Connection Server (continued)

Parameter	Value	Description
SIP Trunk Security Profile	Unity Connection SIP Trunk Security Profile	See Table 5-2.
SIP Profile	Unity Connection SIP Profile	See the SIP Profile section.

Route Group

Create a separate route group RG_CUC for the Unity Connection cluster. The route group contains the SIP trunks to the Unity Connection subscriber and publisher nodes. Ensure that the SIP trunk that connects to the subscriber node (US_CUC2_SIP_Trunk) appears first in the list, followed by the publisher node (US_CUC1_SIP_Trunk). The route group distribution algorithm should be set to the **Top Down** trunk selection method. A route group configured with the **Top Down** distribution algorithm ensures that the calls are always sent to the Unity Connection subscriber server node (US-CUC2) first. If the Unity Connection subscriber server node is busy or unavailable, then the calls are sent to the publisher server node (US-CUC1).

Route List

Create a separate route list RL_CUC for the Unity Connection cluster. The route list should contain only the Unity Connection route group (RG_CUC) created previously. Ensure that the options **Enable this Route List** and **Run on all Active Unified CM Nodes** are selected.

Route Pattern

Create a separate route pattern for the voicemail pilot number pointing to the Unity Connection route list created above. This number must match the voicemail pilot number. Table 5-4 shows the route pattern configuration example.

Table 5-4 Unity Connection Pilot Number-Route Pattern Example

Parameter	Value
Route Pattern	+14085554999
Route Partition	DN
Gateway/Route List	RL_CUC
Call Classification	OnNet
Provide Outside Dial Tone	Unchecked

Voice Mail Pilot

The voicemail pilot number designates the directory number that users dial to access voice messages. Unified CM automatically dials the voicemail pilot number when a user presses the Messages button on an IP endpoint. A single voicemail pilot number is created for all three sites. Table 5-5 shows the voicemail pilot configuration example.

Table 5-5 Voicemail Pilot Example

Parameter	Value
Voice Mail Pilot number	+14085554999
Calling Search Space	DN
Description	VM Pilot
Make this the default Voice Mail Pilot for the system	Checked

Voicemail users located at remote sites can check their messages from the PSTN by dialing the voicemail access number from their own DID range. A separate translation pattern is created to translate the voicemail PSTN access number to the voicemail pilot number. Table 6 shows the translation pattern configuration for the voicemail pilot.

Table 5-6 Voicemail Pilot Translation Pattern Example

Parameter	Value
Translation Pattern	+19195551999
Partition	DN
Use Originators Calling Search Space	Checked
Route Option	Route this pattern
Called Party Transformations	
Called Party Transform Mask	+14085554999

Additional translation patterns would be created for other remote sites.

Voicemail Profile

A voicemail profile is assigned to each user's phone line on all endpoint devices and Extension Mobility profiles. The profile enables users to press the Messages button on an endpoint for one-touch access to the voicemail system. If Unity Connection is integrated with a single phone system, we recommend using the default voicemail profile. During the initial provisioning of a line on an endpoint device, the default voicemail profile (None) is assigned to the directory number. For the users who do not require voicemail access, no voicemail profile is assigned to their endpoint lines. Table 5-7 shows the settings for the voicemail profile configuration example.

Table 5-7 Voicemail Profile Example

Parameter	Value
Voice Mail Profile Name	Default
Description	VM Profile
Voice Mail Pilot	+14085554999/DN
Voice Mail Mask	Blank
Make this the default Voice Mail Profile for the System	Checked

3. Unity Connection Base Configuration

Service Activation

- After Unity Connection installation is complete, login to Cisco Unified Serviceability and activate the **DirSync** service on the publisher server node.
- Under Unified Serviceability, **Navigate** to **Tools –> Control Centre-Feature Services**. Verify that the Cisco DirSync service is started on publisher server node.
- Under Unity Connection Serviceability, **Navigate** to **Tools –> Service Management**. Verify the status of services on the primary and secondary Unity Connection server nodes. Table 5-8 shows the services status for this deployment.

Table 5-8 Unity Connection Services Status

Services	Primary Unity Connection	Secondary Unity Connection
Status Only Services (Can be deactivated from OS command line interface)		
All the Services in this category	Yes	Yes
Critical Services		
Connection Conversation Manager	Yes	Yes
Connection Mailbox Sync	Yes	No
Connection Message Transfer Agent	Yes	No
Connection Mixer	Yes	Yes
Connection Notifier	Yes	No
Base Services		
All the Services in this category	Yes	Yes
Optional Services		
Connection Branch Sync Service	No	No
Connection Digital Networking Replication Agent	No	No
All other remaining services in this category	Yes	Yes

Database Replication

After activating services on both primary and secondary Unity Connection server nodes, confirm that the subscriber node can connect to the publisher node. Also check the database replication status using the OS Command line interface (CLI) command **show perf query class "Number of Replicates Created and State of Replication"** on both the nodes

Unified CM Integration

Each Unity Connection cluster is integrated with the co-located Unified CM cluster. This provides a simple integration model with each Unity Connection cluster dedicated to a Unified CM cluster. While SIP trunks are configured on the Unified CM for interconnectivity into the Unity Connection cluster, voicemail ports are used for capacity and licensing purposes on the Unity Connection system. This section discusses design considerations, capacity planning, and configuration settings of the voicemail ports.

Voicemail Port Audio Codec Configuration

In Unity Connection, a call in any audio codec format that is supported by Unity Connection SIP signaling (G.711 mu-law, G.711 a-law, G.722, G.729, and iLBC) will always be transcoded to PCM linear. From PCM linear, the recording is encoded in the system-level recording audio codec (PCM linear, G.711 mu-law, G.711 a-law, G.729a, or G.726-a) system-wide setting in Unity Connection Administration. G.711 mu-law is the default.

In this section, we refer to the audio codec that is negotiated between the calling device and Unity Connection as the *line codec*, and the audio codec that is set as the system-level recording audio codec as the *recording codec*.

Supported line codecs (advertised codecs):

- G.711 mu-law
- G.711 a-law
- G.722
- G.729
- iLBC

Supported recording codecs (system-level recording audio codecs):

- PCM linear
- G.711 mu-law (default)
- G.711 a-law
- G.729a
- G.726
- GSM 6.10

Because transcoding is inherent in every connection, there is little difference in system impact when the line codec differs from the recording codec. For example, using G.729a as the line codec and G.711 mu-law as the recording codec does not place a significant additional load on the Unity Connection server for transcoding. However, the iLBC or G.722 codecs require more computation to transcode, and therefore they place a significant additional load on the Unity Connection server. Consequently, a Unity Connection server can support only half as many G.722 or iLBC connections as it can G.711 mu-law connections.

For this example topology, the system recording codec is left at default (G.711 mu-law). The supported line codes are set to G.729 and G.711 mu-law. Using this default configuration, the users located at the same site of Unity Connection will use G711 mu-law. For the users located over the WAN from the centralized Unity Connection servers, the selected line codec will be G.729.

Use of the G.722 or iLBC codec as line codecs or advertised codecs reduces the number of voice ports that can be provisioned on the Cisco Unity Connection server. For more information on the number of voice ports supported for each platform overlay when using G.722 or iLBC codecs, refer to the documentation on Virtualization for Cisco Unity Connection.

Phone System Settings

Phone system integration enables communication between Unity Connection and Unified CM. We recommend using default **PhoneSystem** if Unity Connection is integrated with single Unified CM cluster. Table 5-9 shows the Phone System settings.

Table 5-9 Phone System Settings

Parameter	Value	Description
Phone System Name	PhoneSystem	PhoneSystem
Default TRAP Phone System	Checked	Phone system enables TRAP connections so that administrators and users without voicemail boxes can record and playback through the phone in Unity Connection web applications.
Call Loop Detection by Using Extension		
Enable for Forwarded Message Notification Calls (by Using Extension)	Checked	Unity Connection uses the extension to detect and reject new-message notifications that are sent to a device (such as a mobile phone) and that the device forwards back to Unity Connection because the device did not answer. If the call loop is not detected and rejected, the call creates a new voice message for the user and triggers Unity Connection to send a new-message notification call to the device.
Outgoing Call Restrictions		
Enable outgoing calls	Checked	Unity Connection places outgoing calls (for example, setting MWIs) as needed through the phone system.

Port Group Settings

A port group is used to control the SIP communications between the Unified CM and Unity Connection clusters. The port group allows the system to restrict and specify which Unified CM servers the Unity Connection server will accept SIP messages from, and the order and preference that the Unity Connection servers will use to route outbound calls to the Unified CM servers. The Unity Connection servers are configured to mirror the Unified CM SIP routing design for Unity Connection, hence outbound routing should be configured on Unity Connection servers to prefer the first available Unified CM subscriber node. Table 5-10 provides the port group settings.

Table 5-10 Port Group Settings

Parameter	Value	Description
Display Name	PhoneSystem-1	Descriptive name for the Phone System
Integration Method	SIP	The method of integration that is used to connect Unity Connection and Unified CM
Session Initiation Protocol (SIP) Settings		
Register with SIP Server	Checked	This ensures that Cisco Unity Connection is registered with the SIP server.
SIP Servers		

Table 5-10 Port Group Settings (continued)

Parameter	Value	Description
Order 0	10.195.100.21	The SIP server configured for Order 0 will have higher preference. Enter the IP address of the primary Unified CM call processing node.
Order 1	10.195.100.20	The SIP server configured for Order 1 will have lower preference. Enter the IP address of the secondary Unified CM call processing node.
Port	5060	Enter the TCP port of the Unified CM server that Unity Connection uses.

Voice Messaging Port Sizing Considerations

Each Unity Connection server in a cluster must have voice messaging ports designated for the following dial-in function in case either server has an outage:

- Answer Calls

Further, each Unity Connection server must have voice messaging ports designated for the following dial-out functions:

- Sending message waiting indications (MWIs)
- Performing message notifications
- Allowing telephone record and playback (TRAP) connections

We recommend reserving 20% of the total number of voicemail ports on the system for message notification, dial out MWI, and TRAP to reduce the possibility of call blocking on the ports for answering calls versus ports dialing out.

Alternatively, the answer and dial-out port selection can be done using previous voicemail traffic reports. Use the Port Usage Analyzer Tool to collect traffic for the last one or two weeks, then make adjustments based on actual port traffic.

Port Settings

As discussed in the previous section, ports will be either incoming or outgoing ports. Table 5-11 shows a voicemail port allocation configuration example, and Table 5-12 provides the configuration template for answer port configuration.

Table 5-11 Voicemail Port Allocation Configuration Example

CUC Server	Port Range	Function
US-CUC1	1-80	Answer
US-CUC2	1-80	Answer
US-CUC1	81-100	Dial-Out
US-CUC2	81-100	Dial-Out

Table 5-12 Voicemail Answer Port Configuration Example

Parameter	Value	Description
Enabled	Checked	Check the box to enable the phone system port.
Phone System Port		
Port Name	Auto Created	Unity Connection Automatically creates the port name.
Phone System	PhoneSystem	Choose the appropriate Phone System.
Port Group	PhoneSystem-1	Choose the appropriate Port Group.
Server	US-CUC2/US-CUC1	Choose the Cisco Unity Connection (CUC) subscriber node first, and similarly add ports for the CUC publisher node.
Phone behavior		
Answer Call	Checked	This setting designates the port for answering the call.
Perform Message Notification	Unchecked	This setting designates the port for notifying users of messages.
Send MWI Requests	Unchecked	This setting designates the port for sending MWI on and off requests.
Allow TRAP Connections	Unchecked	This setting designates the port for Telephony Recording and Playback (TRAP) connections.

The configuration shown in the Table 5-12 should also be used to create voicemail dial out ports. However, in the case of dial out ports, uncheck the Answer Call parameter and check the Perform Message Notification, Send MWI Requests, and Allow TRAP Connection parameters instead.

Active Directory Integration

Unity Connection supports Microsoft Active Directory synchronization and authentication for Unity Connection web applications, such as Cisco Personal Communications Assistant (PCA) for end users, that rely on authentication against Active Directory. Likewise IMAP email applications that are used to access Unity Connection voice messages are authenticated against the Active Directory. For telephone user interface or voice user interface access to Unity Connection voice messages, numeric passwords (PINs) are still authenticated against the Unity Connection database.

The administrator account must be created in the Active Directory that Unity Connection will use to access the sub-tree specified in the user search base. We recommend using an account dedicated to Unity Connection, with minimum permissions set to "read" all user objects in the search base and with a password set to never expire.

Ensure that the Unified CM Mail ID field is synchronized with the Active Directory mail field. During the integration process, this causes values in the LDAP mail field to appear in the Corporate Email Address field in Unity Connection. Unity Connection uses Corporate Email Address in the Unified Messaging account to enable Single Inbox.

Unity Connection integrates with Active Directory to enable importing of user information. Integrating Unity Connection with an Active Directory provides several benefits:

- User creation — Unity Connection users are created by importing data from the Active Directory.
- Data synchronization — Unity Connection is configured to automatically synchronize user data in the Unity Connection database with data in the Active Directory.
- Single sign-on — Configure Unity Connection to authenticate user names and passwords for Unity Connection web applications against the Active Directory, so that users do not have to maintain multiple application passwords.

Refer the Call Control chapter for Active Directory settings.

Unity Connection Partitions and CSS

All the users for this deployment are configured in the default calling search space (US-CUC1 Search Space), which contains the default partition (US-CUC1 partition).

Restriction Tables

Unity Connection uses restriction tables to prevent the voicemail system from calling unauthorized telephone numbers. These rules are normally configured to explicitly match either allowed or blocked numbers. For this deployment, the Unity Connection system is not using restriction rules for call blocking from the voicemail system but instead is using the SIP trunk incoming calling search space (CSS) to prevent unauthorized calling from Unity Connection.The SIP trunk CSS is set to allow Unity Connection to dial only on-net destinations. Table 5-13 lists the Default Transfer restriction table settings.

Table 5-13 Restriction Table in Unity Connection

Order	Blocked	Pattern
0	Uncheck the check box	+*
1	Uncheck the check box	9+*
2	Uncheck the check box	91???????*
3	Uncheck the check box	9011???????*
4	Uncheck the check box	9???????????*
5	Uncheck the check box	900
6	Uncheck the check box	*

Unity Connection contains four additional restriction tables for Default Fax, Default Outdial, Default System Transfer, and User-defined and Automatically-Added Alternate Extensions. These restriction tables can also be disabled using the settings mentioned in Table 5-13.

Class of Service

Class of service (CoS) defines limits and features for users of Unity Connection voice mail. Class of service is typically defined in a User Template, which is then applied to the user's account when it is created. For this deployment, the default Voice Mail User COS is associated with all users.

User Provisioning

Import the users into Unity Connection by using the user template from the Active Directory server. The user template contains settings that are common to a group of users. Users inherit the common settings from the user template when their account is created. Separate user templates should be created for each site in the local time zone. Table 5-14 provides the user template settings.

Table 5-14 Voicemail User Template

Section	Field	Value
Basics	Alias	SJC_User_Template
	Display Name	SJC_User_Template
	Display Name Generation	First name, then last name
	Phone System	PhoneSystem
	Class of Service	Voice Mail User COS
	Set for Self-enrollment at Next Login	Checked
	List in Directory	Checked
	Time Zone	(GMT-8:00) America/Los_Angeles
	Language	English(United States)
	Generate SMTP Proxy Address from the Corporate Email Address	Checked
Password Settings - VM	User Must Change at Next Sign-In	Checked
	Does Not Expire	Checked
	Authentication Rule	Recommended Voice Mail Authentication Rule
Change Password-Voicemail	PIN	30071982

Basing new user settings on a template minimizes the number of settings to be modified on individual user accounts, making the job of adding users quicker and less prone to error.

Note that any subsequent user template changes (after the creation of user accounts using the template) are not applied to existing user accounts; that is, the common settings are picked up from the template at user account creation time only. An individual user's settings can be changed after the template has been used to create a Unity Connection account without affecting the template or other users.

The web application password should not be changed here because Unity Connection is integrated with LDAP and user authenticates from Active Directory. You have to give these PINs and passwords to users so that they can sign in to the Unity Connection system telephone user interface (TUI) and to the Cisco Personal Communications Assistant (PCA).

Select the options **Allow Users to Use the Messaging Assistant** and **Allow Users to Use the Web Inbox and RSS Feeds** under **Voice Mail User COS class of Service** to allow users to access their web inbox using Cisco PCA.

Import the users from LDAP using the template created above.

Unity Connection User Self Enrollment

End users must enroll as Unity Connection users. The Unity Connection administrator should provide an ID (usually the user's desk phone extension) and a temporary PIN (set during User Provisioning) for each user. The first-time enrollment conversation is a set of prerecorded prompts that guide users to do the following tasks:

- Record user name.
- Record a greeting that outside callers hear when the user does not answer the phone.
- Change user PIN.
- Choose whether to be listed in the directory. (When the user is listed in the directory, callers who do not know the user's extension can reach the user by spelling or saying user's name.)

Unity Connection users can dial the voicemail pilot number from an IP endpoint within the organization or from the outside network for the self-enrollment process. If the user is calling from an extension number that is unknown to Unity Connection, either from within your organization or from outside, the user must press * (star key) when Unity Connection answers to continue the self-enrollment process. If the user hangs up before enrollment finishes, the first-time enrollment conversation plays again the next time the user signs in to Unity Connection.

4. Enable Single Inbox

Single Inbox, one of the unified messaging features in Unity Connection, synchronizes voice messages in Unity Connection and Microsoft Exchange mailboxes. When a user is enabled for a Single Inbox, all Unity Connection voice messages that are sent to the user, including those sent from Unity Connection ViewMail for Microsoft Outlook, are first stored in Unity Connection and immediately replicated to the user's Exchange mailbox. This section explains configuration tasks required for integrating Unity Connection with Microsoft Exchange 2013 and 2010 to enable Single Inbox.

Perquisites for Enabling Single Inbox with Unity Connection

- Before enabling the Single Inbox feature, ensure that Microsoft Exchange is configured and users can send and receive emails.
- Microsoft Active Directory is required for Unified Messaging service account authentication.
- Unity Connection users are imported and configured for basic voice messaging. See the section on User Provisioning.

Unity Connection Certificate Management

When you install Cisco Unity Connection, local self-signed certificates are automatically created and installed to secure communication between Cisco PCA and Unity Connection, and between IMAP email clients and Unity Connection. This means that all the network traffic (including usernames, passwords, other text data, and voice messages) between Cisco PCA and Unity Connection is automatically encrypted, and the network traffic between IMAP email clients and Unity Connection is automatically encrypted, if you enable encryption in the IMAP clients.

The other option is to use the certificate issued by the certificate authority (CA).In this case self-signed certificates are replaced with certificates issued and signed by a trusted CA.For more information on this process, refer to the section on Cisco Unified CM and IM and Presence Certificate Management.

Confirm the Exchange Authentication and SSL Settings for Unity Connection

Confirm that the Exchange server is configured for the desired web-based authentication mode (Basic, Digest, or NT LAN Manager) and web-based protocol (HTTPS or HTTP).The authentication mode must match on both Exchange and Unity Connection for them to communicate.

If you select the option to validate certificates signed by an external CA for Exchange servers and Active Directory domain controllers, obtain and install the external CA signed certificate on both the Exchange and domain controller servers.

Configure SMTP Proxy Addresses in Unity Connection

When Single Inbox is configured, Unity Connection uses SMTP proxy addresses to map the sender of a message that is sent from Unity Connection ViewMail for Microsoft Outlook to the appropriate Unity Connection user, and to map recipients to Unity Connection users.

For example, suppose an email client is configured to access Unity Connection with the email address aross@ent-pa.com. This user records a voice message in ViewMail for Outlook and sends it to user ahall@ent-pa.com. Unity Connection then searches the list of SMTP proxy addresses for aross@ent-pa.com and ahall@ent-pa.com. If these addresses are defined as SMTP proxy addresses for the Unity Connection users ahall and aross respectively, Unity Connection delivers the message as a voice message from the Unity Connection user aross to the Unity Connection user ahall.

The SMTP proxy address for the user is automatically created when you import the users via the user template. In the user template, select the **Generate SMTP Proxy Address from the Corporate Email Address** option for creating the SMTP proxy address. Refer to the section on User Provisioning for more information.

Create Unified Messaging Services Account in Active Directory and Grant Permissions for Unity Connection

Single Inbox requires an Active Directory account (called the Unified Messaging Services account), and the account must have the rights necessary for Unity Connection to perform operations on behalf of users. Unity Connection accesses Exchange mailboxes using the Unified Messaging Services account. When creating the Unified Messaging Services account, follow these guidelines:

- Do not create an Exchange mailbox for the account.
- Do not add the account to any administrator group.
- Do not disable the account, otherwise Unity Connection cannot use it to access Exchange mailboxes

Sign in to a server on which the Exchange Management Shell is installed and assign the **ApplicationImpersonation Management** role to the Unified Messaging Services account for Unity Connection using following command:

new-ManagementRoleAssignment -Name: *RoleName* **-Role:ApplicationImpersonation -User:'** *Account* **'**

Where:

- *RoleName* is the name that you want to give the assignment; for example, Unity ConnectionUMServicesAcct. The name that you enter for RoleName appears when you run the command **get-ManagementRoleAssignment**.
- *Account* is the name of the Unified Messaging Services account in domain\alias format.

SMTP Smart Host

Unity Connection relays the message to the user email address using SMTP Smart Host. When a Unity Connection user receives a new message, Unity Connection can send a text notification to an email address. With this type of notification, you can configure Unity Connection to include a link to Cisco PCA in the body of the email message. Under the user configuration, navigate to the **Edit Notification Device** page for the user and select the option to **Include a Link to the Cisco Unity Connection Web Inbox in Message Text**. Table 5-15 lists the SMTP Smart Host configuration.

Table 5-15 SMTP Smart Host Details (System Settings > SMTP Configuration > Smart Host)

Parameter	Value
SmartHost	US-EXCH1.ent-pa.com

Unified Messaging Service

In Unity Connection Administration, expand **Unified Messaging**, then select **Unified Messaging Services**.

- Unified Messaging Services define the type of Microsoft Exchange and authentication method that Unity Connection will use to communicate with Microsoft Exchange.
- Configure Unified Messaging Services to communicate with a specific Exchange server using an FQDN.
- Configure the Unity Connection Unified Messaging Services for the same Web-based Authentication Mode (Basic, Digest, or NT LAN Manager) and Web-Based Protocol (HTTPS or HTTP) that is configured on Microsoft Exchange.
- Enter the Active Directory account credentials created in the section Create Unified Messaging Services Account in Active Directory and Grant Permissions for Unity Connection.
- Select the options to **Access Exchange Calendar and Contacts** and **Synchronize Connection and Exchange Mailboxes (Single Inbox)** to enable Unified Messaging features.
- Self-signed certificates cannot be validated. If you want the Unity Connection server to validate SSL certificates from Exchange, then use the public certificates from a certification authority (CA) instead of self-signed certificates. Refer to the section on Unity Connection Certificate Management for details.

Unified Messaging Account

In Unity Connection Administration, expand **Users** then select **Users**. On the Edit User Basics page, in the Edit menu, select **Unified Messaging Account**s.

- When you create a user account, Unity Connection does not automatically create a unified messaging account for that user. A unified messaging account can be created for one user or multiple users. Use the Bulk Administration Tool (BAT) to create the unified messaging account for large number of users.
- Unified messaging requires that you enter the Exchange email address for each Unity Connection user. On the Unified Messaging Account page, select **Use Corporate Email Address: None Specified** to cause Unity Connection to use the corporate email address specified on the Edit User Basics page as the Exchange email address.
- In the Active Directory integration, the Unified CM Mail ID field is synchronized with the Active Directory mail field. This causes values in the LDAP mail field to appear in the Corporate Email Address field in Unity Connection.

For more information on creating unified messaging accounts for multiple users with the Bulk Administration Tool, refer the information on creating unified messaging accounts in the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Voice Mail User COS

Edit the Voice Mail User Class of Service (**Class of Service –> Voice Mail User COS**) to enable the user for Single Inbox. In the **Licensed Features** select the option to **Allow Users to Access Voicemail Using an IMAP Client and/or Single Inbox**. Also select the option to **Allow IMAP Users to Access Message Bodies**.

Install ViewMail for Outlook on User Workstations

Cisco ViewMail for Microsoft Outlook provides a visual interface from which users can send, listen to, and manage their Unity Connection voice messages from within Outlook. Download ViewMail for Outlook from Cisco website, http://www.cisco.com, and install it on each user workstation. After installing ViewMail, open the ViewMail settings or Options tab and associate an email account with a Unity Connection server. Enter the user information and Unity Connection server details.

When using another email client to access Unity Connection voice messages in Exchange, or in cases when ViewMail for Outlook is not installed, note the following:

- The email client treats Unity Connection voice messages like emails with .wav file attachments.
- When a user replies to or forwards a Unity Connection voice message, the reply or forward is treated like an email, even if the user attaches a .wav file. Message routing is handled by Exchange, not by Unity Connection, so the message is never sent to the Unity Connection mailbox for the recipient.

5. Enable Visual Voicemail

Visual Voicemail provides access to Unity Connection directly from the voicemail tab on Jabber clients. Users can view a list of voice messages and play messages from Jabber. Users can also compose, reply to, forward, and delete voice messages.

Unity Connection Configuration

- Ensure that the Unity Connection users are imported and configured for basic voice messaging. Refer to the section on User Provisioning.
- Ensure that the Unity Connection **Connection Jetty** service and **Connection REST Service** are up and running. Both services are activated during Service Activation under the **Optional Services** category.
- Ensure that **Class of Service** is enabled for voicemail access from the IMAP client. Refer the section on Voice Mail User COS.
- Edit the Unity Connection Voice Mail Class of Service (CoS) to allow users to use web inboxes. Under the **Features** tab, select the option to **Allow Users to Use Unified Client to Access Voicemail**.
- Select the following options under the API settings (**System Settings** > **Advanced**):
  - Allow Access to Secure Message Recordings through CUMI
  - Display Message Header Information of Secure Messages through CUMI
  - Allow Message Attachments through CUMI

Unified CM Configuration

Add a **Voicemail** UC service for each Unity Connection server node. Table 5-16 shows the voicemail UC service configuration.

Table 5-16 Voicemail Service Settings (User Management > User Settings > UC Service)

Parameter	Value	Comments
Product Type	Unity Connection	Enter the product name of the voicemail system.
Name	us-cuc1	Enter the name of the voicemail service. Choose the display name that will help to distinguish between publisher and subscriber voicemail services.
Description	us-cuc1	Enter the display name that will help to distinguish between publisher and subscriber voicemail services.
Host Name/IP address	us-cuc1.ent.pa.com	Enter the address of the voicemail service in either IP address or FQDN format.
Port	443	Enter the port to connect with the voicemail service.
Protocol	HTTPS	Select the protocol to route voice messages securely.

Apply the **Voicemail** UC service created previously to the **Standard** Service Profile (**User Management –> User Settings –> Service Profile**). Ensure that the Voicemail UC service created for Unity Connection publisher (us-cuc1.ent.pa.com) is set to the primary profile and the Unity Connection subscriber (us-cuc2.ent.pa.com) is set to the secondary profile. To synchronize credentials for the voicemail service, select **Unified CM - IM and Presence** from the **Credentials source for voicemail service** drop-down list.

6. Voice Mail in SRST Mode

With the centralized messaging deployment model, during a WAN outage the branch site's Survivable Remote Site Telephony (SRST) routes the unanswered and busy calls to the central Unity Connection. Incoming calls that reach a busy signal, calls that are unanswered, and calls made by pressing the message button are forwarded to Unity Connection. This configuration allows phone message buttons to remain active. To enable this functionality, configure POTS dial peer access to Unity Connection through PRI.

However, when calls are routed over the PSTN, Redirected Dialed Number Information Service (RDNIS) can be affected. Incorrect RDNIS information can affect voicemail calls that are rerouted over the PSTN. If the RDNIS information is not correct, the call will not reach the voicemail box of the dialed user but will instead receive the automated attendant prompt, and the caller might be asked to reenter the extension number of the party they wish to reach. This behavior is primarily an issue when the telephone carrier is unable to ensure RDNIS across the network. There are numerous reasons why the carrier might not be able to ensure that RDNIS is properly sent. Check with your carrier to determine whether it provides guaranteed RDNIS delivery end-to-end for your circuits.

Unified CM Configuration

Ensure that the settings mentioned in Table 5-17 are enabled in Unified CM configuration for the SIP trunk to the central site PSTN gateway.

Table 5-17 Settings for the SIP Trunk to the PSTN gateway for Voicemail in SRST Mode

Parameter	Value	Comments
Call Routing Information – Inbound Calls		
Redirecting Diversion Header Delivery - Inbound	Checked	This ensures that the redirecting Information Element, the first redirecting number, and the call forward reason are sent and accepted as a part of incoming messages. Unity Connection uses the first redirecting number to answer the call.
Call Routing Information – Outbound Calls		
Redirecting Diversion Header Delivery - Outbound	Checked	This ensures that the redirecting Information Element, the first redirecting number, and the call forward reason are sent and accepted as a part of outgoing messages. Unity Connection uses the first redirecting number to answer the call

Branch SRST Router Configuration

Configure the following command on the branch site SRST router to enable voicemail access over PRI.

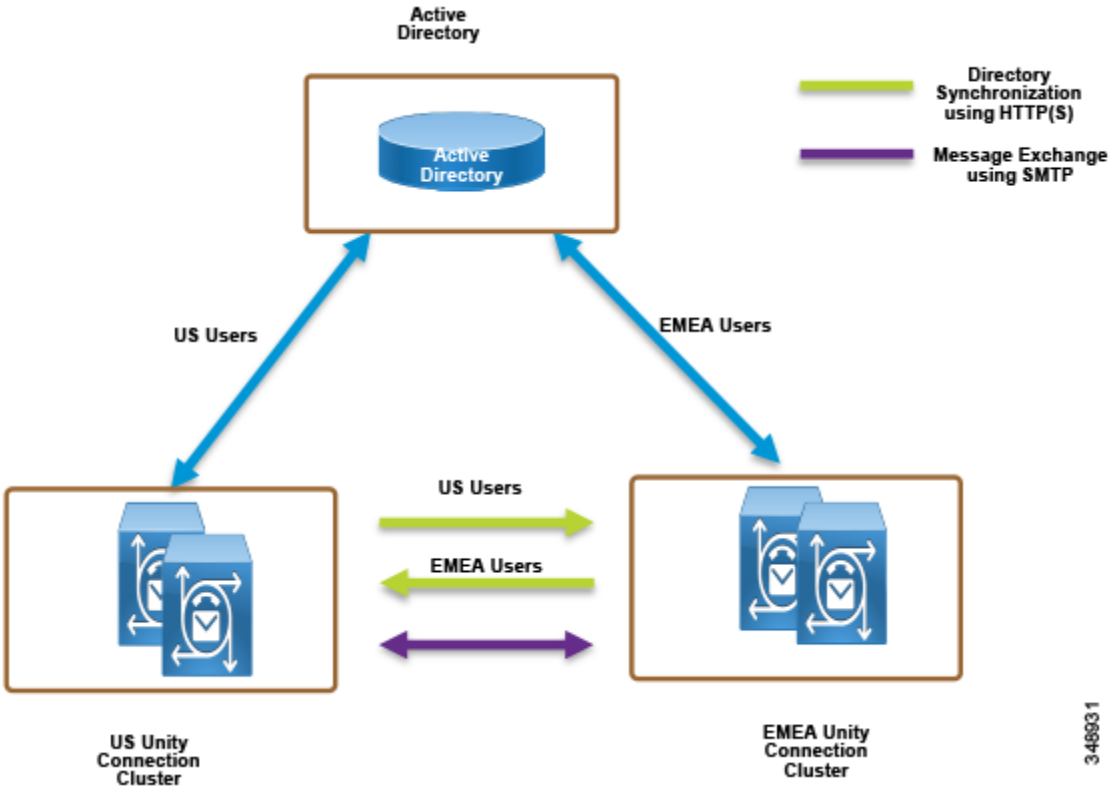
```
!
!
dial-peer voice 10 pots
destination-pattern +14085554999
direct-inward-dial
port 1/0:15
!
!
voice register pool 1
call-forward b2bua busy +14085554999
call-forward b2bua noan +14085554999 timeout 12
!
!
```

7. HTTPS Internetworking of Two Unity Connection Clusters

Figure 5-4 shows HTTPS internetworking of two Unity Connection clusters. HTTPS networking connects multiple Unity Connection clusters so that they can share directory information and exchange of voice messages. You can join two or more Unity Connection servers or clusters to form a well-connected network, referred to as a Unity Connection site. The servers that are joined to the sites are referred to as *locations*. Within a site, each location uses HTTPS protocol to exchange directory information and SMTP protocol to exchange voice messages with each other.

Within a site, Unity Connection locations automatically exchange directory information, so that a user in one location can dial out to or address messages to a user in any other system by name or extension, provided that the target user is reachable in the search scope of the originating user. The networked systems function as though they share a single directory.

Figure 5-4 HTTPS Internetworking of Two Unity Connection Clusters



In HTTPS networking, Unity Connection clusters are joined together using a hub-and-spoke topology. In this topology, all the directory information among the spokes is shared through the hub that connects the spokes. The number of Unity Connection locations that can be connected in an HTTPS network and the maximum number of users in HTTPS networking depend on the deployed OVA template. For more information on the maximum number of supported locations and maximum directory size, refer to the information on *directory object limits* in the *System Requirements for Cisco Unity Connection*.

In HTTPS networking, the directory replication is accomplished by means of a Feeder service and a Reader service running on each location in the network. The Reader service periodically polls the remote location for any directory changes since the last poll interval. The Feeder service checks the change tracking database for directory changes and responds to poll requests with the necessary information.

In the HTTPS networking, when the publisher server of a cluster location is up and running, it is responsible for the synchronization of directory information. However, if the publisher server is down, the subscriber server takes the role of synchronizing directory information.

Depending upon the server of a cluster (publisher or subscriber) with which the directory synchronization is being performed, the directory synchronization can be either of the following types:

- Standard — Specifies that the directory synchronization is done by the publisher server with the connected locations.
- Alert — Specifies that the publisher server is unreachable and the subscriber server is responsible for providing directory information to the connected locations. However, the subscriber server has the directory information stored that was last synchronized with the publisher server when it was running.

In the event of a publisher failure, directory synchronization occurs in the Alert mode. During the Alert mode, the connected nodes in the HTTPS network have limited access to directory synchronization with the subscriber. The limited access means that the connected nodes can fetch only the directory information that was last synchronized with the publisher when it was running. When the publisher comes up, the nodes that are directly connected to the publisher synchronize the updated directory information through the publisher. Therefore, the key benefit of the Alert mode is that the connected nodes remain synchronized with the subscriber server even when the publisher is down.

The clusters that are networked together are directly accessible through TCP/IP port 25 (SMTP).In addition, both locations must be able to route to each other via HTTP on port 8081 or HTTPS on port 8444.

For the purposes of this deployment documentation, we assume there is HTTPS networking between US and EMEA Unity Connection clusters. Table 5-18 shows the server node information of both clusters that are joined using HTTPS networking.

Table 5-18 Unity Connection Cluster Details for HTTPS Networking

	US Unity Connection Cluster		EMEA Unity Connection Cluster	
Server	**Hostname**	**IP address**	**Hostname**	**IP address**
Publisher	US-CUC1	10.195.100.30	EMEA-CUC1	10.195.99.30
Subscriber	US-CUC2	10.195.100.31	EMEA-CUC2	10.195.99.31

To set up HTTPS networking between two Unity Connection clusters, perform the following tasks described in this section.

Check the Display Name and SMTP Domain of Each Unity Connection Server

- The Unity Connection server that you join to an HTTPS network must have a unique display name and SMTP domain.
- Before enabling HTTPS networking, verify the display name and SMTP domain of the Unity Connection publisher server in the **Networking** –> **Locations** settings.

Create the HTTPS Network Between Unity Connection Clusters

- To create an HTTPS network of Unity Connection servers, start by linking two clusters together by creating an HTTPS link and then ensuring that the subscribers of each cluster are added for the SMTP Access.
- On each Unity Connection publisher, add a new HTTPS link. Table 5-19 shows the HTTPS Link settings.

Table 5-19 HTTPS Link Settings (Networking > HTTP(s) Links)

Parameter	Value	Comments
Link to Cisco Unity Connection Remote Location		
Publisher (IP address/FQDN/Hostname)	emea-cuc1.ent-pa.com	Enter the IP address, fully qualified domain name (FQDN), or hostname of the remote Unity Connection publisher node.
Username	Name of admin user	Enter the Username of an administrator at the location specified in the above publisher field. The administrator user account must be assigned the System Administrator role.
Password	Password of the admin user	Enter the password for the administrator specified in the Username field.
Transfer Protocol		
Use Secure Socket Layer (SSL)	Checked	This option enables SSL to encrypt directory synchronization traffic between the various HTTPS locations.
Accept Self-Signed Certificates	Check the check box only if a self-signed certificate is used	Check this check box to allow the local node in a network to use a self-signed certificate to negotiate SSL with this location. Uncheck this check box to require the local node in a network to use a certificate signed by a certificate authority (CA).

Configure SMTP Access for Cluster Subscriber Servers

In an HTTPS network that includes a Unity Connection cluster server pair, you can join only the publisher server of the pair to the network. In order for all locations in the network to communicate directly with the cluster subscriber server node when the subscriber is the primary server, all network locations should be configured to allow SMTP connections from the subscriber server.

In this example we are adding the EMEA subscriber to the SMTP configuration of the US publisher, as well as adding the US subscriber to the EMEA publisher SMTP configuration.

- In the US cluster on the US publisher, add the EMEA subscriber to the SMTP configuration (System Settings). In the **Edit** menu, select **Search IP Address Access List**. On the New IP Address page, enter the IP address of an EMEA subscriber server (10.195.99.31 in this example). Ensure that the **Allow Connection** option is selected.
- Repeat the above steps on the EMEA cluster publisher, emea-cuc1.ent-pa.com, to add the US cluster subscriber IP address.

Replication Between the Locations

After creating the HTTPS network, verify that the complete database is replicated between the two locations added to network. When initial replication begins, it can take a few minutes to a few hours for the data to be fully replicated between all locations, depending on the size of your directory.

Open the **HTTP(S) Link** created in the above step, and check the following values:

- Time of Last Synchronization

  Indicates the time stamp of the last time the local reader service attempted to poll the remote location feeder service for directory changes on the remote locations, regardless of whether a response was received.

- Time of Last Failure

  Indicates the time stamp of the last time the local reader service encountered an error while attempting to poll the remote location feeder service. If the value of this field is 0, or if the Time of Last Synchronization value is later than the Time of Last Error value, replication is likely to be progressing without problems.

- Object Count

  Indicates the number of users that the local Unity Connection location has synchronized from the remote location.

Add Remote Location Partition to Local Unity Connection CSS

When you initially set up a network between locations, users that are provisioned on the US cluster will not able to send voice messages to users on the EMEA cluster because the users in each location are in separate partitions and separate user search spaces that do not contain the partitions of users in the other locations.

- Edit the us-cuc1 calling search space (CSS) configured for the US Unity Connection server to include the EMEA location Unity Connection server partition emea-cuc1.
- Edit the emea-cuc1 CSS configured for the EMEA Unity Connection server to include the US location Unity Connection server partition us-cuc1.

Related Documentation

- *Voice Messaging* chapter of the *Cisco Collaboration System SRND*

  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab10/collab10/vmessage.html

- *Design Guide for Cisco Unity Connection*

  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/design/guide/10xcucdgx.html

- *HTTPS Networking Guide for Cisco Unity Connection*

  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/https_networking/guide/10xcuchttpsnetx.html

- *Unified Messaging Guide for Cisco Unity Connection*

  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/unified_messaging/guide/10xcucumgx.html

Conference Scheduling with Cisco TelePresence Management Suite (TMS)

This section describes the functionality of scheduling collaboration meetings utilizing TelePresence and hosted web conferencing. In addition to the Collaboration Meeting Room (CMR) functionality for users, a user is able to reserve rooms through existing calendaring tools, such as Microsoft Outlook clients, and have easy end-user connection to the collaboration session. This functionality is beneficial when the need for collaboration is known in advance and specific meeting locations (conference rooms) within the organization are equipped with TelePresence endpoints. The meeting organizer is then able to reserve the individuals and the locations, and have the technology configured for the meeting ready for use in a single application workflow.

Prerequisites

Before deploying the scheduling architecture, ensure that:

- The Call Control and Conferencing chapters of this document are understood and have been implemented.
- Room endpoints are registered with Unified CM for call control, and point-to-point calling is functional.
- Sizing and licensing of the scheduling solution are understood.

Core Components

The core architecture contains these key products:

- Cisco TelePresence Conductor
- Cisco TelePresence Servers
- Cisco TelePresence Management Suite (TMS) for conference provisioning, monitoring, and scheduling
- Cisco TelePresence Suite Provisioning Extensions (TMSPE) for configuring CMRs, as discussed in the Conferencing chapter
- Cisco TelePresence Management Suite Extension for Microsoft Exchange (TMSXE) for interfacing with Microsoft Exchange room / resource calendars.
- Cisco WebEx Software as a Service (SaaS)

The architecture includes these non-Cisco components as well:

- Microsoft SQL database
- Microsoft Active Directory
- Microsoft Exchange or Microsoft Office 365
- Network Load Balancer

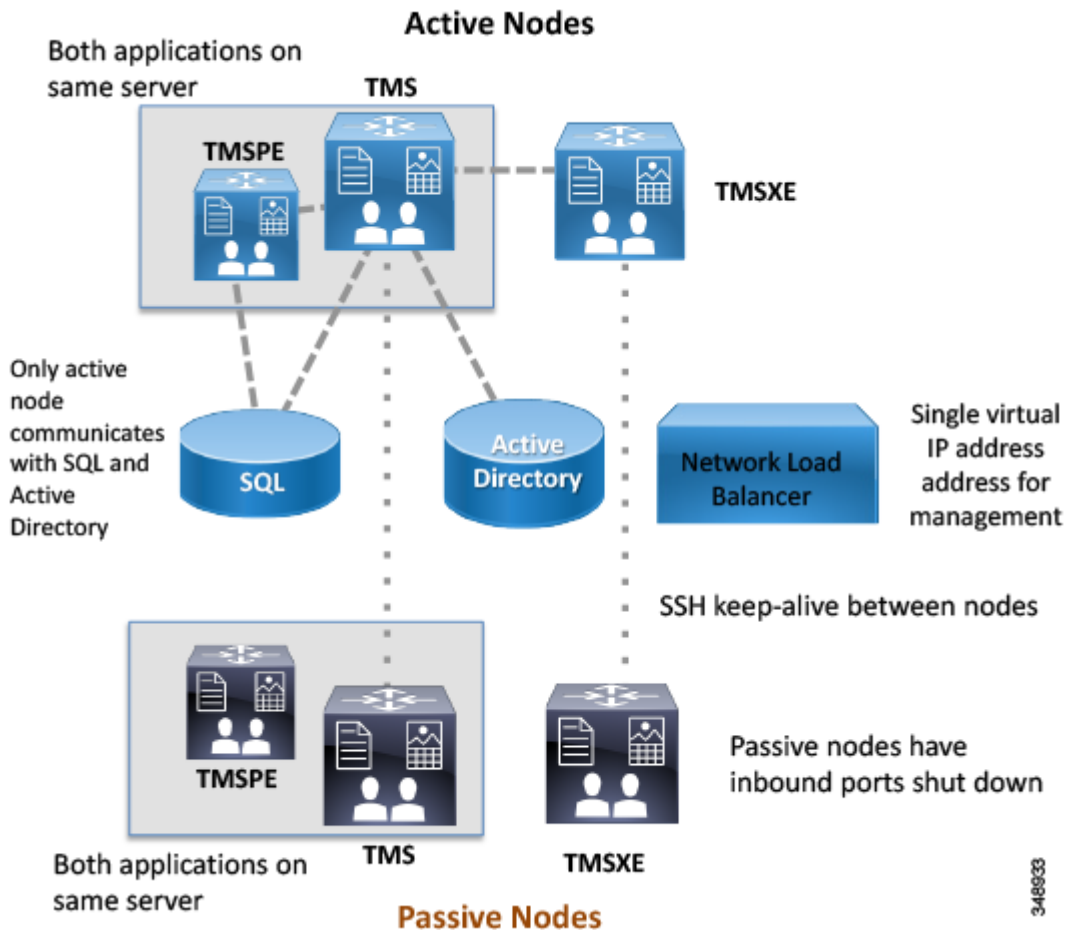
Key Benefits

- Scheduling for technology using the same tool to schedule the individuals and locations
- Integration of web conferencing participants without additional end-user intervention at meeting start
- High availability of scheduled conferencing resources and processes
- Resilience in the video network, which allows components to be taken off-line for maintenance

Core Architecture

The scheduling architecture consists of an active and a passive node for both Cisco TMS and TMSXE, which are deployed behind a network load balancer. For some deployments, Cisco TMS, TMSPE, and TMSXE can be installed on the same virtual machine; but for larger deployments TMSXE must be installed on a separate virtual machine, as indicated in Figure 5-5. (See the Sizing chapter for sizing details.) The TMS servers are installed in the customer data center that also hosts the organization's SQL deployment. All the server nodes function from a single, external Microsoft SQL database. Additionally, endpoints, TelePresence Conductor, TelePresence Servers, and Unified CM are involved in a successful scheduled conference. (See Figure 5-5.)

Figure 5-5 High-Level View of the Architecture



Role of the Cisco TMS

Cisco TMS integrates the conference room endpoints, TelePresence Conductor, and connections to the WebEx cloud in a manner that provides a unified experience for scheduled conferencing for the end user. Unified CM maintains the configuration control for endpoints, and TMS is then able to push the calendar to those endpoints. Administrators are able to set the parameters for the default conference for their organization, and then individual conferences will be created according to this template.

Some of the TMS features are not used in the Preferred Architecture; for example, phone books, software management, and reporting functions.

For more information on CMRs and TMS Provisioning Extensions (TMSPE), see the Conferencing chapter. CMRs are used for nonscheduled conferencing where specific endpoints are not identified, and the user simply dials in to the CMR number.

Role of the Cisco TMS Extensions for Microsoft Exchange

When end users schedule a meeting in Microsoft Outlook with multiple conference room resources, the Exchange Web Services (EWS) feature of Exchange synchronizes that event into TMS as a scheduled conference. This synchronization is bidirectional, allowing an administrator or support staff to update meetings as well without the need to access the meeting organizer's Outlook event. All endpoint resources within the organization that are intended to be in the conference must be listed on a single Exchange meeting request.

Conference Bridges for Scheduled Conferencing

Scheduled conferencing, including CMR Hybrid meetings for participation by Cisco WebEx users, works with TelePresence Conductor for allocation of conference resources that are connected directly to Unified CM. If TelePresence Conductor is clustered, Cisco TMS can recognize only one of the TelePresence Conductor cluster nodes and, therefore, add only a single TelePresence Conductor node to Cisco TMS for scheduled conferencing. For additional information on scheduled conferencing, refer to the Conferencing chapter.

Resilience

A deployment of Cisco TMS includes: Two TMS front-end servers that also host the TMS Provisioning Extension (TMSPE) application, two servers running TMSXE, a network load balancer, and a single external Microsoft SQL database.

TMS resiliency supports only two servers – one active node and one passive node – and this model does not increase or decrease the capacity of the TMS deployment. However, Cisco TMS can recognize only one of the TelePresence Conductor cluster nodes, and if that cluster node should fail, Cisco TMS scheduling will be unavailable until that node is brought back up or Cisco TMS is updated to communicate with a different TelePresence Conductor node within the cluster.

Cisco TMS Deployment Process

Deployment Overview

This section describes the high-level configuration tasks required to deploy Cisco TelePresence management Suite (TMS) in the Enterprise Collaboration Preferred Architecture. To deploy Cisco TMS in a redundant configuration for scheduled applications, perform the following tasks in the order listed here:

1. Planning
2. Install and Configure TelePresence Management Suite (TMS) on Active and Passive Nodes
3. Install and Configure Network Load Balancer (NLB)
4. Configure File Share Between Active and Passive Node Servers
5. Additional TMS Configuration
    a. ISDN and IP Zones
    b. Active Directory Integration, Group Structure, and Users
    c. System Navigator Folder Structure
    d. WebEx Connections
    e. Default Conference Settings
6. Add Managed Devices to TMS
    a. Install and Configure Scheduled TelePresence Conductor
    b. Add Unified CM to TMS
    c. Add Conference Room Endpoints to TMS
7. Install and Configure TMS Extensions for Microsoft Exchange

1. Planning

Before beginning the installation and configuration process, you must decide on several items to align with the specific structure and preferences of your organization. Additionally, some specific settings must be used during the configuration process and should be gathered prior to beginning the install process.

Microsoft SQL

Cisco TMS utilizes an external Microsoft SQL database to store all data regarding meetings, users, and systems. During the installation process, TMS and associated software extensions create a number of specific databases. The TMS application does not allow users to log into the web page if communication is not currently active with the tmsng database. This dependency on constant communication with the SQL database requires the SQL database to utilize Microsoft's methods for making the database resilient as well. The databases will vary in size depending upon the deployment size and number of scheduling events; but as a general guideline, 1 GB of initial storage will suffice for most organizations.

Table 5-20 lists the Microsoft SQL 2012 specifics required to support Cisco TMS, TMSXE, and TMSPE.

Table 5-20 Microsoft SQL 2012 Specifics Required to Support Cisco TMS, TMSXE, and TMSPE

Requirement	Parameter
SQL user account permissions for account used by TMS	**dbcreator** and **security admin** roles
Authentication	SQL Server and Windows authentication (mixed mode)
Default language	English
Time zone	Must match the time zone on TMS server
Databases created	tmsng (CiscoTMS) tmspe (CiscoTMSPEmain) mspe_vmr (Cisco TMSPE Collaboration Meeting Rooms) tmspe_userportal (Cisco TMSPE self-service portal)
Resiliency model	**AlwaysOn Failover Cluster** instances through Windows Server Failover Clusters (WSFC)

Note While other modes of SQL resiliency are supported by TMS, any method besides **AlwaysOn Failover Cluster** requires manual adjustments by the TMS administrator during an SQL outage situation.

Active Directory

Cisco TMS functions using many aspects of Microsoft Active Directory, and the server must be added to the organization's domain,. All TMS users must be imported from and authenticated with Active Directory.

During the configuration process, you must enter an **AD Service account username and password** for TMS to import users. This is a read-only account, and TMS does not modify any information in Active Directory. This account should have access to the highest level of the AD structure that enables all subsequent end users to access its functionality. In organizations with multiple domains, the TMS user account must be associated with the top level domain. An additional service account is required for the TMSXE application for end-user booking of Exchange resources. This should also be a read-only service account, and end user credentials are used for the actual event booking. TMSXE user account permits only the TMSXE application to authenticate and communicate with the Exchange Servers through Exchange Web Services.

Additionally, identify existing, or create new, Groups with AD that will serve to synchronize TMS administrators and end users with scheduling access to TMS.

Note Local machine accounts on the TMS server should not be used because they are not duplicated between front-end servers, and the user credentials would not be available if the other node became active.

Email Integration

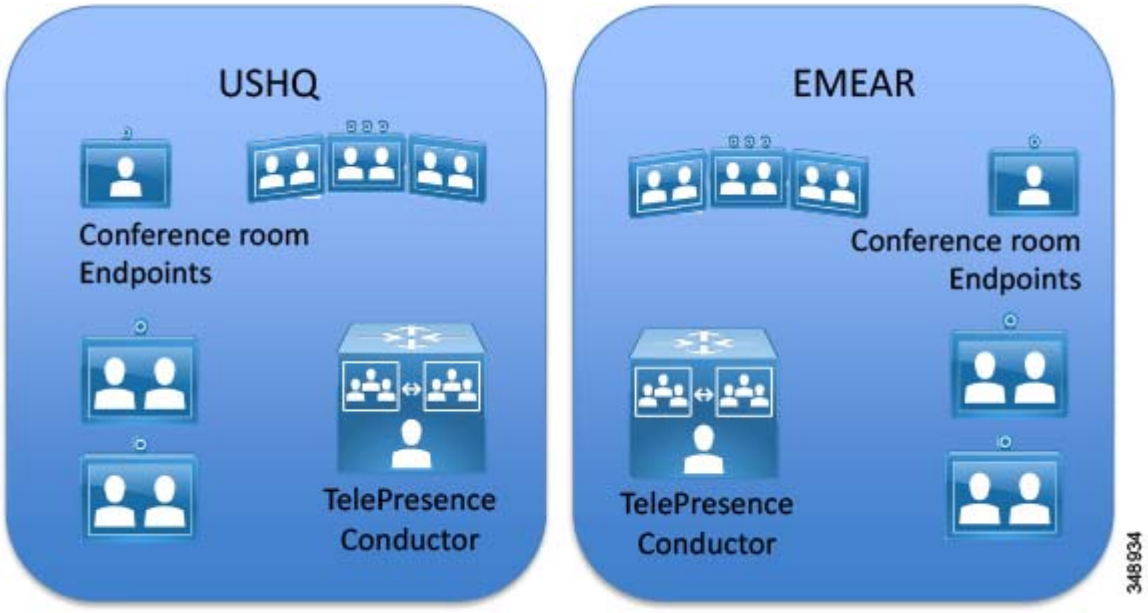
TMS sends automated emails to users when they schedule meetings, with all connection information included for the participants. During the installation process, you must enter the "from" address that end users will see as the originating for these emails, so select an address such as collabconferencing@ent-pa.com or a similar address not currently used in your organization.

You will also need to enter the SMTP address of the outgoing mail server.

Zones

Cisco TMS uses a concept called *zones* to provide guidance to the scheduling engine on how to build the calls and keep the traffic localized as much as possible. Endpoints, conferencing resources, and ISDN gateways are all assigned to these zones. The zones define where to use which kind of network connections. The Preferred Architecture is based upon all endpoints being able to use a single IP network for connections, and ISDN would be used only for connecting outside of the organization. (See Figure 5-6.)

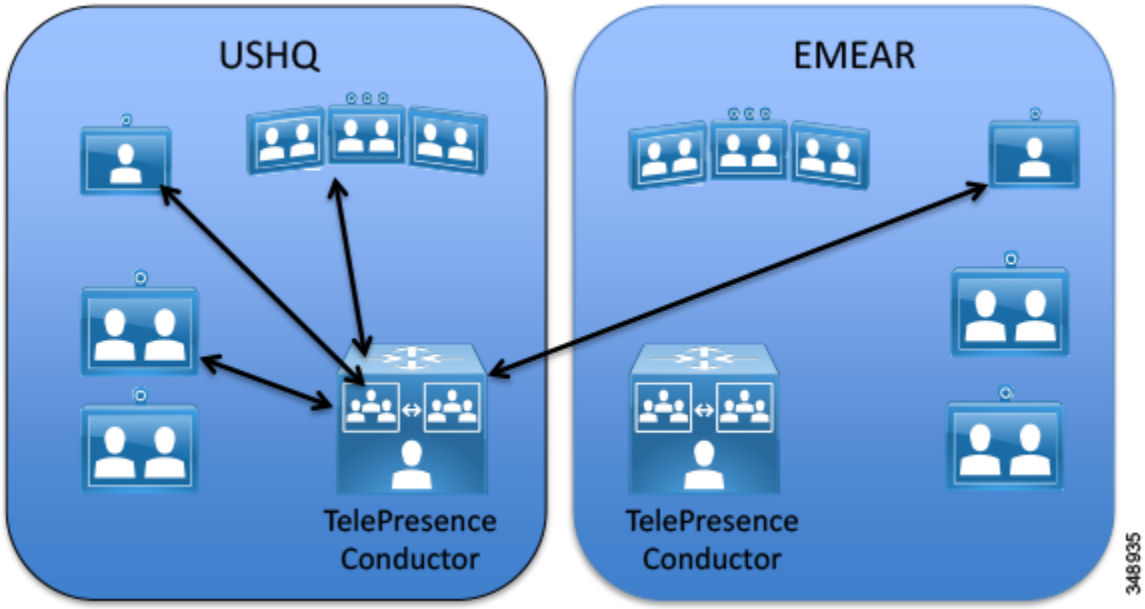
Figure 5-6 Cisco TMS IP Zones



IP Zones

IP zones refer to areas of you network that share a common primary data center, and they are used primarily to identify "local" conferencing resources. During the configuration process, you will need to add IP zones for each location where conferencing resources will be placed. (See Figure 5-7.)

Figure 5-7 Cisco TMS Uses IP Zones to Select Best TelePresence Server for a Conference



ISDN Zones

ISDN zones are similar to the IP zones, but specific to any deployment of ISDN gateways in the organization. If no ISDN functionality is needed, you still have to configure a single ISDN zone for the entire enterprise during the installation.

Endpoint Naming Conventions

Endpoints are added to Cisco TMS for two reasons:

- Correlation with Exchange resources for conference resource allocation
- Enabling TMS to provide One Button to Push connection information on the endpoint user interface

As endpoints are added to TMS, use the same character string as the room or resource name in Exchange. This provides uniformity and consistency to end users when system names appear in the call history and fill the text of on-screen labels from conferencing resources.

An organized plan for how to use the folder structure of TMS Systems Navigator will also assist the administrator in having a simplified interface.

Default Conference Parameters for Your Organization

These settings are customizable for each organization and should be used in accordance with your own network considerations, meeting flows, and corporate culture. The default conference settings are used for all meetings scheduled through Outlook by end users. For all possible settings of the default conference, refer to the *Cisco TelePresence Management Suite Administrator Guide*, available at

http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html

WebEx Site for CMR Hybrid

Be sure that you have the hostname and site name for your WebEx site. Then configure this WebEx site for integration between the on-premises TelePresence conferencing infrastructure and the WebEx cloud.

CMR Provisioning

As discussed in the Conferencing chapter, an understanding of how the organization plans to utilize Collaboration Meeting Rooms is foundational to understanding the workflow that end users expect for meetings. Some organizations may choose to leverage ad-hoc CMRs instead of scheduled resources for certain meeting types, especially when most workers are individually separated and not likely to aggregate into local conference rooms.

Location of Servers

Both the active and passive nodes for a redundant TMS deployment must be configured with the same time zone within the server operating system. In addition, this must be the same time zone as the SQL server. Support of TMS redundancy is limited to the same local network for both the active and passive nodes, along with the SQL server.

2. Install and Configure TelePresence Management Suite (TMS) on Active and Passive Nodes

Cisco TelePresence Management Suite (TMS) should be installed for redundant deployments according to the guidelines in the *Cisco TelePresence Management Suite Installation and Upgrade Guide*, available at

http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-guides-list.html

- Install the application on the primary server.
- Point to the external SQL resource configured in the planning stage.
- Make note of the encryption key.
- Verify basic operation by logging into the web portal and enabling TMS redundancy.
- Install the application on the second server using the encryption key from the first server, and using the same SQL credentials as the first server.

Both servers will access the single SQL database that holds all conferencing and configuration data. In the active and passive node configuration, a single encryption key and certificate are used for both servers. Having this encryption key and certificate on each server allows for all communications from end users to TMS, and from TMS to managed devices, to be done using secure protocols.

3. Install and Configure Network Load Balancer (NLB)

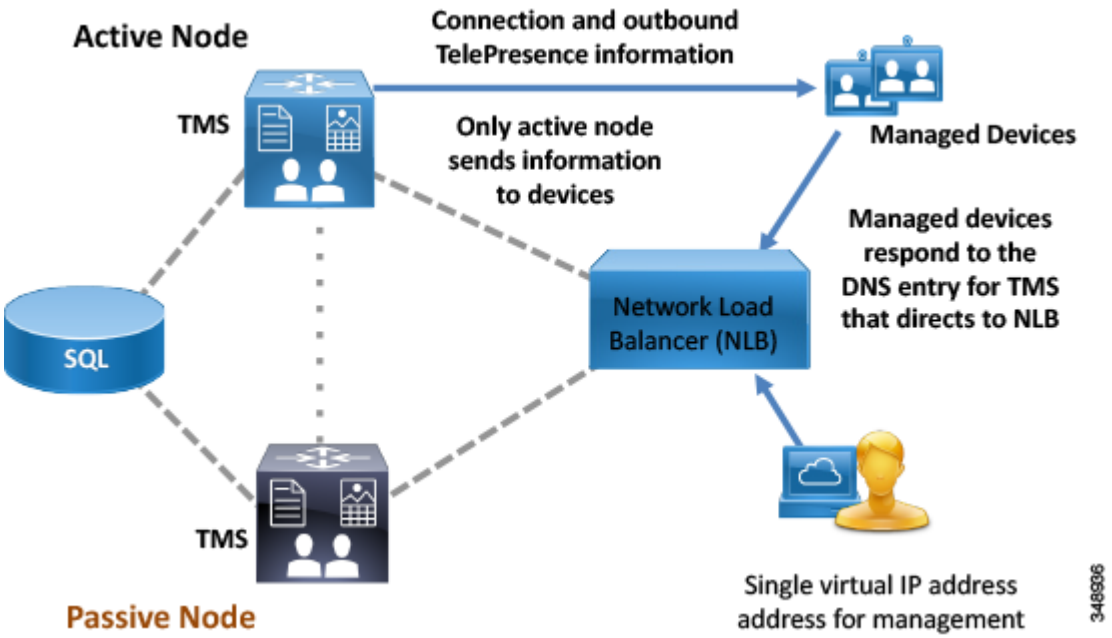
The specifics of the network load balancing configuration are left to the instructions of the load balancer chosen by the customer. The following are functional requirements that must be configured:

- Forward HTTP, HTTPS, and SNMP traffic to the active node.
- Configure the network load balancer probe to the Probe URL within Cisco TMS.
- Push all traffic to the active node.

The Cisco TMS server sends outbound communications directly to managed devices without routing that traffic through the NLB. However, all return communications from managed devices and all web portal requests must be routed through the NLB. The communication path permits end users and endpoints to use a single address, regardless of which TMS server node is in the active mode.

Configure TMS Network Settings to the FQDN of the TMS address configured on the network load balancer. This setting within TMS will populate the address that the managed devices will use to initiate communications to TMS. By using a FQDN of tms.company.com that resolves to the load balancer, all inbound traffic from endpoints or end user web clients will be directed through the NLB and resolve to the active node. (See Figure 5-8.)

Figure 5-8 NLB Directs Communications from Managed Devices to the Active TMS Node



4. Configure File Share Between Active and Passive Node Servers

While the SQL database is used for all operational data, some application specific files are stored within the file structure of the host server. These customizable files are added by the TMS application and must be synchronized between the two servers when using a redundant deployment. The files include software and images that can be uploaded to Cisco TMS, and images created by Cisco TMS.

In a default installation the files are located at:

C:\Program Files\TANDBERG\TMS\Config\System\

C:\Program Files\TANDBERG\TMS\Data\GenericEndpoint\

C:\Program Files\TANDBERG\TMS\Data\SystemTemplate\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\CompanyLogo\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles\

C:\Program Files\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\

Use the Distributed File System (DFS) function within the Windows Server operating system to complete this replication process between the two servers. DFS will keep these folds in sync between the two servers when the "Full mesh" configuration is used.

5. Additional TMS Configuration

Perform the following additional configuration tasks during the installation of Cisco TMS to make the deployment function as intended in the Preferred Architecture:

- ISDN and IP Zones
- Active Directory Integration, Group Structure, and Users
- System Navigator Folder Structure
- WebEx Connections
- Default Conference Settings
- Modify Email Templates within TMS

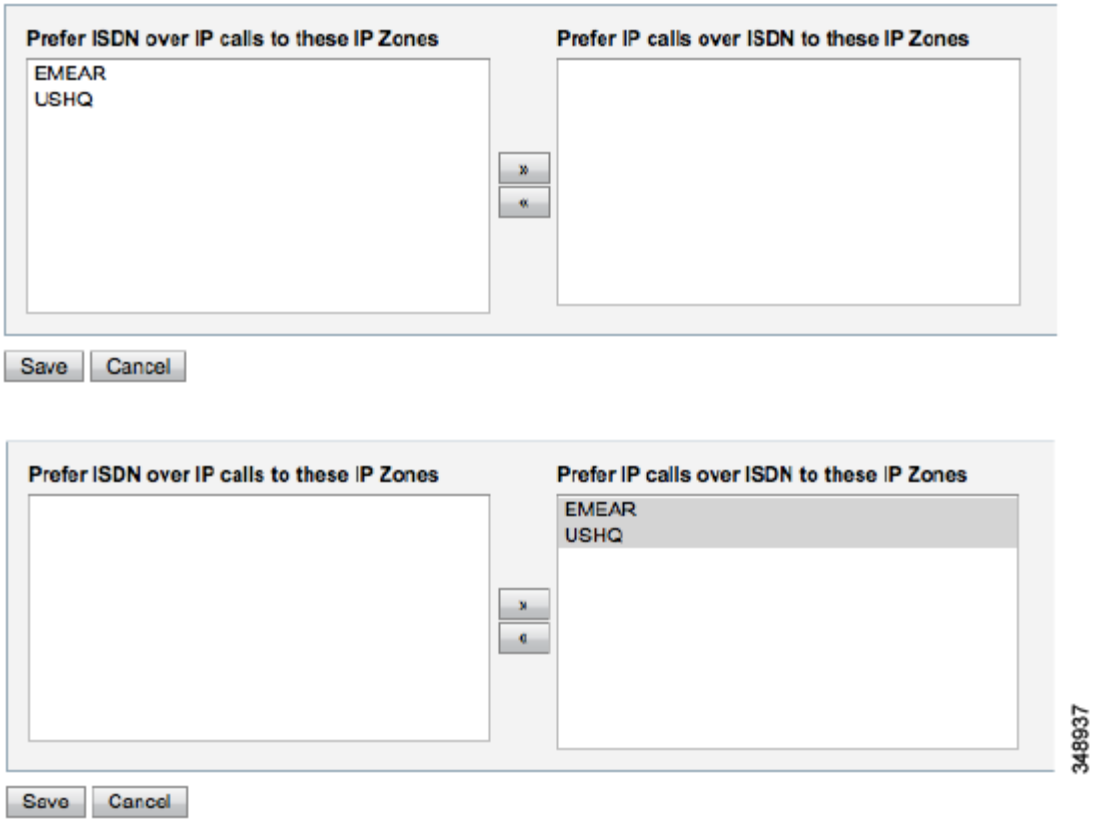
ISDN and IP Zones

Configure additional IP zones for each location that will have conferencing resources.

Each location that has conferencing resources should be identified with a unique IP Zone.

Note Be sure to populate the **Prefer IP calls over ISDN to these IP Zones** according to your network configuration (see Figure 5-9). By default, all new IP Zones will "prefer" ISDN over IP to all other existing IP Zones. Failure to make this selection could cause a failure in conference configuration by TMS because TMS will not see any way to route calls between zones.

Figure 5-9 Configure IP Zones to Prefer IP Calls over ISDN



Configure any additional ISDN zones.

For each intended ISDN gateway, create an additional ISDN Zone in TMS. This will make endpoints use your intended ISDN gateway for all scheduled calls, as defined in the Collaboration Edge chapter. Each of your ISDN gateways will have a prefix for dialing externally, and that prefix must be configured into TMS.

Active Directory Integration, Group Structure, and Users

Verify that all of the information is correctly entered for your Active Directory service account.

Note Make sure all of your settings for AD connectivity are correct, and test the connection. Other AD interfacing commands within TMS might not display errors, even if AD synchronization is not functioning.

Build a group structure to match your organizational needs using Active Directory Groups.

Three different groups are created by default during the TMS installation:

- Users
- Video Unit Administrator
- Site Administrator

These groups may be modified to meet customer needs, but they cannot be removed. By default, all groups have the same access permissions as Site Administrator.

These default groups are limited to manual entry of users; therefore groups should be imported from Active Directory, and existing Active Directory Groups should be used to manage end user access to TMS functions. Be sure to consider groups for end users that schedule conferences and support desk personnel and technical administrators.

For additional information about groups, see the *Cisco TelePresence Management Suite Administrator Guide*, available at

http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html

Using the **Import from AD** feature allows for a single point of end user job function management. When employees are added or removed, or job functions change and organizational Active Directory groups are modified, TMS permissions are automatically updated.

Once you have imported groups from Active Directory, assign appropriate permissions to each group. On the screen that appears, simply uncheck any permissions that you do not want that group to have. Failure to restrict these permissions can result in unintended configuration changes.

Also, be sure to select the appropriate default group for all users.

Note Anyone accessing Cisco TMS will be added automatically to the Users group, and this cannot be unselected. De-select any permissions that the administrator does not want everyone within the organization to have.

Import Users

Once permissions are set for groups, import users using the **Synchronize All Users with AD** function. Depending upon organization size and number of groups involved, the synchronization can take many minutes to complete.

Note Users will not appear in the list of users until they log into TMS for the first time.

System Navigator Folder Structure

The TMS System Navigator utilizes a folder structure to group devices logically for the administrator. Build a folder structure to match your organization's physical deployment. These folders are visible only to the administrators, not to end users. Arrange the folders according to the logical flow for your organization. For example, create a folder for each geography, and then create a sub-folder for the infrastructure and another folder for conference room endpoints. Folders within the System Navigator may contain endpoints and/or infrastructure devices that receive connection instructions from TMS.

WebEx Connections

To benefit from Cisco CMR Hybrid, connections must be made to the organization's WebEx site. (See the Conferencing chapter for information on CMR Hybrid.) Verify that the settings in Table 5-21 have been made within TMS.

Table 5-21 TMS Settings for WebEx

Parameter	Value
Enable WebEx	Yes
Add WebEx to All Conferences	Yes
Get WebEx Username from Active Directory	Username (samAccountName)
WebEx Site	Configured per customer account
Default site for new users	Yes
Enable SSO	Yes

The settings in Table 5-21 allow TMS to communicate with the organization's WebEx site on behalf of the end user during scheduling. By automatically adding WebEx to every conference, even if the administrator needs to generate a meeting through methods other than WebEx Productivity Tools, a WebEx link will be made available to end users. The SSO settings allow end users to use a single set of credentials to access all collaboration services, because WebEx services are able to leverage AD credentials for end users to access WebEx tools.

Default Conference Settings

Before scheduling conferences, the administrator should understand the end user community usage model as well as any endpoint limitations. Important Cisco TMS settings to consider include:

- One Button to Push
- Bandwidth
- Add WebEx to all Conferences
- Allow Participants to Join 5 minutes Early

One Button to Push

One Button to Push enables end users to see a calendar of the day’s meetings for a particular room and to launch the connection to the conference. Cisco TMS gives users 72 hours worth of calendar information per request.

Bandwidth

This setting is per endpoint. Adjust the bandwidth to the desired setting for your network. To allow for HD main channel and maximum resolution of content, the default bandwidth for non-immersive systems should be set at 2048 kbps. Any endpoint that has a lower setting for maximum bandwidth will join at its maximum bandwidth.

Add WebEx to all Conferences

This setting should be selected to provide a full collaboration experience for each meeting. Select the option to set the Method of User Access to **WebEx (Username)**. This setting will cause the username of the person scheduling the meeting to appear in the WebEx portion of the invitation, and it allows the meeting to populate that end user's Jabber or WebEx mobile client agenda.

Allow Participants to Join 5 minutes Early

This setting should be selected to allow for slight variations of end-user time interfaces. Allowing users to join prior to the exact time of the TMS server provides a more consistent end-user experience and prevents end users from receiving an "unable to connect" message if they attempt to connect to a meeting a few minutes before the meeting start time.

Modify Email Templates within TMS

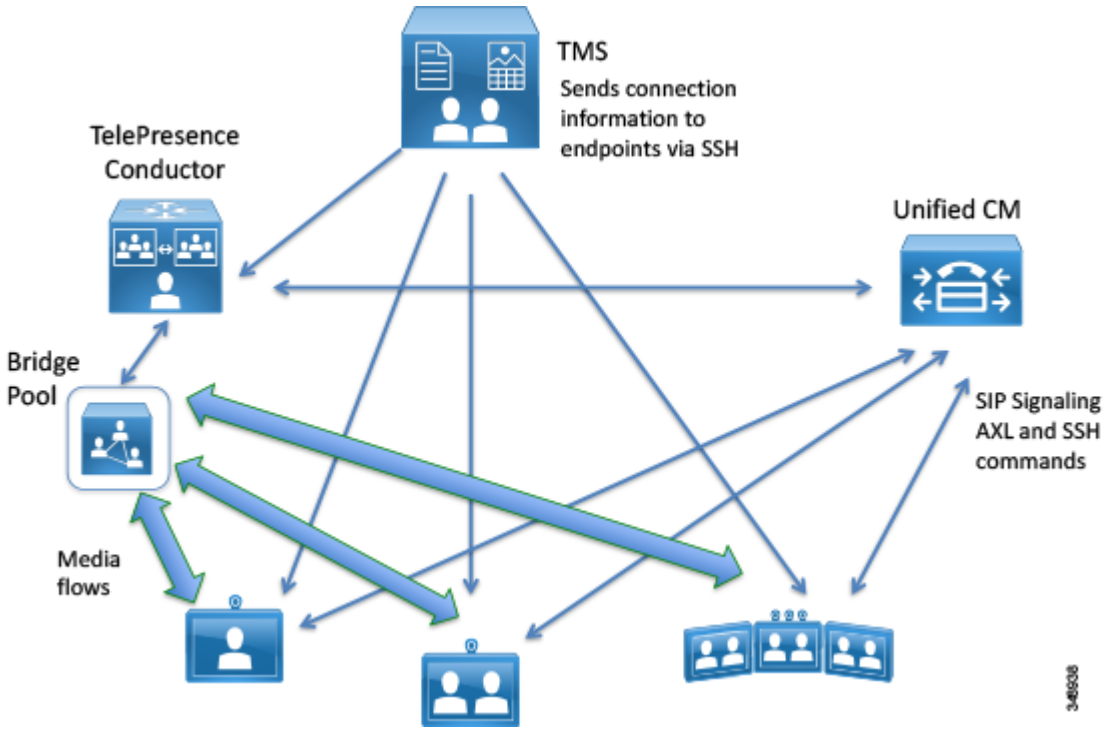
Cisco TMS contains the templates used to notify conference organizers. However, Cisco TMSXE can inject errors, warnings, and informational text into email messages sent by Cisco TMS. These messages can be modified by the administrator. Avoid removing or changing text in curly brackets – for example, {MEETING_TITLE}, {CONTACT_HOST}, and so forth – because these are variables that embed other specific content from the scheduled event.

Look at all email templates to ensure that communications automatically generated by TMS align with your intended procedures. Many of these templates might be rather simplistic and are intended to be enhanced by individual organizations. The templates may be modified using any standard HTML editor.

6. Add Managed Devices to TMS

For Cisco TMS to build scheduled conferences, you must add the needed components into TMS as systems. Unified CM is added to TMS to allow the TMS scheduling mechanisms be aware of the call control entity for all devices. TMS does not control any settings on Unified CM, but it does communicate directly to conference room endpoints managed by Unified CM. (See Figure 5-10.)

Figure 5-10 Cisco TMS Communicates Directly with Unified CM Managed Endpoints



Install and Configure Scheduled TelePresence Conductor

This section provides an overview of what is required to install and deploy TelePresence Conductor ready to be scheduled by Cisco TMS. The major deployment tasks are:

- Add TelePresence Conductor and TelePresence Servers to TMS for Scheduling
- Integrate TelePresence Conductor with the Dial Plan
- Adjust the TMS Ticket Filter to Remove Gatekeeper Warnings

The physical location of a TelePresence Server is important to consider because media traffic will flow between this point and each participant. Centralize the location of the TelePresence Conductor with its managed TelePresence Servers in each region where they will be deployed.

Cisco TMS recognizes only a single TelePresence Conductor node within the cluster. If multiple TelePresence Conductors are configured (one per TelePresence Conductor cluster), then they are considered by Cisco TMS for scheduled conferences. Cisco TMS uses the IP Zone configuration of the TelePresence Conductor and the endpoints scheduled at the time of the booking to decide which TelePresence Conductor should be preferred in the booking.

Install and configure TelePresence Conductor according to the information in the Conferencing chapter.

Add TelePresence Conductor and TelePresence Servers to TMS for Scheduling

Using the folder structure established in the planning and configured into TMS System Navigator during the configuration process, add a single TelePresence Conductor node to TMS for management. Be sure to select the appropriate IP Zone for each installed TelePresence Conductor. Also, add each TelePresence Server managed by the TelePresence Conductor to the same folder in TMS with the same IP Zone as TelePresence Conductor.

Note TelePresence Conductor and TelePresence Servers are added as non-SNMP devices when adding them through the TMS System Navigator.

Integrate TelePresence Conductor with the Dial Plan

As part of preparing to install the TelePresence Conductor for scheduled calls, you created conference alias and identified a numeric range for the TelePresence Conductor to use as part of the dial plan and designated in the SIP trunks. Table 5-22 lists the TelePresence Conductor dial plan parameter settings.

Table 5-22 TelePresence Conductor Dial Plan Settings

Parameter	Value
Numeric ID Base	This is the first number in the scheduled conferencing range of the dial plan.
Numeric ID Step	Keep the default value of 1 to utilize every number in the range.
Numeric ID Quantity	Specify the number of digits allowed in the dial plan for this TelePresence Conductor.
Register with Gatekeeper	This should be set to **off** because the Preferred Architecture uses SIP connections, not H.323.

Leave all other settings as default and save the configuration to add the TelePresence Conductor to TMS.

Adjust the TMS Ticket Filter to Remove Gatekeeper Warnings

Cisco TMS will populate the dial plan numbers provided in the previous steps into both E.164 aliases and SIP URIs. However, the implementation of E.164 logic within TMS differs from its use elsewhere in the Preferred Architecture. TMS associates an E.164 alias with H.323 communication only. It is therefore necessary to adjust the integrated ticket system of TMS to ignore certain warnings for the TelePresence Conductor.

Once the TelePresence Conductor has been added to TMS, adjust the Ticket Filters for this entry by adding the filter for **Gatekeeper Mode Off**.

Add Unified CM to TMS

While Unified CM administers the conference room endpoints for all other aspects of configuration and management, the Unified CM cluster must be added into TMS to allow for booking and connection initiation. To add Unified CM to TMS, perform the following tasks:

- Create an Application User for Cisco TMS within Unified CM
- Add the Publisher for each Unified CM Cluster in Your Environment

Adding multiple Unified CM clusters requires adherence to the dial plan configuration outlined in the Call Control chapter.

Create an Application User for Cisco TMS within Unified CM

This application user allows TMS to communicate with endpoints controlled by Unified CM. This user must be assigned all of the conference room devices within Unified CM that will be scheduled. This user must also be added to a user group just for Cisco TMS, with the following roles:

- Standard AXL API Access
- Standard CTI Enabled
- Standard SERVICEABILITY
- Standard CCM Admin Users
- Standard RealtimeAndTraceCollection

For more information, refer to the *Cisco Unified Communication Manager Configuration Guide for the Cisco TelePresence System*.

Add the Publisher for each Unified CM Cluster in Your Environment

Adding the Unified CM publisher to TMS makes TMS aware of the call control authority for its endpoints. Without knowledge of Unified CM, the TMS scheduling engine cannot properly utilize the full functionality of your deployment, and connection failures could occur.

The publisher is added using the same method as other devices, by using the application user you created in the above step for the user name and password when prompted by TMS.

Add Conference Room Endpoints to TMS

Rather than adding devices by IP address or DNS name, use the **From List** tab and then select Unified CM. Select all the conference room TelePresence devices that you wish to have available through the scheduling interfaces of TMS. Be sure to select the appropriate IP Zone for each endpoint. This IP Zone will be used to select the best TelePresence Server available for the endpoints in any conference. Make sure that the DN for each endpoint in Unified CM complies with the E.164 guidelines listed in the Call Control chapter.

Do not add personal TelePresence devices (for example, Cisco TelePresence EX or DX Series endpoints) that will not be scheduled through Exchange as resources to TMS.

7. Install and Configure TMS Extensions for Microsoft Exchange

Cisco TelePresence Management Suite Extension for Microsoft Exchange (Cisco TMSXE) is an extension for Cisco TelePresence Management Suite that enables videoconference scheduling via Microsoft Outlook, and it replicates Cisco TMS conferences to Outlook room calendars.

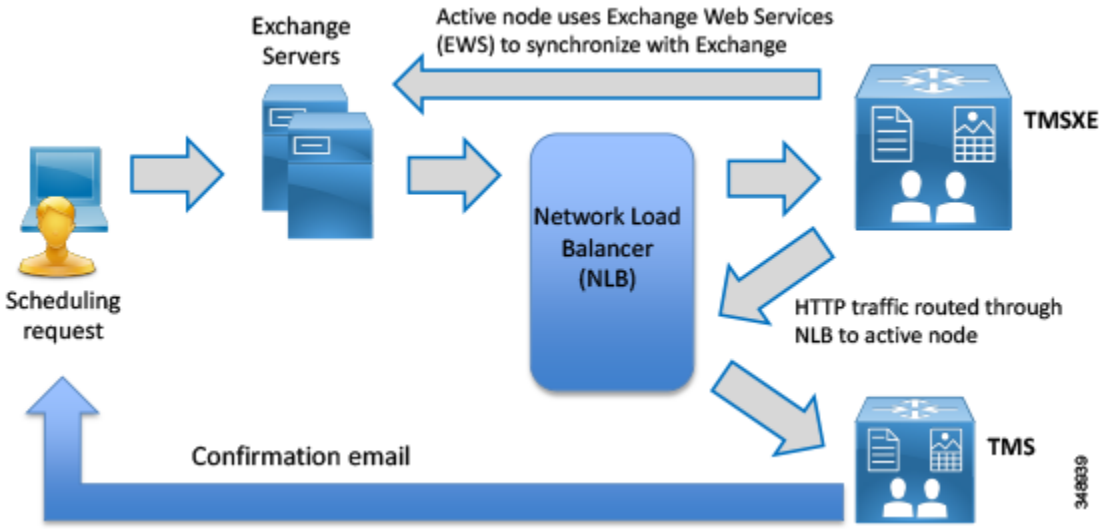
This software extension to TMS requires a license key to activate the functionality within TMS. This key must be installed in TMS before installing the TMSXE software. For deployments with more than 50 scheduled endpoints, TMSXE must be installed on its own server or virtual machine instance.

Prerequisites

Before installing Cisco TMSXE, make sure both Outlook and Exchange are already set up so that users are able to book meetings that include room mailboxes (see Figure 5-11). This integration is licensed either by groups of endpoints or as an Application Integration license key. The correct key must be procured and entered into TMS before proceeding with the installation. If both option keys are added, only the Application Integration Package option will be used by Cisco TMS

Cisco TMSXE may use Microsoft Exchange Resources that are either on-premises, Office 365 hosted deployments, or hybrid customer deployments. Consult the Microsoft Exchange administration and deployment guides for any guidelines or recommendations that might apply to specific customer environments.

Figure 5-11 Sample Flow for Scheduling a Conference by an End User



Once the per-system option key has been activated in Cisco TMS, the **Allow Remote Bookings** setting determines whether each system is using a license. This setting allows the administrator to select which endpoints are able to be booked by end users and consume one of the individual endpoint licenses. This setting is void and hidden if the Application Integration Package option is used.

Before endpoints can be added to Cisco TMSXE, they must be represented by a room mailbox in Exchange. To simplify TMSXE setup, we recommend using the endpoint's Cisco TMS display name as the mailbox name (with any spaces removed). This provides commonality across all methods by which end users would see the system name appear.

Special Notes About Privacy Features of Exchange:

All room mailboxes added to Cisco TMSXE must be configured to handle booking subjects and privacy settings in the same way. This means that the following settings must be applied to either all or none of the mailboxes:

- Delete the subject

  We recommend not using this feature so that support staff is able to identify a particular meeting in the Conference Control Center. Also, this will allow the meeting title to appear on the One Button to Push interface of capable endpoints.

- Add the organizer's name to the subject

  Use of this setting should be considered very carefully, and will depend upon organizational culture and practices. Keep in mind that if one person schedules meetings for multiple groups, those meetings will be listed by that scheduler's user name and not by the meeting subject, which might be more beneficial. On the other hand, if meetings are scheduled by their respective hosts, then it would be easy to identify "Bob's meeting" instead of remembering the specific meeting title. For most organizations, we recommend not using this setting.

- Remove the private flag on an accepted meeting

  While the "private" flag is respected within the Outlook client, it is not supported by Cisco TMS, and meeting subjects will be freely viewable:

  - In Cisco TMS
  - On endpoints that support the Meetings calendar, if other individuals also have use of a room used for a meeting where the subject title should not be public within the organization. (For example, if a "Merger meeting" for the chief executive is scheduled in a room also used by lower-level employees who would not need to have knowledge of a pending merger, those lower-level employees would be able to see the meeting on a room system calendar.)
  - If a booking that has a "private" flag in Exchange has its participants or recurrence pattern modified in Cisco TMS, the "private" flag will be removed when these changes are replicated to Exchange.

Installation Process

Create TMSXE User

- Create a TMSXE user in Active Directory and import that user into TMS.
- In TMS, the user needs to be in a new or existing group with the following permissions enabled under Booking:
  - Read
  - Update
  - Book on Behalf of
  - Approve Meeting

Install Certificates

Cisco TMSXE and TMS communicate using HTTPS. The certificate also allows for secure communications between the TMSXE server and the Exchange environment. As with the TMS application server, the same certificate is loaded on both the active and passive nodes of TMSXE, and the certificate DNS entry points to the entry of the Network Load Balance address used for TMSXE.

Run Software Installer

- Be sure to select TMS Booking Service to allow use of WebEx Productivity Tools for scheduling.
- Select the appropriate redundancy option for active or passive nodes.
- Complete the software installation on both active and passive nodes.

Once both the active and passive nodes have been installed, configure the Network Load Balancer with the probe URL for each node.

Configure Cisco TMSXE

Cisco TMS Connection Information

Configure TMS connection information using the TMSXE account created in Active Directory to allow the TMSXE application to communicate with the TMS application.

Configure Exchange Web Services

Configure Exchange Web Services (EWS) to allow TMSXE to communicate with the Exchange servers for user and resource mailboxes. The credentials used for this connection are also the same TMSXE credentials used elsewhere.

Align Exchange and TMS Resources

Align Exchange resources to TMS System IDs. This may be done individually or by using a .csv file as outlined in the *Cisco TelePresence Management Suite Extension for Microsoft Exchanged Deployment Guide*.

Use of WebEx Productivity Tools for End Users

To provide the best experience for end-user collaboration tool usage, deploy WebEx Productivity Tools for all users. WebEx Productivity Tools with TelePresence adds a special panel to Outlook for Windows that allows users to synchronously book and configure:

- CMR Hybrid meetings that include both WebEx and TelePresence
- WebEx-only meetings
- TelePresence-only meetings

The panel provides access to simple and advanced settings for both WebEx and TelePresence, including the option of adding call-in and call-out TelePresence participants, and allowing WebEx participants to join the meeting ahead of start time.

Note that all organizers must be set up with a WebEx user for Productivity Tools to work, even when booking TelePresence-only meetings.

Detailed instructions on configuration and deployment of WebEx Productivity Tools with TelePresence can be found in *Cisco WebEx Site Administration User's Guide*, which is available as web help and a PDF file from your WebEx site.

Tools for Application Deployment

In addition to the core applications described in this chapter, there are two useful tools to help administrators deploy the Enterprise Collaboration Preferred Architecture:

- Cisco Prime Collaboration Deployment — Assists the administrator by automating many of the steps necessary to install a Unified CM cluster with IM and Presence Servers.
- Cisco Prime License Manager — Is integrated into Cisco Unified CM as a tool to provide the administrator with a single management point for the various licenses used in a deployment.

Cisco Prime Collaboration Deployment (PCD)

Prime Collaboration Deployment (PCD) assists the administrator with the tasks of deploying new clusters of Unified CM and IM and Presence servers. The automation greatly assists administrators by configuring all common settings in the nodes of the cluster.

PCD is a standalone application that must be installed on its own virtual machine prior to beginning any other installation tasks. To install a new cluster using PCD:

1. Deploy the host hardware and configure the ESXi.
2. Download the necessary OVA template and Cisco ISO images for the target release.
3. Deploy the recommended OVA template for your enterprise:
   a. Create the virtual machines for each node on the ESXi hosts (one virtual machine for each server to be installed).
   b. Configure the network settings on the new virtual machines.
4. Add the ESXi host to the PCD user interface.
5. Create a new task within PCD for the type of cluster being created. Define the nodes to be installed and their associated virtual machines.

Cisco PCD will then complete the process of installing the application on the virtual machines and will provide an email notification to the administrator when the task is complete.

Cisco Prime License Manager (PLM)

Cisco Prime License Manager (PLM) provides simplified, enterprise-wide management of user-based licensing, including license fulfillment. Cisco Prime License Manager handles licensing fulfillment, supports allocation and reconciliation of licenses across supported products, and provides enterprise-level reporting of usage and entitlement.

A single virtual machine is required for an enterprise, and the application should be backed up through VMware tools. As a standalone instance of PLM, all nodes of the Preferred Architecture could be effectively managed. Since this is not an end-user facing application and does not have any real-time usage impacts, no clustering is required. Since one of the features of PLM is the ability to support e-Fulfillment of additional licenses, this server must have access to the Internet to pull new license files.

Within the Preferred Architecture, the following products are supported by PLM:

- Cisco Unified CM
- Cisco Unity Connection

Key features of PLM that benefit the administrator:

- License usage history
- e-Fulfillment of new licenses

License Usage History

The ability for an administrator to track usage of collaboration portfolio licenses over time gives that administrator better ability to plan for additional licenses when needed. In addition, this license usage tool assists the administrator with remaining in compliance with all license usage rules.

An application is allowed 60 days of non-compliance, during which administrators can make changes if there are insufficient licenses or if the PLM node has lost communication with the application node. After 60 days of non-compliance, the Unified CM application(s) will no longer allow administrative changes; however, the application(s) will continue to function (call control) with no loss of service. After 60 days of non-compliance, the Unity Connection application(s) will allow administrative changes, but the application(s) will not continue to function (users will not have access to voice messaging).

e-Fulfillment of New Licenses

When the administrator needs to procure additional licenses, the e-Fulfillment tool within PLM simplifies the number of steps required, and it imports the licenses into the appropriate product for use.

Additional Applications

There are many additional applications provided by Cisco and ecosystem partners that enhance a collaboration environment. Table 5-23 is not intended to be all-inclusive, but it lists some frequently referenced applications for customer deployments.

Table 5-23 Additional Cisco Applications for the Preferred Architecture

Application Name	Functions	Integration Method
Contact Center Enterprise (CCE)	Provides internal and external customer collaboration technologies, including agent login, Interactive Voice Response (IVR) for call vectoring, outbound connection methods, and multi-channel agent interactions.	Enterprise contact centers operate on a dedicated Unified CM cluster that is trunked to the enterprise Unified CM cluster.
Contact Center Express (CCX)	Provides dial-by-name and a subset of Contact Center ideal for small contact centers or internal use.	Communicates through JTAPI to Unified CM.
TelePresence Content Server (TCS)	Provides video, audio, and content recording functionality that can be included in scheduled calls through a check-box in TMS or dialed, allowing any endpoint to easily be a recording station.	TCS registers with Cisco TelePresence Video Communication Server (VCS) Control for call control and connects to Unified CM devices through a SIP trunk between Unified CM and VCS Control.
Show and Share	Provides an internal stored video content portal.	TCS automatically uploads content to Show and Share. No other integration to call control is required.
Prime Collaboration Provisioning	Provides an administrative portal for "Day 2" operations.	Standalone software that communicates through SSH and HTTPS interfaces of infrastructure devices and endpoints.

Table 5-23 Additional Cisco Applications for the Preferred Architecture (continued)

Application Name	Functions	Integration Method
Prime Collaboration Assurance	Provides quality and fault detection services for collaboration deployment administrator	Stand alone software that communicates through SSH and HTTPS interfaces of infrastructure devices and endpoints
Prime Collaboration Analytics	Provides up to one year of usage data for usage and fault trend analysis by the collaboration deployment administrator.	Deployed with Prime Collaboration Assurance and utilizes data collected by that application.
Attendant Console	Gives corporate operators or receptionists a desktop application to handle incoming calls.	Standard version installs on the end user's Windows computer and connects to Unified CM. Advanced version runs on a dedicated server, and the end users log into the application.
MediaSense	Provides recording for both full-time and selective recording scenarios in Unified CM.	Recording Profiles are configured in Unified CM, and MediaSense is connected to Unified CM and Cisco Unified Border Element through SIP trunks.
Jabber Guest	Provides click-to-connect functionality for business-to-consumer (B2C) collaboration.	Requires a dedicated Expressway-C and Expressway-E pair, using a distinct domain from the enterprise Expressway-C and Expressway-E implementation used for Mobile and Remote Access and business-to-business video calls. Unified CM has SIP trunks to this dedicated Expressway pair.