Conferencing

Revised: February 19, 2019

This chapter describes the components and deployment of video and audio conferencing in an enterprise deployment. The chapter describes the Architecture for conferencing and then outlines the major tasks involved in the Conferencing Deployment Process.

Each major task of the Conferencing Deployment Process starts with an *Overview* section listing the steps required for that task, followed by a section on the important *Deployment Considerations* for that task, and then a section (or sections) detailing the deployment tasks listed in the *Overview* section.

What's New in This Chapter

Table 3-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 3-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:	Revision Date
Cisco Meeting Management	Various sections throughout this chapter	January 23, 2019
Maximum number of conference participants	Scaling the Conferencing Solution, page 3-15	August 30, 2017

Core Components

The core architecture contains these key conferencing elements:

- Cisco Meeting Server for audio and video conferencing as well as conference resource management
- Cisco TelePresence Management Suite (TMS) for conference provisioning, monitoring, and scheduling
- Cisco TelePresence Management Suite Extension for Microsoft Exchange (TMSXE) for interfacing with Microsoft Exchange room and resource calendars
- Cisco Meeting Management for monitoring and managing meetings

In addition, Cisco TMS architecture includes these non-Cisco components:

- Microsoft SQL database
- Microsoft Active Directory
- Microsoft Exchange or Microsoft Office 365
- Network load balancer

Key Benefits

- Simplified and optimized conferencing user experiences with all device types
- Flexible, extendable architecture that supports deployment of one or more permanent, scheduled, and/or instant conference resources
- High availability of conference resources and processes
- Resilience in the video network
- A single tool for hosts to schedule participants and conference rooms for a meeting
- Multiparty licensing enables full access to all conference resources on the bridge
- White glove service to monitor and manage meetings on a single interface

Conference Types

The conferencing solution supports the conference types and conferencing features listed in Table 3-2.

Table 3-2 Types of Conferences

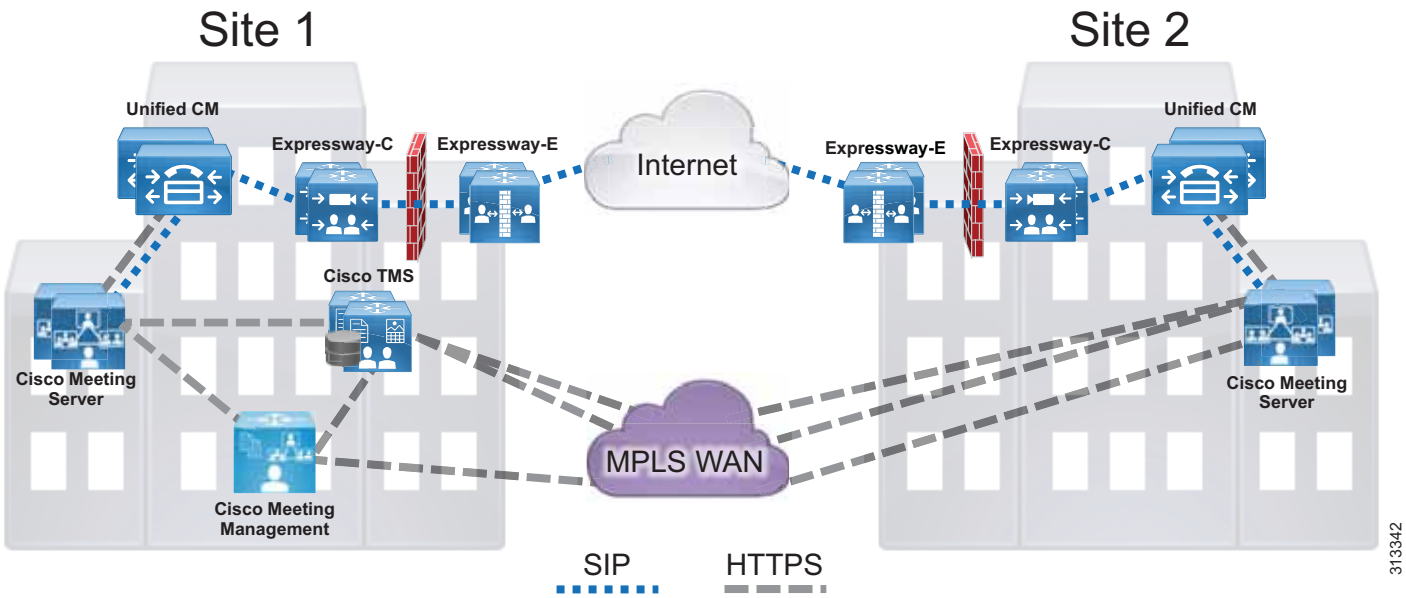
Conference Type	Description
Instant conferences	Manually escalated from a point-to-point call hosted on Unified CM, to a three-party call hosted on a conference bridge. (Also referred to as ad hoc conference.) Instant conferences are not scheduled or arranged prior to the conference.
Permanent conferences	Predefined addresses that allow conferencing without previous scheduling. The conference host shares the address with other users, who can call in to that address at any time. (Also referred to as meet-me, static, or rendezvous conferences.) Permanent conferences covered in this chapter use Cisco Meeting Server Spaces. Spaces can be user based and are provisioned from Cisco Meeting Server for items such as conference name, layouts, and PIN. Spaces can be created by importing users, API, or manually.
Scheduled conferences	Conferences booked via Cisco TMS and/or integration using Cisco TMS with a start and end time, optionally with a predefined set of participants.

Architecture

The conferencing architecture consists of Cisco Meeting Server for bridge resources as well as resource management; Cisco TelePresence Management Suite (TMS) for resource provisioning and scheduling; Cisco Meeting Management for conference monitoring and meeting management; and Cisco Unified Communications Manager (Unified CM) for call processing. SIP call control is used exclusively in this architecture. Use Cisco Meeting Server as the conference bridges for all conference types, and SIP trunks to connect the Cisco Meeting Server with Unified CM (Figure 3-1).

Unified CM communicates with Cisco Meeting Server using XML-RPC over HTTPS to control the conference bridges for instant conferences. Cisco TMS uses the REST API connections to link to the Cisco Meeting Server for provisioning and scheduling conference resources. Cisco Meeting Management and Cisco Meeting Server are connected via REST API, Event subscription, and Call Detail Record (CDR) interfaces to perform meeting management functions. Also, Cisco Meeting Management uses the TMS Booking API to connect with Cisco TMS to manage scheduled meetings. (Figure 3-1)

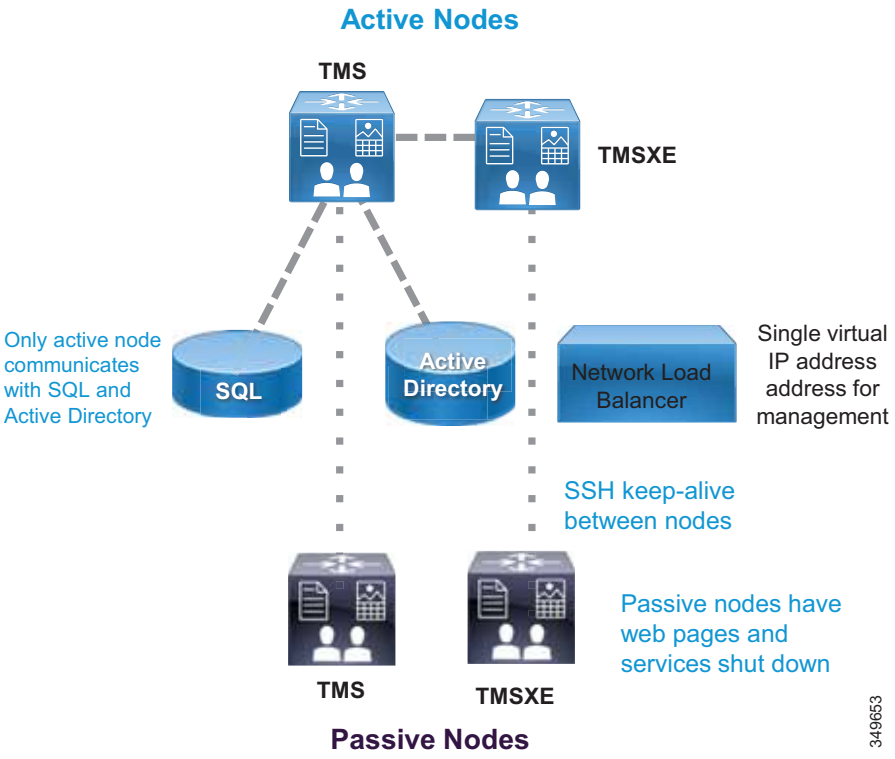
Figure 3-1 Architecture Overview



For licensing, use and install multiparty licenses along with other feature licenses onto each Cisco Meeting Server. By default, all users in the system use Shared Multiparty plus (SMP+); and if Personal Multiparty plus (PMP+) is desired, PMP+ should be assigned to users via the Cisco Meeting Server API.

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. The active node processes the incoming requests, while the passive node runs in standby mode with its web pages and services locked down and refusing all incoming traffic. For large Cisco TMS deployments (see the Sizing chapter), Cisco TMS and TMSXE must be installed on separate virtual machines, as indicated in Figure 3-2. TMS servers are installed in the customer data center that also hosts the organization's SQL deployment. All the server nodes function from an external Microsoft SQL database. Additionally, endpoints, Cisco Meeting Server, and Unified CM are involved in a successful scheduled conference. (Figure 3-2)

Figure 3-2 High-Level View of the Scheduling Architecture



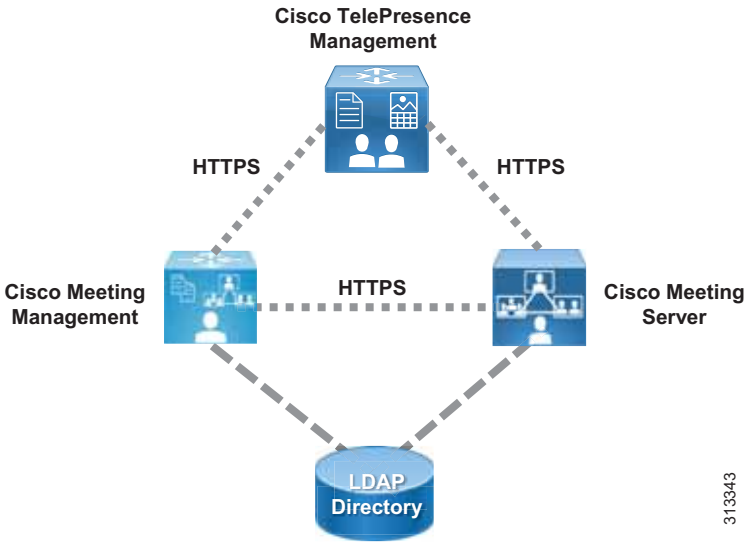
Cisco Meeting Management runs on a separate server outside of Cisco Meeting Server and is dedicated for Cisco Meeting Server deployment only. Cisco Meeting Management users reside in the LDAP directory that it utilizes for user authentication and for determining user roles. Cisco Meeting Management uses the Event subscription interface and REST API to perform meeting management functions on Cisco Meeting Server. Cisco Meeting Management configures itself as the CDR receiver on Cisco Meeting Server to receive call related events so that it knows when a meeting has started or ended along with other call activities. Cisco Meeting Management uses the TMS Booking API to retrieve information on upcoming scheduled meetings from Cisco TMS. (Figure 3-3)

For compatible versions of Cisco Meeting Server and TMS, refer to the latest version of the *Cisco Meeting Management Installation and Configuration Guide*, available at

https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-installation-guides-list.html

Note Cisco Meeting Management requires no extra license other than properly licensed Cisco Meeting Server instance(s).

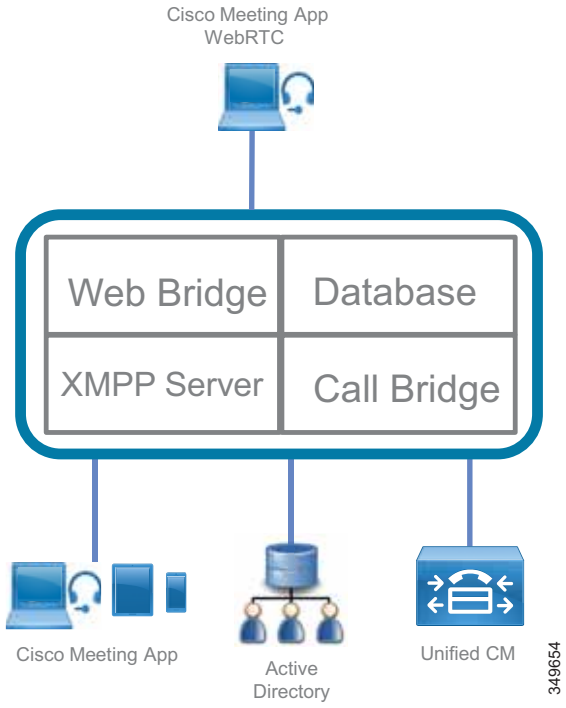
Figure 3-3 Cisco Meeting Management Architecture



Role of Cisco Meeting Server

Cisco Meeting Server consists of multiple components that provide video conferencing capability (Figure 3-4) and can handle conferences of all types. The call bridge component integrates with Unified CM for call control and provides resources to perform conference functions. All Cisco Meeting Server conferences are hosted on the Spaces. Spaces are virtual meeting rooms that have audio, video, and content sharing capability and are accessible using the Space URI or directory number. Cisco Meeting Server must integrate with a directory server such as Microsoft Active Directory to import users into the system. During the import process, Spaces will be created using the field mapping expressions configuration. All the information for users and Spaces is stored in the database. Participants can join conferences using Cisco or third-party standard video endpoints, Cisco Jabber client, or the Cisco Meeting App. The XMPP server authenticates users logging in through the Cisco Meeting App. The Web Bridge connects WebRTC client users to the call bridge after they log in.

Figure 3-4 Components Inside Cisco Meeting Server



Note Not all Cisco Meeting Server components are shown in Figure 3-4, but only components relevant to the Enterprise Collaboration Preferred Architecture are shown.

Cisco Meeting App is the client to Cisco Meeting Server, and it can be a native desktop or mobile application or a WebRTC browser application. With Cisco Meeting App, users can log in and join the conference with audio and video along with content sharing. With the WebRTC client, users without an account in Cisco Meeting Server can join the conference as a guest. In addition, users can use Cisco Meeting App to run their meetings and perform actions such as view participants, mute and remove participants, start and stop recording, as well as create and edit their own Spaces.

Note Cisco Meeting App can be deployed inside or outside of the enterprise network to join a conference, but only deployment inside the enterprise network is covered in this Enterprise Collaboration Preferred Architecture. For deployment outside of the enterprise network, refer to the latest version of the Cisco Meeting Server configuration guides available at https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html.

Using Cisco Meeting Server for conferences has several benefits, including:

- Scaling easily for small or large deployments, allowing capacity to be added incrementally as needed
- Simplified, intuitive, and optimal conference experiences across all device types
- Unrestricted number of participants in a meeting up to the limit of available underlying hardware when using multiparty licensing
- Single deployment model for all conference types

Role of Cisco TMS

Cisco TMS provides conference scheduling as well as conference room system reservation. Unified CM maintains the configuration control for endpoints, and TMS is then able to push the calendar information 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.

Role of 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.

Role of Cisco Meeting Management

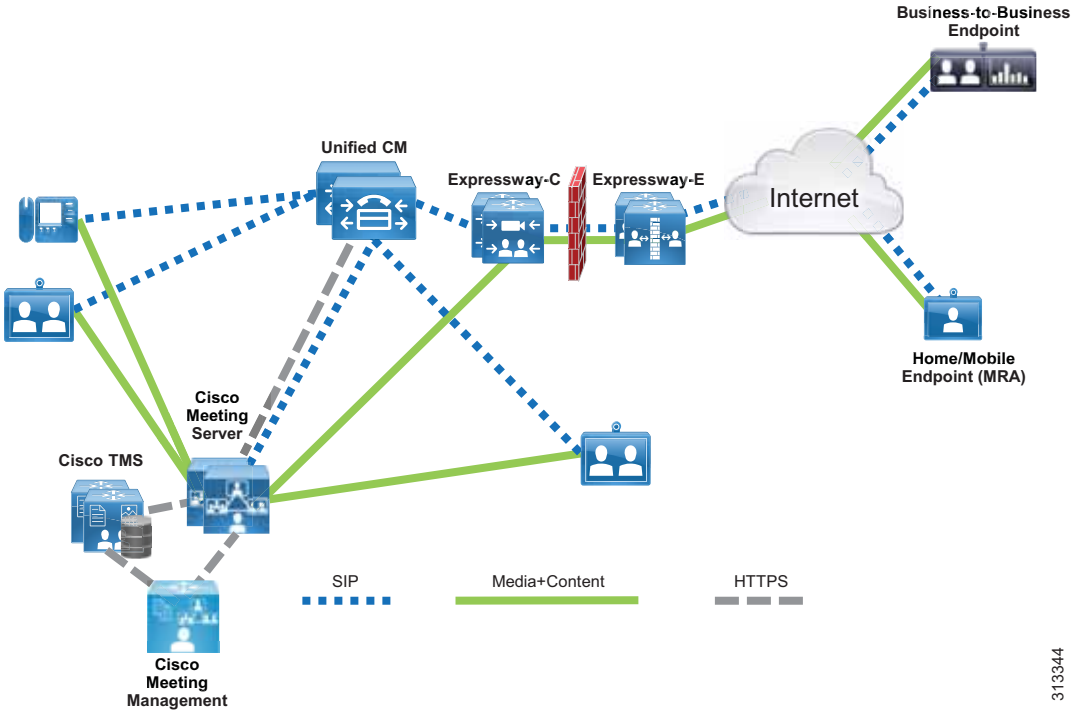
Cisco Meeting Management and Cisco TMS work together to provide the complete management functions for Cisco Meeting Sever. Meeting Management can provide white glove service for customers, and it allows operators to see a list of active meetings, meetings in the past (up to 7 days ago), or upcoming meetings (up to 24 hours ahead). Furthermore, operators can view detailed information about individual meetings, such as participants, meeting duration, and meeting start time. For active meetings, operators can perform meeting management functions such as start/stop recording or streaming, change layout, add/drop participants or end the meeting, and see who is the active speaker. On the individual participant level, operators can mute/unmute audio/video, change layout, set/unset importance, or display call statistics for the participant.

Users in Cisco Meeting Management belong to one of the user groups, Administrator or Video Operator. Each user group maps to an LDAP group defined inside the directory with users assigned to it. When users log into the portal, Meeting Management authenticates them using the directory and determines their group membership. Administrators have full access to all functions in the Cisco Meeting Management portal. Video Operators only have access to the meeting monitoring and management as well as system status checking functions in the Cisco Meeting Management portal.

Deployment Overview

The standard deployment uses multiple Unified CM nodes for call control. Cisco Meeting Server connects to Unified CM with SIP trunks to manage conference resources and to bridge calls. (Figure 3-5) Cisco TMS and Cisco Meeting Management provide conference management facilities and scheduling. The same conferencing infrastructure is used for both non-scheduled and scheduled conferencing. Cisco Expressway provides the firewall traversal capability to enable business-to-business and mobile and remote access (MRA) calling into the local enterprise. These elements together provide voice and video conferencing for the local enterprise.

Figure 3-5 Standard Deployment



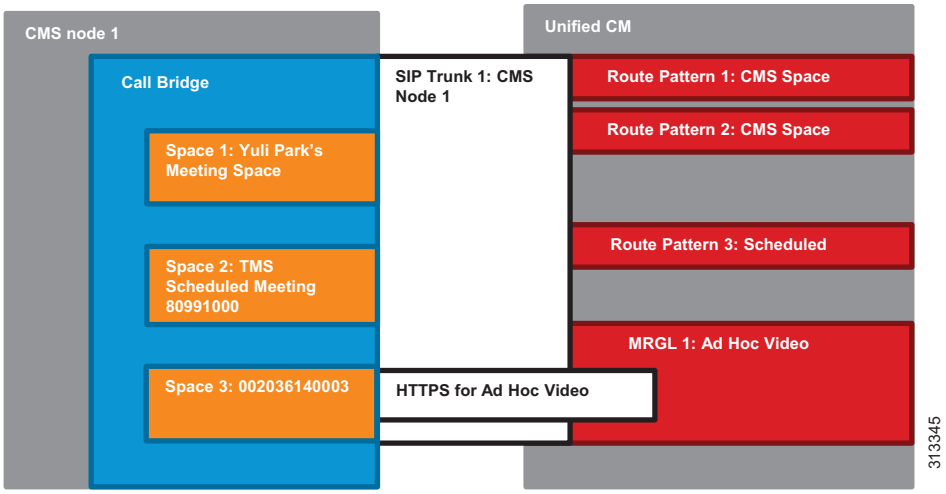
Requirements and Recommendations

- Early Offer messaging is recommended for all SIP trunks connected to Unified CM that carry TelePresence calls.
- Use a single SIP trunk for all conference types (instant, permanent, and scheduled) with Cisco Meeting Server.
- Configure Multiparty License in Cisco Meeting Server to host conferences.

Conference Call Flows

Unified CM provides device registration and routing of voice and video calls between the connected endpoints. Permanent, instant, and scheduled conference calls are all routed over a single SIP trunk to the call bridge on Cisco Meeting Server. Each call bridge requires a separate SIP trunk. An HTTPS connection is configured on the Unified CM node that carries the XML-RPC requests to the Cisco Meeting Server nodes for instant conferences (see Figure 3-6). When users press the conference softkey on the device to escalate a two-party to three-party call, Unified CM sends an API request to Cisco Meeting Server to create a temporary Space for hosting the conference via this HTTPS connection. Instant, permanent, and scheduled conferences are hosted on Spaces that are created by different components. For more information on Spaces, see section 5. Deploy Cisco Meeting Server Spaces.

Figure 3-6 Unified CM and Cisco Meeting Server SIP Trunk



Instant call flows that are managed by Unified CM cannot be used to add participants to conferences created by any other method, such as scheduled conferences. Other call flows cannot be used to add participants to instant conferences. The instant call escalation method is supported only in an instant conference that was created by it, and conferences generated by other methods cannot be extended by the instant mechanism. This avoids any potential for chained conferences.

Instant Conferences

Instant conferences use an HTTPS XML-RPC connection associated with the SIP trunk between Unified CM and the call bridge on Cisco Meeting Server. When a user presses the conference softkey to initiate an instant conference, Unified CM issues an API request through the HTTPS connection to create a temporary Space on Cisco Meeting Server. Unified CM then routes all the participants to that Space through the SIP trunk. When the conference is done, Unified CM issues another API request to delete that Space from Cisco Meeting Server.

Permanent Conferences with Cisco Meeting Server Spaces

Permanent conferences are deployed using Cisco Meeting Server Spaces. Spaces provide a permanent-type conference and are created as part of the users import process from LDAP. Users can dial the Space URI at any time to start a meeting. Administrators can specify the Space's attributes (for example, name, username, URIs, and so forth) through the field mappings so that the Spaces can be created using those mappings. Users can then log in using Cisco Meeting App and add members to their Space. Connect a SIP trunk between Unified CM and the call bridge on Cisco Meeting Server for this conference type. The same SIP trunk is used for other conference types to route conference participants to the Space.

Scheduled Conferences

This solution supports scheduling of conferences on Cisco Meeting Server, and scheduling is performed with Cisco TMS. Scheduled conferences require a SIP trunk between Unified CM and the call bridge on Cisco Meeting Server. Again the same SIP trunk is used as with other conference types, and Unified CM routes the scheduled conference participants to the destination of the SIP trunk. Add Cisco Meeting Server to Cisco TMS to allow for issuing REST API requests on Cisco Meeting Server through the HTTPS connection. After configuring a range of numeric IDs for scheduled conferences, Cisco TMS creates an inactive Space on Cisco Meeting Server for each numeric ID via the API link. Cisco TMS will then randomly chooses a dial-in number from the range when an organizer schedules a meeting. When it is time to start the scheduled meeting, Cisco TMS activates the Space using the API, and participants can start calling in.

Third-Party Endpoints

Endpoints from other equipment providers can participate in any conferences using standard SIP. Only endpoints registered to Unified CM that support the conference button can initiate an instant conference. Cisco Expressway or Cisco VCS can be used to interwork H.323 calls to SIP, allowing H.323 endpoints to join conferences.

High Availability for Conferencing

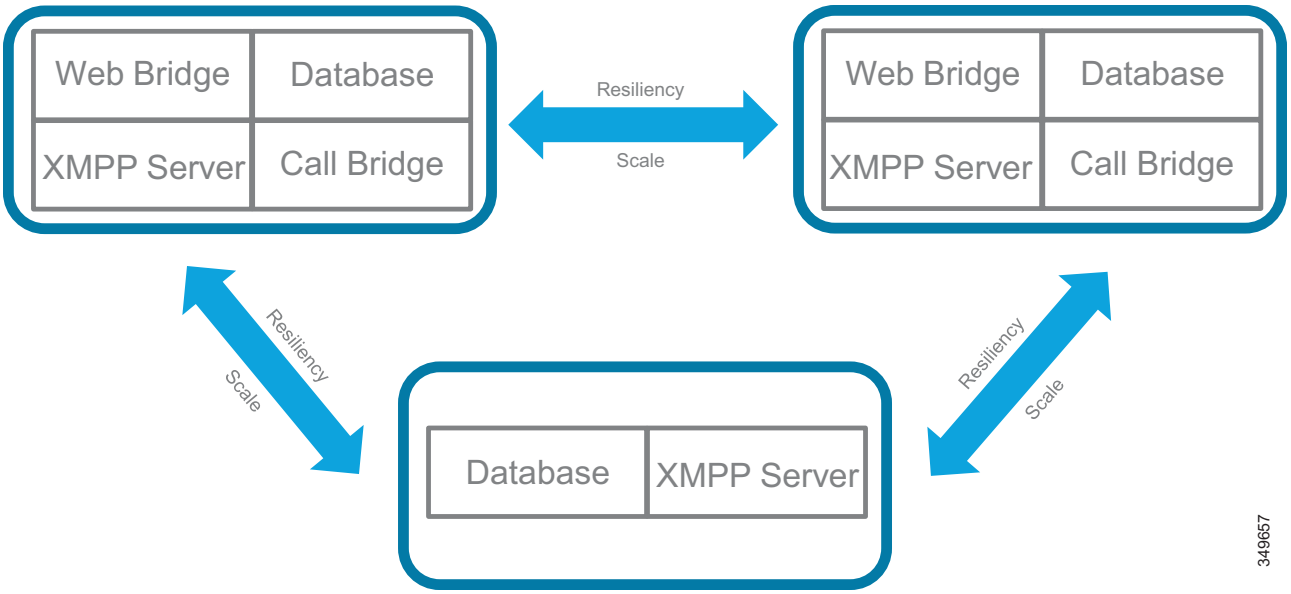
High availability must be considered at several levels with the conferencing solution and is achieved in different ways depending on the service being considered.

For both scheduled and non-scheduled conferences, high availability involves Cisco Unified CM, Cisco Meeting Server, and Cisco TMS.

Cisco Meeting Server High Availability

Deploying additional instances of components on one or more servers can provide resiliency for Cisco Meeting Server so that the component instances can share the load, and if one of them fails, the backup instance would pick up the load. In addition, XMPP servers, call bridges and databases can be clustered together to operate as a single instance. See Figure 3-7.

Figure 3-7 Minimum Configuration for Cisco Meeting Server Cluster with High Availability



A standard Cisco Meeting Server cluster consists of two or more (up to 8) nodes with call bridge service enabled. Maximum round trip time (RTT) between call bridges is 300 ms. Call bridge cluster peers are connected to each other in full mesh via the distribution link. This link is an HTTPS connection used for passing call signaling and control status messages between call bridges. Calls can be sent to any call bridges in the cluster. If one call bridge goes down, Unified CM can route calls to the remaining call bridges to join the conferences. In the event that a call bridge fails during a live conference, those calls will be dropped and participants will need to dial the same number to join the conference on a new call bridge. Using the Unified CM route group and route list construct, calls can be distributed through the SIP trunks to Cisco Meeting Server.

Call bridges that are configured as a cluster can be put into one or more call bridge groups. For call bridges within the group, Cisco Meeting Server can intelligently load-balance calls across them and send calls for the same conference to the same call bridge whenever possible. When a call is sent to a call bridge, Cisco Meeting Server decides to reject or accept the call based on the current load in the call bridge. If the current load is less than the preset threshold, the call will be accepted. Otherwise, the call will be rejected and Unified CM will reroute the call to another call bridge in the call bridge group using the dial plan configuration. If Unified CM cannot find any call bridge that accepts the call, the whole call will be rejected. After a Cisco Meeting Server accepts the call, the call could be hosted on the call bridge of this Cisco Meeting Server or moved to another call bridge with highest priority according to an internal ordered list for the conference. When the call is moved, the target Cisco Meeting Server with the call bridge enabled sends an INVITE with Replaces to Unified CM to take over the call. By default, a call bridge in a call bridge group will reject all calls for new participants at 80% load, and only new distribution calls will be allowed. For network requirements between call bridges, RTT should be 100 ms or less between call bridges inside the group and 300 ms or less between any two call bridges in the same cluster.

Note If call bridge groups and load balancing are not used, then calls will not be rejected, but the quality of all calls will be reduced when the load limit is reached. If this happens often, we recommend deploying additional hardware.

The database cluster consists of one master and multiple slaves, up to a maximum of 5 nodes with maximum RTT of 200 ms between databases. The database master can perform both read and write operations, while slaves can only do reads. Call bridges always connect to the database master for read and write, and all changes made on the master are replicated to the slaves. Call bridges with a local database automatically connect to the master of the local database cluster, while call bridges with no local database have to be connected manually to the database cluster. If the master fails, one of the slaves will become the new master, and other slaves will re-register with this new master. After correcting the failure, the old master will become the slave and register with the new master. In cases where a network partition occurs, only database nodes that can see more than half of the cluster members are considered for promotion to become a master. Likewise, any existing master that cannot see more than half of the cluster members will be demoted to a slave. This ensures that multiple masters are not created. So, if a database cluster consists of an even number (2 or 4) of nodes and the network is partitioned into 2 segments with an equal number of nodes are on each side, the master on one side will be demoted to a slave since it cannot see more than half of the cluster members. In that case, there will be no master in the cluster, and the call bridges can still take calls but no database write operations are possible. For this reason, we recommend having an odd number of nodes in the database cluster to ensure that a master is always elected. As a result, the minimum number of database nodes in a cluster is 3.

XMPP resiliency provides failover protection for a client that is unable to reach a specific XMPP server. The XMPP server cluster must be configured using an odd number of XMPP server nodes, with a minimum of 3. This is due to the master election algorithm requirement that more than half of the cluster nodes should be available in order for Cisco Meeting Server to elect an XMPP server master. If no XMPP server master is available in the cluster, Cisco Meeting App users cannot log in. Each XMPP server knows the location of the others, with links established between them. They use keep-alive messages to monitor each other and elect a master. XMPP messages can be sent to any server and are forwarded to the master XMPP server. If the master fails, a new master is elected and the other XMPP servers will forward messages to the new master. The call bridge uses the DNS SRV record (_xmpp-component) to connect with an available XMPP server based on the configured priority and weight with the SRV record. A call bridge connects to one XMPP server at a time. If a network problem results in the call bridge losing connection to the XMPP server, the call bridge will attempt to reconnect to another XMPP server. All call bridges must be configured inside each XMPP server.

Figure 3-7 illustrates the minimum configuration for a Cisco Meeting Server cluster with high availability. In this configuration, a minimum of 3 servers is required to host 3 instances of the database and XMPP servers. Enable at least 2 instances of each component service (Web Bridge and Call Bridge) in separate servers, and put the call bridges into a group. There is no need to activate all services inside each server; activate only the ones that are required. If the deployment requires more capacity than the 2 call bridges can handle, additional call bridge can be set up in the third server (no need to acquire a fourth server for just the call bridge). Table 3-3 lists the minimum Cisco Meeting Server cluster configuration required for various numbers of call bridges for a single Unified CM cluster.

Table 3-3 Minimum Cisco Meeting Server Cluster Configuration for Various Numbers of Call Bridges for a Single Unified CM Cluster

Call Bridge Group	Number of Call Bridges	Cisco Meeting Server Cluster Configuration
A	2	Node A1: Web Bridge, Call Bridge, Database, XMPP Node A2: Web Bridge, Call Bridge, Database, XMPP Node A3: XMPP, Database
	3	Node A1: Web Bridge, Call Bridge, Database, XMPP Node A2: Web Bridge, Call Bridge, Database, XMPP Node A3: Call Bridge, Database, XMPP
	4	Node A1: Web Bridge, Call Bridge, Database, XMPP Node A2: Web Bridge, Call Bridge, Database, XMPP Node A3: Call Bridge, Database, XMPP Node A4: Call Bridge
	5	Node A1: Web Bridge, Call Bridge, Database, XMPP Node A2: Web Bridge, Call Bridge, Database, XMPP Node A3: Call Bridge, Database, XMPP Node A4: Call Bridge Node A5: Call Bridge

TMS High Availability

High availability of a large Cisco TMS deployment includes: Two TMS front-end servers, two servers running TMSXE, a network load balancer, and an external Microsoft SQL database (see Figure 3-2). 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. The network load balancer (NLB) is deployed in front of the TMS servers. Inbound traffic to TMS goes through the NLB, which forwards it to the active node. Outbound traffic from TMS is sent directly to the destination without going through the NLB. If the NLB detects a failure on the existing active node, it automatically switches to the new active node without any user intervention.

Cisco Meeting Management High Availability

Cisco Meeting Management does not have the built-in cluster function for resiliency. For high availability, customers can configure two independent Cisco Meeting Management instances with identical configurations, and both instances should connect to the same Cisco Meeting Servers and Cisco TMS. Then put a network load balancer in front of the Cisco Meeting Management instances, and users can connect to the Cisco Meeting Management portal through the load balancer. The load balancer configuration and availability of the Cisco Meeting Management servers will determine which one of the Cisco Meeting Management servers users connect to.

Security for Conferencing

The Preferred Architecture fully supports media and signaling encryption; but for simplicity, the solution presented in this document implements non-secure SIP trunks between Unified CM and Cisco Meeting Server for all conferences. An exception to this is the solution requirement that API communications between unified CM and the Cisco Meeting Server must be encrypted, and therefore HTTPS must be used in this case.

Cisco Meeting Server uses secure connections to communicate with external components as well as between internal components, and certificates are required. Use certificate authority (CA) signed certificates to secure the connections between components. Refer to the Security chapter for further detail.

Another level of security can be added to restrict access to the conferences themselves with PINs or passwords. Any scheduled conference or permanent conference can have a PIN set so that all participants are challenged to enter the PIN before being allowed to connect.

Scaling the Conferencing Solution

You can scale the conferencing solution primarily by adding more call bridges (up to 8) to a standard Cisco Meeting Server cluster.

In this deployment, based on the dial plan and route group and route list configuration with the SIP trunks in Unified CM, calls can be routed to any call bridge within the cluster. If calls for the same conference are routed to different call bridges, the audio and video of the last 4 active speakers are exchanged between call bridges for participants on one bridge to see the active speakers on the other bridge.

Note Cisco Meeting Server supports clustering with more than 8 call bridges, but deployment requires prior approval by Cisco. Contact your local Cisco account team for details.

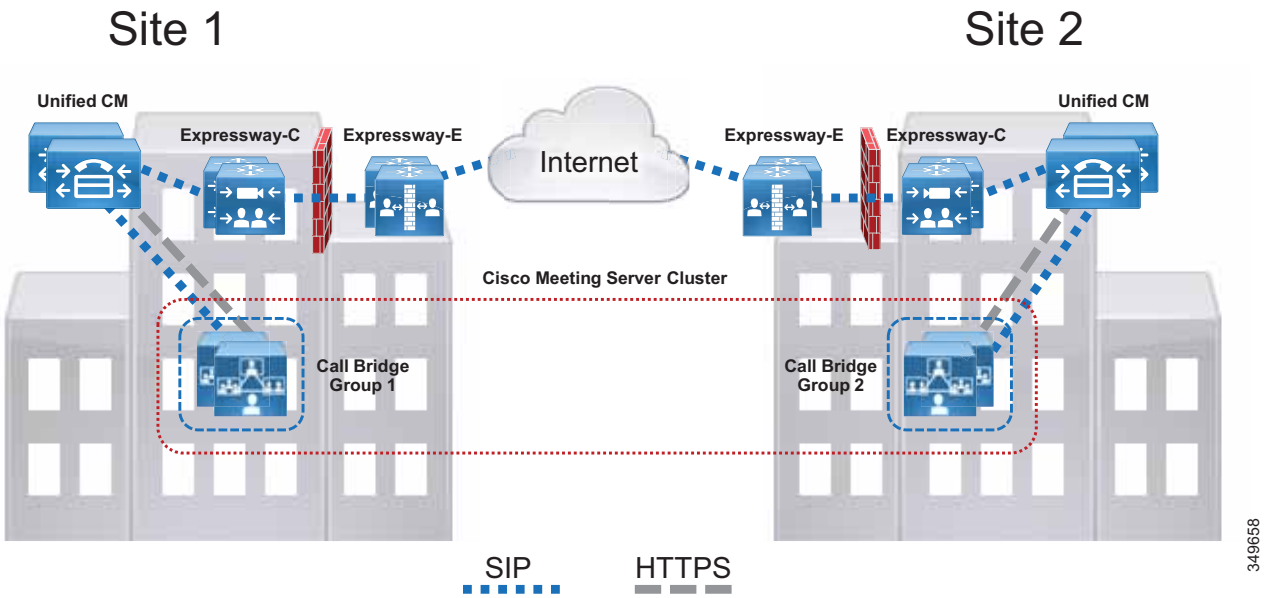
Each call bridge can support 450 participants. Thus, the maximum number of participants per conference is 450 with a single server, and up to 2,600 participants can be supported across multiple servers in a single cluster.

Considerations for Multiple Unified CM Clusters

For large-scale deployments with multiple Unified CM clusters, use a single Cisco Meeting Server cluster configured with multiple call bridge groups, and dedicate one group to each Unified CM cluster.

For example, if your deployment has three Unified CM clusters, then you should deploy a single Cisco Meeting Server cluster with three call bridge groups, one in each Unified CM cluster. Each Unified CM cluster should have a SIP trunk to each call bridge in its local call bridge group. All incoming conference calls to a Unified CM cluster will be handled by the local call bridge group. Call bridges should have their distribution links connected to their peers inside and outside of the groups in full mesh. For the same conference, users can dial in from their Unified CM cluster to reach the local call bridge group, and the call bridges in different groups will exchange the audio and video of the last 4 active speakers with their peers so that participants can see each other across the bridges. (Figure 3-8)

Figure 3-8 Cisco Meeting Server Deployment with Multiple Unified CM Clusters



For the first Unified CM cluster, refer to the section on Cisco Meeting Server High Availability and Table 3-3 for the design.

For the second Unified CM cluster, expand the Cisco Meeting Server cluster to add 2 extra servers. In each of the servers, enable the web bridge and call bridge. No extra database or XMPP services are required for this Unified CM cluster. Connect the call bridges to the existing database cluster, and add all additional call bridges to the XMPP cluster. Put the call bridges into a new call bridge group that is used by this second Unified CM cluster, and associate the web bridges with this call bridge group. If additional capacity is desired, add an extra server to host a call bridge, and put that call bridge into the call bridge group for this second Unified CM cluster. Table 3-4 illustrates the additional Cisco Meeting Server cluster configuration required for the second Unified CM cluster, based upon the number of additional call bridges required.

Table 3-4 Additional Cisco Meeting Server Node Configuration for the Second Unified CM Cluster

Call Bridge Group	Number of Additional Call Bridges	Additional Cisco Meeting Server Node Configuration
B	2	Node B1: Web Bridge, Call Bridge Node B2: Web Bridge, Call Bridge
	3	Node B1: Web Bridge, Call Bridge Node B2: Web Bridge, Call Bridge Node B3: Call Bridge
	4	Node B1: Web Bridge, Call Bridge Node B2: Web Bridge, Call Bridge Node B3: Call Bridge Node B4: Call Bridge

For the third Unified CM cluster, expand the Cisco Meeting Server cluster to have 2 extra servers. In each of the servers, enable the web bridge and call bridge. Connect the call bridges to the existing database cluster, and add all additional call bridges to the XMPP cluster. Put the call bridges into a new call bridge group that is used by this third Unified CM cluster, and associate the web bridges with this call bridge group. If additional capacity is desired, add an extra server to host a call bridge, and put that call bridge into the call bridge group for this third Unified CM cluster. Table 3-5 illustrates the additional Cisco Meeting Server node configuration required for the third Unified CM cluster, based upon the number of additional call bridges required.

Table 3-5 Additional Cisco Meeting Server Node Configuration for the Third Unified CM Cluster

Call Bridge Group	Number of Additional Call Bridges	Additional Cisco Meeting Server Node Configuration
C	2	Node C1: Web Bridge, Call Bridge Node C2: Web Bridge, Call Bridge
	3	Node C1: Web Bridge, Call Bridge Node C2: Web Bridge, Call Bridge Node C3: Call Bridge
	4	Node C1: Web Bridge, Call Bridge Node C2: Web Bridge, Call Bridge Node C3: Call Bridge Node C4: Call Bridge

With three Unified CM clusters and thus three separate call bridge groups, the three XMPP and database cluster nodes local to the first call bridge group can be distributed among the call bridge groups so that each call bridge group would have a local XMPP and database cluster node. By migrating two of the

XMPP and database cluster nodes local to the first call bridge group to the second and third call bridge groups, respectively, this creates redundancy for the XMPP and database services across each call bridge group. Table 3-6 illustrates this new Cisco Meeting Server cluster configuration.

Table 3-6 Migrating XMPP and Database Services to Second and Third Call Bridge Group

Call Bridge Group	Cisco Meeting Server Cluster Configuration
A (Unified CM Cluster 1)	Node A1: Web Bridge, Call Bridge, Database, XMPP Node A2: Web Bridge, Call Bridge
B (Unified CM Cluster 2)	Node B1: Web Bridge, Call Bridge, Database, XMPP Node B2: Web Bridge, Call Bridge
C (Unified CM Cluster 3)	Node C1: Web Bridge, Call Bridge, Database, XMPP Node C2: Web Bridge, Call Bridge

If the deployment requires a fourth Unified CM cluster, we recommend moving to a Cisco Unified CM Session Management Edition design, which is out of the scope for this document.

The following guidelines apply when expanding the Cisco Meeting Server cluster into different regions for multiple Unified CM clusters:

- A single Cisco Meeting Server cluster should be used for deployment of one or more Unified CM clusters.
- You may deploy up to 8 call bridges for the standard Cisco Meeting Server cluster. If the cluster exceeds 8 call bridges, acquire Cisco account team approval before deployment.
- Deploy a maximum of 5 databases and an odd number of nodes in the Cisco Meeting Server cluster.
- Deploy an odd number of XMPP service nodes in the Cisco Meeting Server cluster.
- Round-trip-time (RTT) network requirements:
  - Maximum of 300 ms between call bridges and 200 ms between databases in the Cisco Meeting Server cluster
  - Maximum of 100 ms between call bridges inside the group

Conferencing Deployment Process

To deploy the conferencing solution, perform the following major tasks in the order listed here:

1. Plan the Conferencing Deployment
2. Deploy Cisco Meeting Servers
3. Enable Unified CM for Conferences
4. Deploy Cisco TelePresence Management Suite
5. Deploy Cisco Meeting Server Spaces
6. Deploy Cisco Meeting Management

1. Plan the Conferencing Deployment

Before deploying the conferencing solution, plan for the following aspects:

Requirements

- Configure DNS for Cisco Meeting Server, which needs a number of DNS SRV and A records. For example, Cisco Meeting App uses the _xmpp-client SRV record to look up the XMPP service for user authentication.
- Cisco Meeting Server requires the use of an API to complete the deployment. Acquire a tool that can be used to issue REST API commands for an update; for example, Postman (https://www.getpostman.com/).

Licensing

Licenses must be installed on various products:

- Cisco TMS must have enough device licenses installed for the deployment.
- Cisco Meeting Server must have enough Multiparty licenses installed on each node running the call bridge.

Multiparty is a user-based licensing model recommended for Cisco Meeting Server deployment, and it should be applied to every node with call bridge service enabled. It comes with two variations: Personal and Shared. Personal Multiparty Plus (PMP+) is for specific named hosts while Shared Multiparty Plus (SMP+) is for conference room systems or for sharing between users. Each license entitles a user to host a conference with unlimited participants and up to 1080p video resolution. Table 3-7 summarizes the features included in the Personal and Shared Multiparty licenses.

Table 3-7 Cisco Personal and Shared Multiparty Plus License Features

Feature	Personal Multiparty Plus	Shared Multiparty Plus
Tied to a named host	Yes	No
Availability	Included in Cisco UWL Meetings	A la carte or discounted with room system
Minimum order	25	1
Maximum conference size	Unrestricted, within the limit of available hardware capacity	

Table 3-7 Cisco Personal and Shared Multiparty Plus License Features (continued)

Feature	Personal Multiparty Plus	Shared Multiparty Plus
Maximum resolution	1080p60 (full HD) for video and 1080p30 for content Single-screen or multi-screen endpoints	
Rich media sessions for business-to-business or business-to-customer	Included	Included
Cisco TMS, TMSXE, and Skype for Business and Lync Interoperability Licenses	Included	New customers buy with Starter Pack[1]
Support for instant, permanent, and scheduled conferences	Yes	Yes

1. If only the TMS and related product licenses are required, a TMS Starter Pack can be purchased.

Multiparty licensing is the license model used in the Preferred Architecture. For more information on Multiparty licenses, refer to *Cisco Multiparty Licensing At-a-Glance*, available at

https://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration/pervasive-conferencing/at-a-glance-c45-729835.pdf

Cisco TelePresence Management Suite

Before beginning the installation and configuration process, you must decide on several items to align with the specific structure and preferences of your organization. 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 3-8 lists the Microsoft SQL 2012 specifics required to support Cisco TMS and TMSXE.

Table 3-8 Microsoft SQL 2012 Specifics Required to Support Cisco TMS and TMSXE

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

Table 3-8 Microsoft SQL 2012 Specifics Required to Support Cisco TMS and TMSXE

Requirement	Parameter
Databases created	tmsng (CiscoTMS)
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 integrates with 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.

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 by end users through Outlook. For all possible settings of the default conference, refer to the latest version of the *Cisco TelePresence Management Suite Administrator Guide*, available at

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

Cisco Meeting Server Space Provisioning

An understanding of how the organization plans to utilize Cisco Meeting Server Spaces requires an understanding of the workflow that end users expect for meetings. Some organizations may choose to leverage the Spaces instead of scheduled resources for certain meeting types, especially in cases where workers are in separate locations and not able to gather in a common conference room.

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. Deploy Cisco Meeting Servers

This section describes the major tasks required to deploy Cisco Meeting Servers and prepare them for use with scheduled and non-scheduled conferences.

Overview

Deployment Tasks for Cisco Meeting Servers:

1. Install the Cisco Meeting Server feature license keys.
2. Generate enterprise CA signed certificates.
3. Configure the Web Admin, XMPP, call bridge, and web bridge services.
4. Set up an additional node for redundancy and configure clustering for XMPP, database, and call bridge.
5. Set up the outbound dial plan to send calls to the call bridge cluster peer for distributed conferences.
6. Create a call bridge group and add all call bridges to it for the Unified CM cluster.
7. Update the call settings parameters.

Deployment Considerations

The physical location of a Cisco Meeting Server is important to consider because media traffic flows between it and each participant in the conference. To provide the best experience for participants, centralize the location of the Cisco Meeting Server with call bridges and put them into a group for each regional Unified CM cluster.

If the deployment includes Cisco Meeting App or a web bridge, an XMPP server should be enabled and configured with an XMPP domain for user authentication. Avoid using the parent domain (for example, ent-pa.com) as the XMPP domain because other components such as Cisco Unified CM IM and Presence Service might have already used it, which could complicate the overall design. We recommend using a sub-domain such as cms.ent-pa.com as the XMPP domain for Cisco Meeting Server.

Deploy a 3-node cluster for XMPP server and database; this should cover a majority of deployment scenarios to provide resiliency and high availability.

Create a DNS A record using the same name (for example, join.ent-pa.com) for each web bridge so it is easy for participants to remember the web bridge URL (from example, https://join.ent-pa.com) used to join the conference.

Instant, Permanent, and Scheduled Conferences

Figure 3-9 Instant Conference Call Flow

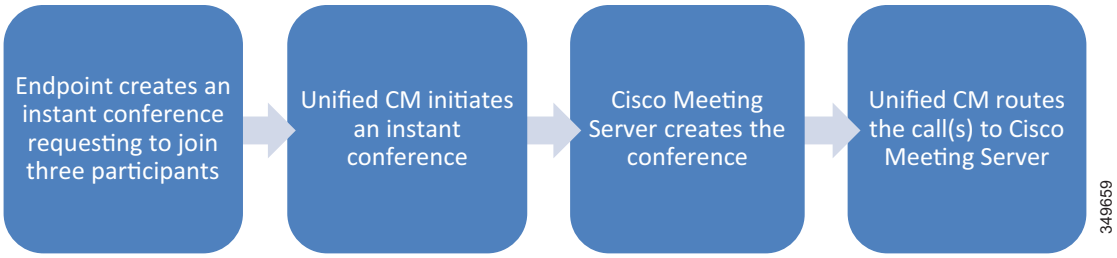
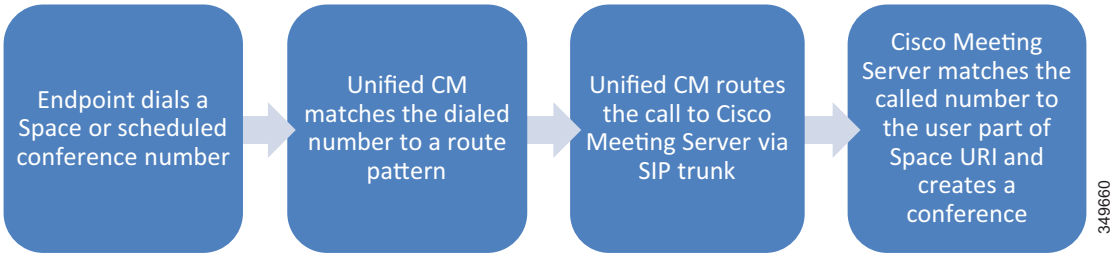


Figure 3-10 Permanent or Scheduled Conference Call Flow



Deployment Tasks for Cisco Meeting Servers

Cisco Meeting Server cannot take calls without a call bridge license. The call bridge, multiparty license along with other feature licenses are bundled into a single license file named **cms.lic**. Use any SFTP client software to upload the license file to every Cisco Meeting Server. The license file ties to the MAC address of the Cisco Meeting Server; be careful to upload the correct file to the corresponding server.

Go to the Cisco Meeting Server section of the Security chapter for details on how to generate the enterprise CA signed certificates. This will generate 2 certificates; one certificate that is shared for web admin, XMPP, call bridge, web bridge, and database cluster in any nodes, while the other certificate is used by any call bridge node without a local database to connect with the database cluster.

Skip if this is not a call bridge node:

For web admin, use the Mainboard Management Processor (MMP) commands to specify the listening interface and port, install the shared CA signed certificate, and enable the service. This allows the administrator to access the Web interface using the specified listening interface and port. By default, both web admin and web bridge use port 443. If they both use port 443, then they need to use different network interfaces. However, if the same interface is used, one of the services must have a different default port. In that case, we recommend changing the web admin default port to some other used port (for example, port 445).

For the call bridge, use MMP commands to specify the listening interface, install the shared CA signed certificate, and restart the service.

For the XMPP server, use MMP commands to specify the listening interface and XMPP domain (for example, cms.ent-pa.com), install the shared CA signed certificate, and enable the service. On the first XMPP server, add the required number of call bridges, and for each call bridge assign a unique name and write down the name and secret string generated. On the subsequent XMPP servers, add the required number of call bridges, using the call bridge names and secret strings generated on the first XMPP server.

Skip if this is not a call bridge node:

Go to the web interface (**Configuration** -> **General**) and configure the XMPP server settings using the values in Table 3-9.

Table 3-9 XMPP Server Settings for the First Call Bridge

Field Name	Value
Unique Call Bridge name	*<unique call bridge name>*
Domain	cms.ent-pa.com
Server address	leave blank
Shared secret	*<call bridge secret string>*

For web bridge, use MMP commands to specify the listening interface, install the shared CA signed certificate, enable trust for the call bridge certificate installed above, and enable the service. The web bridge connects to the call bridge after accepting the connection from the WebRTC client, and therefore it needs to trust the certificate from call bridge.

Repeat the steps above for every node in the cluster.

Set up the database cluster.

On each database node, use the MMP commands to specify the network interface used by the database, and install the shared CA signed certificate. Select one node as the master and run the MMP command to initialize the database. Go to each database slave node, and run the MMP command to join the database with the cluster. On all nodes that have the call bridge without a local database, install the second certificate and run the MMP command to connect to the cluster. Ensure that the command execution status is successful before moving on to the next command. This completes the database cluster setup.

Warning **Data in the slave database will be overwritten by the master after the slave joins the cluster.**

Setup the call bridge cluster.

On each call bridge node, go to the web interface (**Configuration** -> **Cluster**) and configure a Unique name (for example, callbridge1) under **Call Bridge identity** for the call bridge. After that, go back to the cluster configuration (**Configuration** -> **Cluster**) on one of the call bridge nodes, fill in the Clustered Call Bridges with the information for all call bridges, using the sample in Table 3-10, and leave other fields blank or as default:

Table 3-10 Clustered Call Bridges Configuration Example

Unique Name	Address	Comment
callbridge1	https://10.x.x.60:445	Address column is the URL and port number used to access the web interface
callbridge2	https://10.x.x.61:445	
callbridge3	https://10.x.x.62:445	

The Clustered Call Bridges configuration will appear in all call bridge nodes from the web interface. These are the distribution links used by the call bridges to pass call signal and status messages between peers for distributed conferences.

Use the API to set up outbound dial plan rules for sending calls to call bridge cluster peers for distributed conferences. Each call bridge should have an outbound dial plan rule configured for each of its peers so that it routes calls directly to its peer instead of through a call control. If there are 3 call bridges in the cluster, each call bridge should have 2 outbound dial plan rules configured, with a total of 6 outbound dial plan rules configured in the cluster. Use the GET method on the /callBridges node to retrieve the IDs of all call bridges in the Cisco Meeting Server cluster. Using the Clustered Call Bridges configuration example in Table 3-10, run the POST method on the /outboundDialPlanRules node using each row of Table 3-11 as the parameter settings.

Table 3-11 OutboundDialPlanRules Parameters Example

domain	priority	scope	trunkType	callBridge
10.x.x.61	100	callBridge	sip	<*callbridge1 ID*>
10.x.x.62	100	callBridge	sip	<*callbridge1 ID*>
10.x.x.60	100	callBridge	sip	<*callbridge2 ID*>
10.x.x.62	100	callBridge	sip	<*callbridge2 ID*>
10.x.x.60	100	callBridge	sip	<*callbridge3 ID*>
10.x.x.61	100	callBridge	sip	<*callbridge3 ID*>

For each web bridge deployed, the call bridge needs to know the URL for accessing the web bridge. Run the POST method on the /webBridges node using the URL parameter from each row in Table 3-12.

Table 3-12 Web Bridge Configuration Example

Web Bridge IP Address	URL
10.x.x.60	https://10.x.x.60
10.x.x.61	https://10.x.x.61

Set up the XMPP server cluster.

Select one node as the master, run the MMP commands to enable and initialize the cluster, and set up the cluster to trust the shared CA signed certificate. On the remaining XMPP servers, run the MMP commands to enable clustering and join the cluster, and set up the cluster to trust the shared CA signed certificate. Ensure that each command executed successfully before moving on to the next command.

For each XMPP server node, create the DNS SRV records as listed in Table 3-13.

Table 3-13 DNS SRV Records for XMPP Server

Name	Resolve To	Port	Explanation
_xmpp-client._tcp.<*XMPPDomain*>	XMPP Server FQDN	5222	Used by Cisco Meeting App to locate the XMPP server for login authentication
_xmpp-component._tcp.<*XMPPDomain*>	XMPP Server FQDN	5223	Used by call bridge to locate an available XMPP server

Using the same name (for example, join.ent-pa.com) for each web bridge, create a DNS A record that resolves to the IP address of the interface used by the web bridge.

Use an API (POST /callBridgeGroups) with the parameter **loadBalancingEnabled** set to **true** to create a call bridge group with the load balancing option enabled, and write down the returned call bridge group GUID. For each call bridge, use an API (PUT /callBridges) to set the **callBridgeGroup** parameter to the <*callBridgeGroup GUID*> for adding the call bridge to the group. Use an API (PUT /system/configuration/cluster) to set the **loadLimit** parameter value for the maximum load on the server platform, using the platform dependent value as specified in the latest version of the white paper on *Load Balancing Calls Across Cisco Meeting Servers*, available at,

https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html

For each web bridge, use an API (PUT /webBridges) to set the **callBridgeGroup** parameter to the <*callBridgeGroup GUID*> to associate the web bridge with the call bridge group so that only call bridges in the group will attempt to connect to the web bridge.

At this point, a complete Cisco Meeting Server cluster should be configured. Browse to one of the web admin pages and update the call settings parameters in the web interface (**Configuration** -> **General**) using the values in Table 3-14.

Table 3-14 Call Settings Configuration Example

Field Name	Value	Comment
SIP media encryption	allowed	Allow both RTP and SRTP
SIP call participant labels	enabled	Show display name if layout supports it
TIP calls	enabled	Allow use of TIP

Summary

After completing the above tasks, the Cisco Meeting Servers will be ready to add to Unified CM.

3. Enable Unified CM for Conferences

This section describes the major tasks required to enable Unified CM for conferences with the Cisco Meeting Server cluster.

Overview

Deployment Tasks to Enable Unified CM for Instant Conferences:

1. Create a new SIP profile named **Standard SIP Profile for CMS** and a SIP trunk security profile named **Security SIP Trunk Profile for CMS**.
2. Create a SIP trunk pointing to the Cisco Meeting Server call bridge node (SIP_TRUNK_CMS1). This step must be repeated for each call bridge in the Cisco Meeting Server cluster nodes. For example, if there are three call bridges in the cluster, there should be three SIP trunks configured.
3. Create a conference bridge and add a SIP trunk (configured in task 2) to it. Each conference bridge should contain the SIP trunk to one of the call bridge cluster peers.

   Configure each conference bridge with the username and password created on Cisco Meeting Server with API privilege.

   This step must be repeated for each call bridge enabled in the Cisco Meeting Server cluster. For example, if there are three call bridges in the cluster, there should be three conference bridges configured.
4. Create media resource group (MRG) named **Video**. Add all conference bridges to the MRG. If you have three call bridges in the cluster, then the MRG should have three conference bridges in it.
5. Create a media resource group list (MRGL) named **Video** and add the MRG (configured in task 4) to it. To allow an endpoint to use instant conferencing, assign the MRGL to the device pool or the device itself.

Deployment Tasks to Enable Unified CM for Permanent and Scheduled Conferences:

6. Create a route group for permanent and scheduled conferences (RG_SPACE_SCHED). Add all SIP trunks (configured in task 2) to the route group. If you have three call bridge nodes in the cluster, then the route group should have three SIP trunks in it, each pointing to one of call bridge nodes.
7. Create a route list (RL_SPACE_SCHED) and add the route group to it.
8. Create a route pattern (8099[12]XXX) that matches the numeric alias for scheduled conferences to be configured in section 4. Deploy Cisco TelePresence Management Suite. Further route patterns are required to configure Spaces, and they are discussed in section 5. Deploy Cisco Meeting Server Spaces.

Deployment Considerations

Unified CM is the first point of logic that decides how to route a call to Cisco Meeting Server to start the conference. Unified CM has different configuration procedures for instant and permanent or scheduled conferences because the mechanism for joining each type of conference is different.

Note The endpoint used to initiate an instant conference must have a conference button. Endpoints that do not have a conference button can still be participants in an instant conference, but they must be added to the conference by an endpoint that has a conference button.

Instant and Permanent Conferences

Figure 3-11 Unified CM Internal Configuration Flow for Instant Conferences

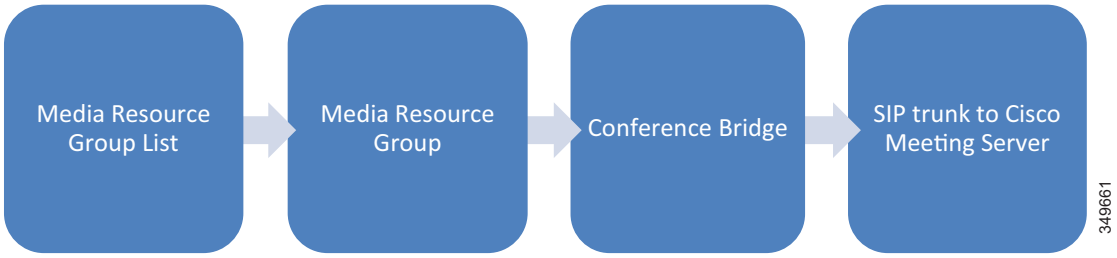
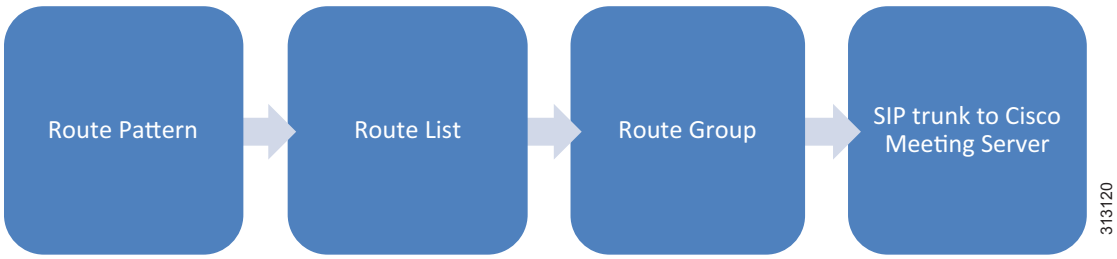


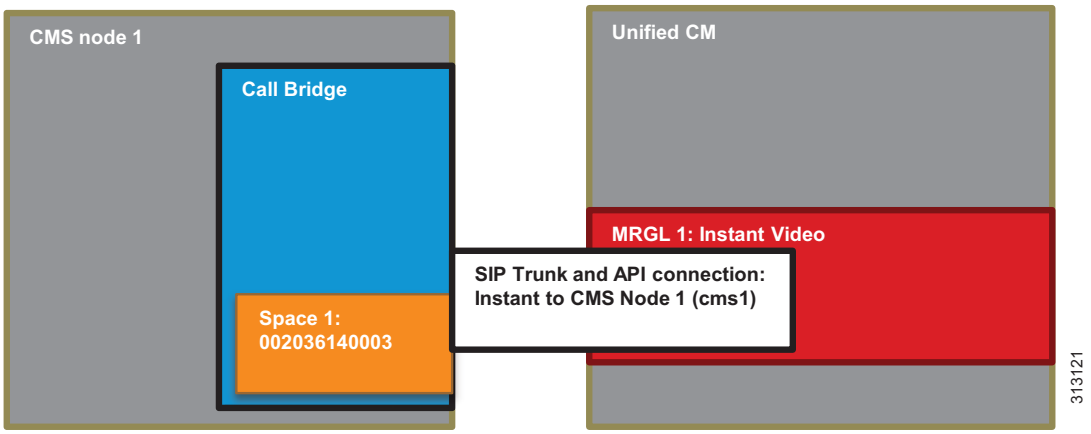
Figure 3-12 Unified CM Internal Configuration Flow for Permanent and Scheduled Conferences



Deployment Tasks to Enable Unified CM for Instant Conferences

It is important to understand that the SIP trunk in Unified CM should point to the call bridge in the Cisco Meeting Server, while the API connection should point to the web admin interface and port. The API connection must be secured using HTTPS. The same SIP trunk can be used for all conference types. Each call bridge node within the Cisco Meeting Server cluster requires a unique set consisting of a SIP trunk and an API connection from the conference bridge in Unified CM (Figure 3-13).

Figure 3-13 Instant Relationship for Cisco Unified CM and Cisco Meeting Server



SIP trunks to Cisco Meeting Server require a customized SIP profile and SIP trunk security profile in order to support calls in all scenarios. To create the SIP profile, copy the **Standard SIP Profile for TelePresence Conferencing** and name the copy **Standard SIP Profile for CMS**, then change the settings as indicated in Table 3-15.

Table 3-15 Settings for SIP Profile

Setting	Value	Comment
Early Offer support for voice and video calls	Best Effort (no MTP inserted)	This is the recommended configuration for all Unified CM trunks. Best Effort Early Offer trunks never use MTPs to create an Early Offer and, depending on the calling device, may initiate an outbound SIP trunk call using either Early Offer or Delayed Offer. In the context of this design, outbound calls always use Early Offer.

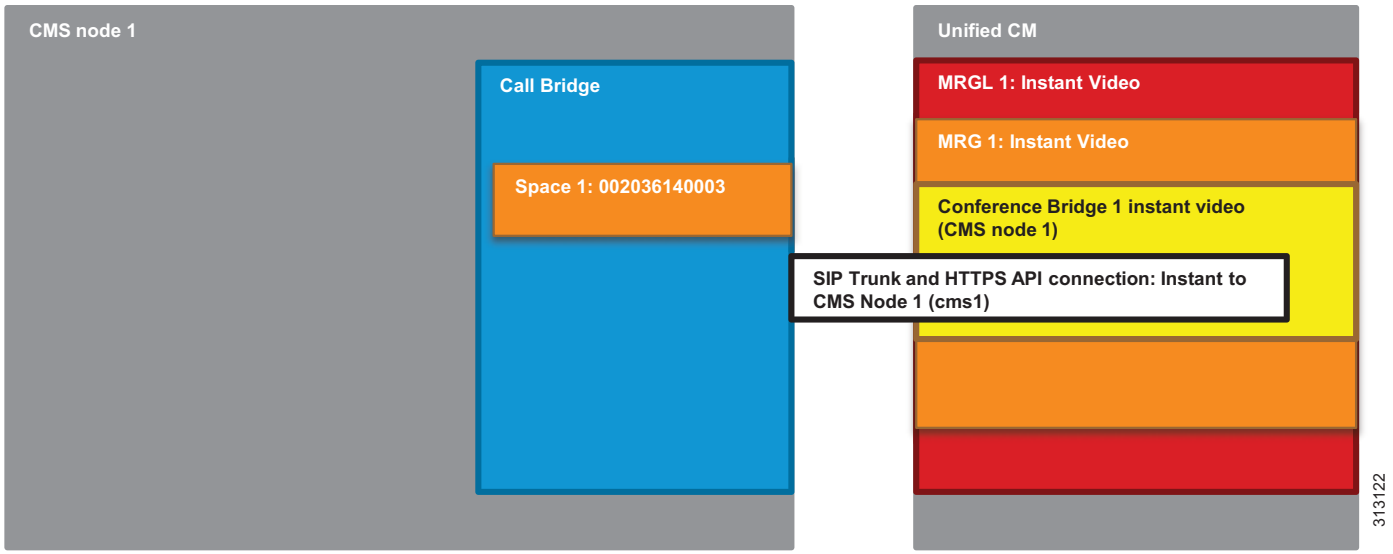
To create the SIP trunk security profile, copy the **Non Secure SIP Trunk Profile** and name the copy **Security SIP Trunk Profile for CMS**, then change the settings as indicated in Table 3-16.

Table 3-16 Settings for SIP Trunk Security Profile

Setting	Value	Comment
Accept replaces header	checked	Enable this option for Unified CM to accept INVITE with Replaces header to reroute calls to the appropriate Cisco Meeting Server in the call bridge group.

SIP trunks inform Unified CM where to route SIP traffic. In the case of instant conferences, the SIP trunks also inform Unified CM where to direct API requests, and they are used in the conference bridge configuration (Figure 3-14). SIP trunks connected to the call bridge in Cisco Meeting Server can be configured to be secure; but for the purpose of this guide, they are assumed to be configured as non-secure.

Figure 3-14 Cisco Unified CM Instant Configuration



Conference bridge configuration provides two key pieces of information to Unified CM: the API credentials to communicate with Cisco Meeting Server and the destination address for that communication (Figure 3-14). The username and password should match those for the API user configured in Cisco Meeting Server. The SIP trunk configured in the conference bridge indicates to Unified CM where to send the HTTPS API traffic. Configure each SIP trunk with the settings indicated in Table 3-17. In addition, each Unified CM cluster should have a unique Conference Bridge Prefix configured in the conference bridges. The prefix does not affect operations in a single Unified CM cluster; but in multi-cluster Unified CM deployments, this prefix would prevent two Unified CM clusters from assigning the same meeting number to different instant conferences at the same time.

Table 3-17 SIP Trunk Settings for Instant Conferences

Setting	Value	Comment
Name	SIP_TRUNK_CMS1	Name of the SIP trunk pointing to Cisco Meeting Server node 1 with the call bridge enabled
Description		Some meaningful description
Device Pool	Trunks_and_Apps	Common device pool for central trunks
Media Resource Group List	<None>	Use the MRGL defined on the device pool
AAR Group	Default	Same everywhere
Transmit UTF-8 for Calling Party Name	Checked	This will allow the ASCII Alerting Name to be transmitted to devices that support UTF-8 characters
PSTN Access	Not checked	
Run On All Active Unified CM Nodes	Checked	This setting is recommended on all SIP trunks. It makes sure that outbound calls to SIP do not require intra-cluster control signaling between Unified CM call processing subscribers.

Table 3-17 SIP Trunk Settings for Instant Conferences (continued)

Setting	Value	Comment
Inbound Calls		
Calling Search Space	TelePresenceConferencing	As defined in the Call Control chapter
AAR Calling Search Space	PSTNReroute	
Outbound Calls		
Use Device Pool Called Party Transformation CSS	Checked	
Use Device Pool Calling Party Transformation CSS	Checked	
SIP Information		
Destination	us-cms1.ent-pa.com	FQDN of Cisco Meeting Server node 1
SIP Trunk Security Profile	Security SIP Trunk Profile for CMS	Use the SIP trunk security profile created above.
Rerouting Calling Search Space	TelePresenceConferencing	Use the same Calling Search Space as configured for Inbound Calls above.
SIP Profile	Standard SIP Profile for CMS	Use the SIP profile created above.

Once all conference bridges are configured, they can be added to media resource groups (MRG). Each media resource group should contain one conference bridge from each call bridge in the Cisco Meeting Server node, so that if communication with one call bridge node is not possible, then calls can be routed to another node.

Each media resource group can then be added to its own media resource group list (MRGL). The media resource group list can be assigned to devices or the device pool in Unified CM and used when those devices escalate a point-to-point call to a conference call using the conference button.

Inside Cisco Meeting Server, the Space used by the instant conference is created dynamically through the HTTPS API connection when a user presses the conference button on the device to initiate the escalation. That Space will be deleted through the API connection after the conference ends.

Deployment Tasks to Enable Unified CM for Permanent and Scheduled Conferences

Permanent and scheduled conferences are configured on Unified CM in a similar way to instant conferences, but they require a dial plan to be configured rather than media resources (Figure 3-15). Use the same SIP trunk and SIP profile for permanent and scheduled conferences that you created for instant conferences, with the settings indicated in Table 3-17.

Figure 3-15 Scheduled Relationship for Cisco Unified CM and Cisco Meeting Server Spaces

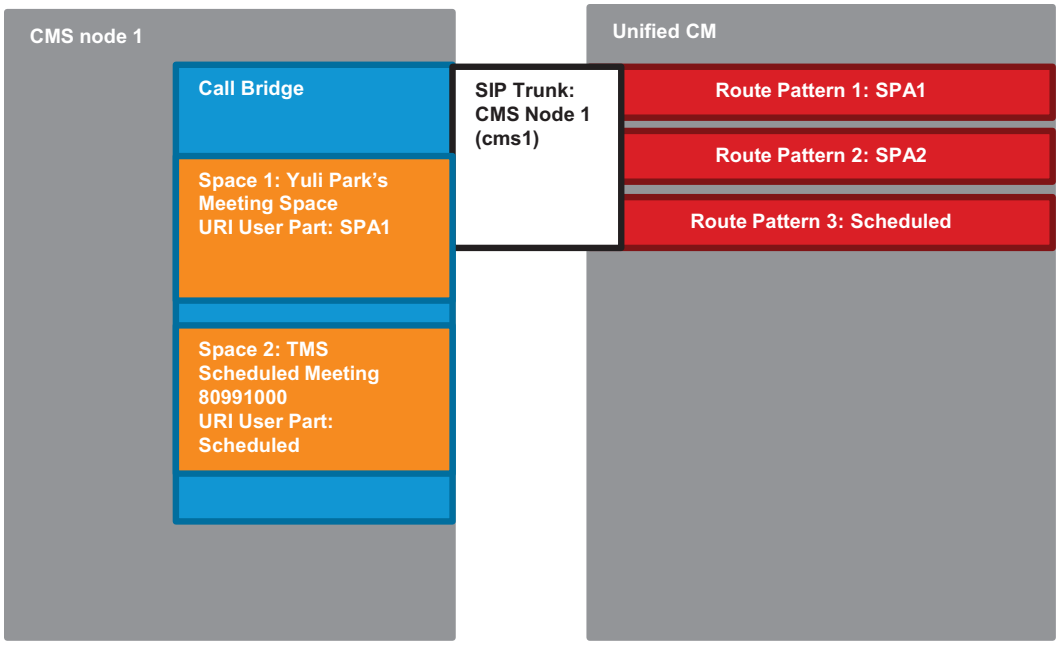
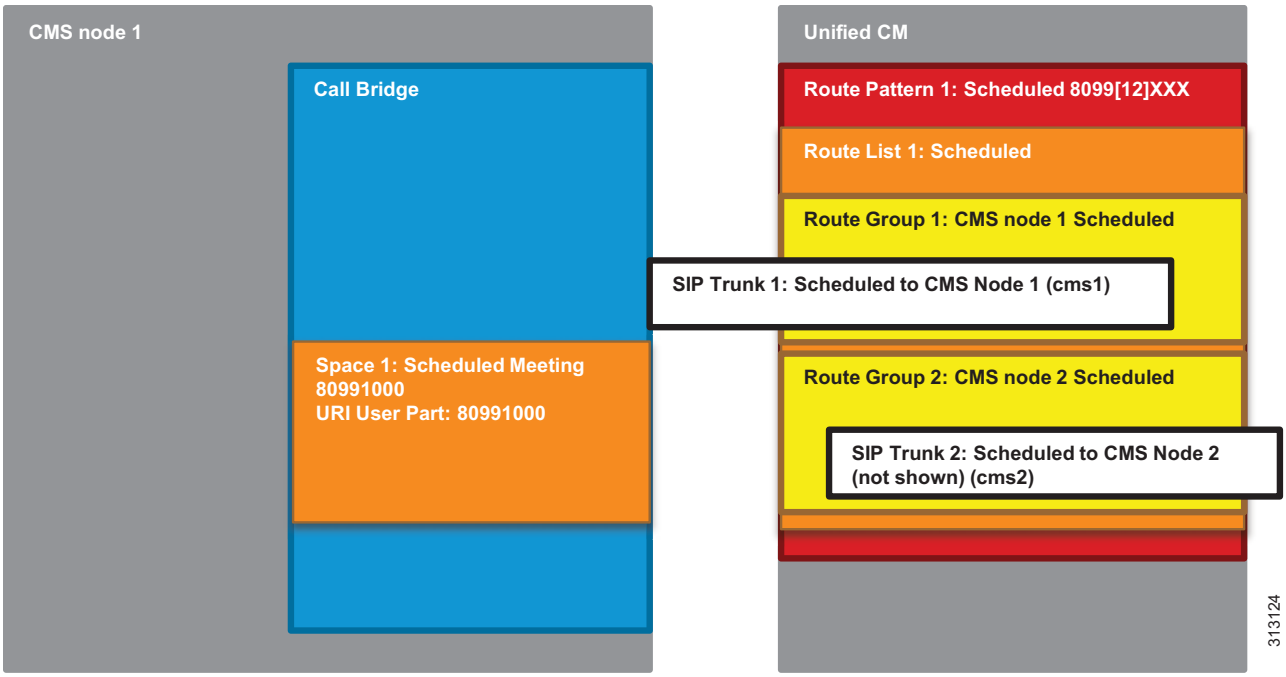


Figure 3-16 Cisco Unified CM Configuration for Permanent and Scheduled Conferences



Create a route group for all the SIP trunks created for instant conferences. Add the route group into a route list. The route list is chosen when a call matches a route pattern that points to it.

To route calls through the SIP trunk to the Cisco Meeting Server, configure a route pattern for the route list. The route pattern should match with the alias range configured for the scheduled conferences, as indicated in Table 3-18. Spaces for scheduled conferences are created when the administrator creates the numeric ID ranges for scheduled conferences in Cisco TMS, and one Space will be created for each number ID. Refer to section 4. Deploy Cisco TelePresence Management Suite for details.

Table 3-18 Route Pattern for Scheduled Conference Route List

Pattern	Partition	Gateway or Route List	Description
8099[12]XXX	ESN	RL_SPACE_SCHED	Pattern to match scheduled alias range

More details on deployment and route pattern configuration for Cisco Meeting Server permanent conferences are discussed in section 5. Deploy Cisco Meeting Server Spaces.

Summary

After you complete the deployment tasks outlined above, Unified CM should be able to communicate with Cisco Meeting Server.

4. Deploy Cisco TelePresence Management Suite

This section describes the deployment tasks for Cisco TMS for scheduled conferences using Cisco Meeting Server.

Overview

Deployment Tasks for Cisco TMS High Availability:

1. Install and configure Cisco TMS on active and passive nodes.
2. Install and configure the network load balancer (NLB).
3. Configure file sharing between active and passive node servers.

Deployment Tasks for Cisco TMS Basic Configuration:

4. Configure Active Directory integration, group structure, and users.
5. Create the TMS System Navigator folder structure.
6. Configure default conference setting.

Deployment Tasks for Cisco TMS for Scheduled Conferences:

7. Integrate Cisco Meeting Server with TMS.
8. Integrate Unified CM with TMS.
9. Add conference room endpoints to TMS.
10. Install and configure TMS Extensions for Microsoft Exchange (TMSXE).

Deployment Tasks for Cisco TMS High Availability

This section describes the tasks required to deploy Cisco TMS with high availability.

Install and Configure Cisco TMS on Active and Passive Nodes

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

https://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.

Install and Configure Network Load Balancer (NLB)

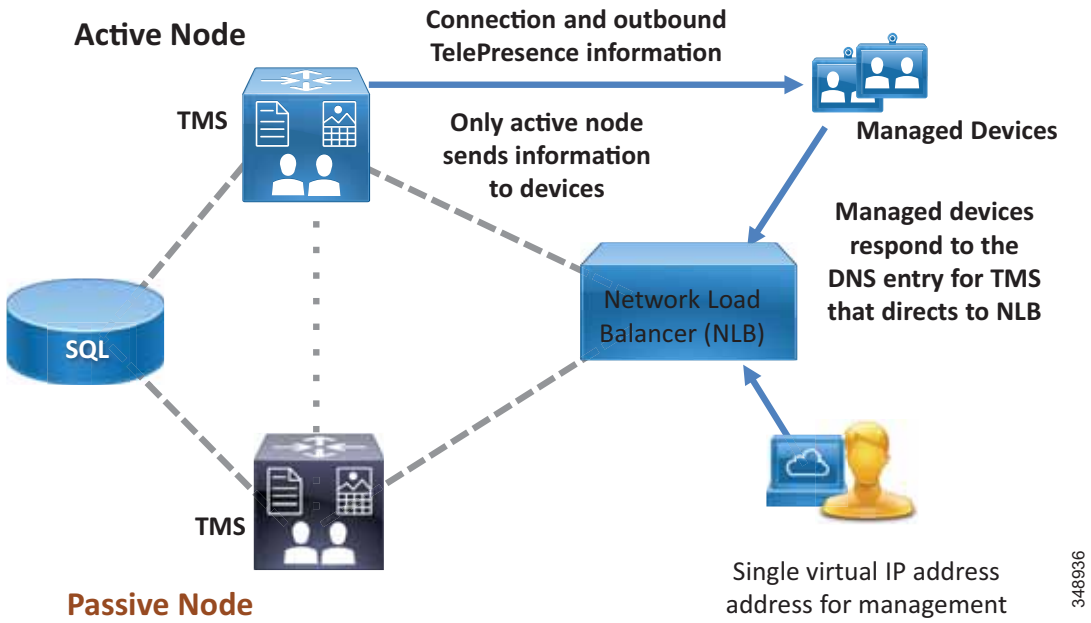
The specifics of the network load balancing configuration are left to the instructions of the load balancer chosen by the customer. The following are functional requirements that must be configured:

- 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 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 use to initiate communications to TMS. By using a FQDN of tms.ent-pa.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 3-17.)

Figure 3-17 NLB Directs Communications from Managed Devices to the Active TMS Node



Configure File Sharing 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.

Deployment Tasks for Cisco TMS Basic Configuration

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

- Active Directory Integration, Group Structure, and Users
- System Navigator Folder Structure
- Default Conference Settings
- Default Conference Settings
- Modify Email Templates within 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 support desk personnel and technical administrators as well as end users who schedule conferences.

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

https://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.

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
- 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-room system video devices should be set to 2048 kbps. Any endpoint that has a lower setting for maximum bandwidth will join at its maximum bandwidth.

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

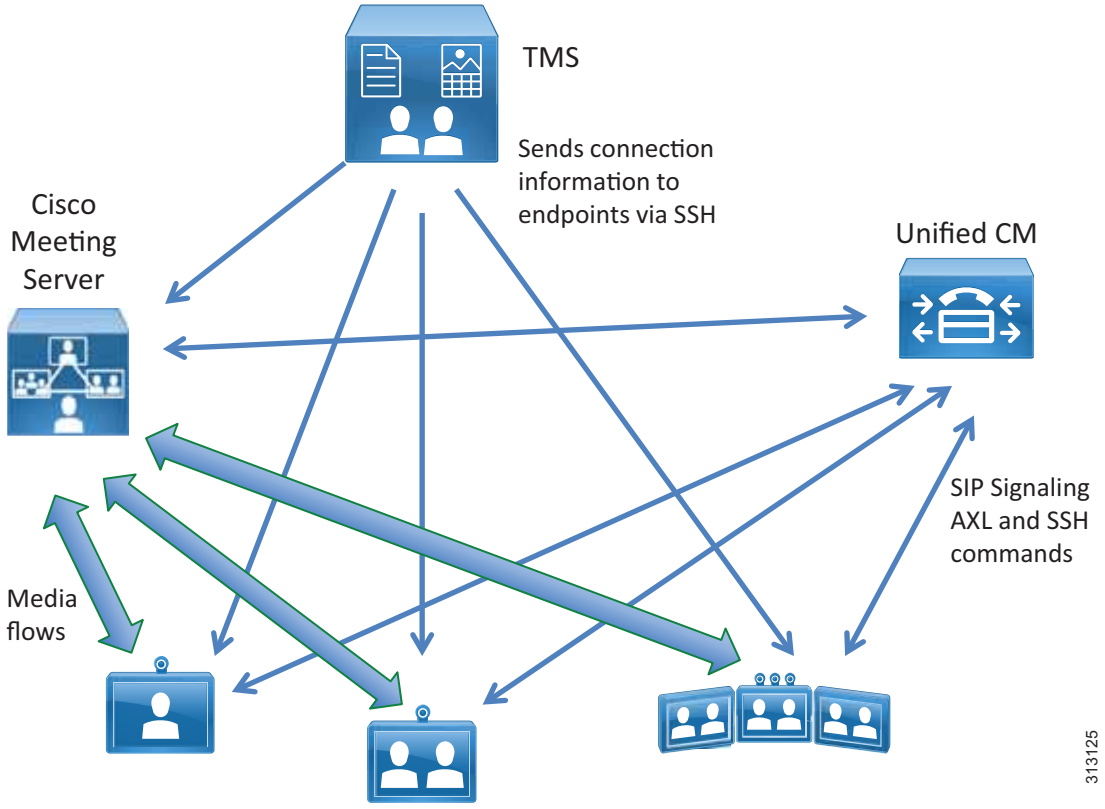
Cisco TMS contains the templates used to notify conference organizers. However, Cisco TMSXE can inject errors, warnings, and informational text into email messages sent by Cisco TMS. These messages can be modified by the administrator. Avoid removing or changing text in curly brackets – for example, {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.

Deployment Tasks for Cisco TMS for Scheduled Conferences

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 3-18.)

Figure 3-18 Cisco TMS Communicates Directly with Unified CM Managed Endpoints



Integrate Cisco Meeting Server with Cisco TMS

To allow Cisco TMS to perform scheduling and conference control for scheduled conferences, add one Cisco Meeting Server node from each Cisco Meeting Server cluster.

Cisco TMS must be configured with a range of numeric IDs, and these are used by Cisco TMS to determine where a scheduled call is placed.

Add one Cisco Meeting Server from each Cisco Meeting Server cluster to Cisco TMS. Add them to the appropriate folder using an administrator account configured on the Cisco Meeting Server. For each Cisco Meeting Server configured in Cisco TMS, set the parameters as listed in Table 3-19.

Table 3-19 Cisco TMS Parameter Settings for Cisco Meeting Server

Setting	Value	Comment
IP Address	10.X.X.2:445	Cisco Meeting Server web admin interface IP address and port number
Username	TMSadmin	This setting should match the username configured on the Cisco Meeting Server
Password	<password>	
Usage Type	Other	

After adding Cisco Meeting Server, specify the alternate IP Network Settings in the Cisco Meeting Server settings as listed in Table 3-20. The alternate IP Cisco Meeting Server takes over the operations in case the first Cisco Meeting Server fails.

Table 3-20 Alternate IP Network Settings for Cisco Meeting Server

Setting	Value	Comment
Alternate IP	*<Select one in drop-down>*	Cisco Meeting Server cluster nodes with call bridge enabled
Alternate IP Username	TMSadmin	User configured in the Cisco Meeting Server with the IP address specified in the alternate IP
Password	*<password>*	

Configure the conference alias and identify a numeric range for Cisco Meeting Server to use as part of the dial plan and as designated in the SIP trunks. Table 3-21 lists the Extended settings for Cisco Meeting Server to specify the numeric ID range for scheduled calls.

Table 3-21 Extended Settings for Cisco Meeting Server

Parameter	Value
Domain	Domain associated with the Cisco Meeting Server.
Numeric ID Base	This is the first number in the scheduled conferencing range of the dial plan.
Numeric ID Quantity	Specify the number of numeric IDs required for scheduled conferences.

Save the configuration to add Cisco Meeting Server. For each numeric ID, Cisco TMS will create an inactive Space using the numeric ID as the URI user part on the Cisco Meeting Server. These Spaces are used to host scheduled conferences created by Cisco TMS. When it is time to start the scheduled conference, Cisco TMS will activate the Space on Cisco Meeting Server, and participants can begin calling in.

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 Cisco Meeting Server.

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

To use Cisco Meeting Server for scheduled calls, you must edit the Cisco Meeting Server settings within Cisco TMS. H.323 dialing should be disabled in both directions, Allow Booking should be enabled, and SIP dialing should be enabled in both directions.

The numeric ID range used must be configured so that the scheduled conference number range matches that configured on Unified CM. Edit the Extended Settings of the Cisco Meeting Server in Cisco TMS, as listed in Table 3-22. The domain should match the XMPP domain configured in Cisco Meeting Server. The numeric ID should match the route pattern configured for the trunk to Cisco Meeting Server from Unified CM.

Table 3-22 Extended Settings for Cisco Meeting Server

Setting	Value	Comment
Domain	cms.ent-pa.com	SIP URI domain for the scheduled meetings
Numeric ID Base	80991000	The first number that Cisco TMS uses to form the dial string used by participants dialing into the scheduled conference; for example, 80991000.
Numeric ID Quantity	1999	The number of times Cisco TMS will increase the number from the Numeric ID Base. This number should be set so that the highest number does not exceed the allocated range for scheduling: 80991000 to 80992999.

It is important to configure Cisco TMS to use Cisco Meeting Server for scheduling, otherwise scheduling will fail. In **Administrative Tools** > **Configuration** > **Conference Settings**, edit the settings as shown in Table 3-23.

Table 3-23 Cisco TMS Conference Settings

Setting	Value	Comment
Preferred MCU Type in Routing	Cisco Meeting Server	Prefers Cisco Meeting Server for scheduling over other devices

Integrate Unified CM with 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 latest version of the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*, available at

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

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.

Add the publisher by the same method used for 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. Make sure the DN for each endpoint in Unified CM complies with the E.164 guidelines listed in the Call Control chapter.

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.

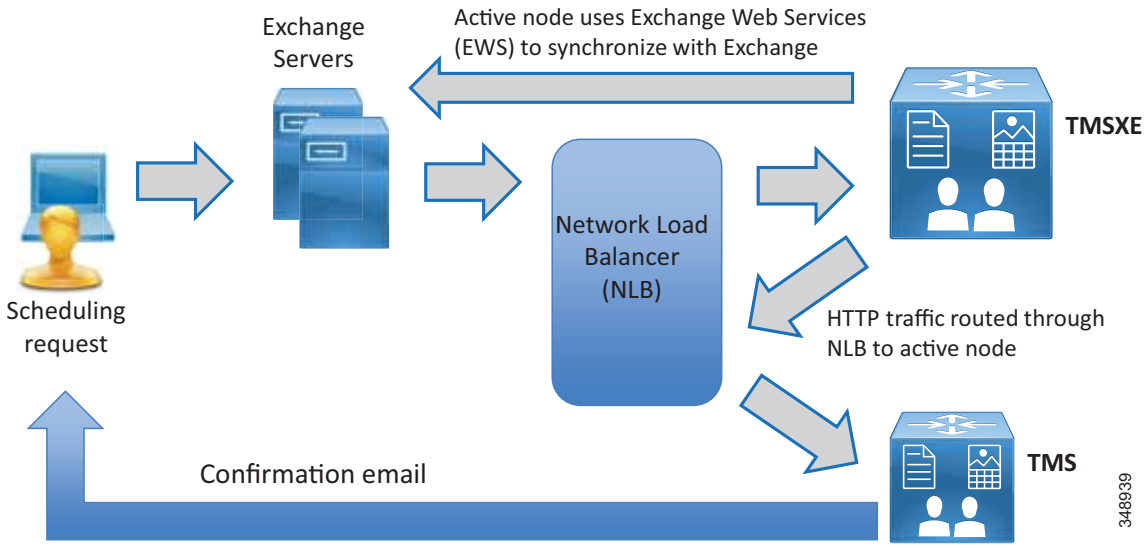
This software extension to TMS requires a license key to activate the functionality within TMS. This key must be installed in TMS before installing the TMSXE software. For deployments with more than 50 scheduled endpoints, TMSXE must be installed on its own server or virtual machine instance.

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 3-19). 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 3-19 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.

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

- Select the TMS Booking Service.
- 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 latest version of the *Cisco TelePresence Management Suite Extension for Microsoft Exchange Deployment Guide*, available at

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

Summary

After you complete the deployment tasks outlined above, Cisco TMS will be configured to communicate with Cisco Meeting Server for scheduled conferencing.

5. Deploy Cisco Meeting Server Spaces

This section describes the major tasks required to deploy Cisco Meeting Server Spaces.

Overview

Deployment Tasks for Unified CM for Cisco Meeting Server Permanent Conferences:

1. Configure an Early Offer SIP trunk between Unified CM and Cisco Meeting Server. The SIP trunk SIP_TRUNK_CMS1 configured previously can be used here.
2. Set up new route pattern(s) for the Space numeric alias that points to the route list containing the relevant trunks. The route list RL_SPACE_SCHED configured previously can be used here.
3. Create a SIP route pattern for the Space URI that points to the route list (RL_SPACE_SCHED) used in task 2.

Deployment Tasks for Cisco Meeting Server to Create Spaces:

4. Create a User Profile and assign Multiparty licenses to users.
5. Import users from LDAP and create Spaces.
6. Create dial plan rules to handle incoming calls.

Deployment Considerations

Cisco Meeting Server Spaces are similar to permanent conferences created in the TelePresence infrastructure that resides in the enterprise's data center. Each Space has a unique set of video addresses that a user can call into to start a meeting at any time, and the video addresses can be in the format of numeric aliases or SIP URIs. Each Space can be associated with an individual user and can be created through LDAP user synchronization.

Cisco Meeting Server Spaces provide an easy way for participants to join a conference regardless of where those participants are located. Everyone dials into the same virtual meeting room from their laptop, telepresence room, desktop endpoint, or mobile device.

Deploying Spaces involves the deployment of Unified CM and Cisco Meeting Server. The following sections describe the high-level process for deploying each component for Spaces.

Tip Before deploying Spaces, decide on the format of the conference aliases (numeric or SIP URI).

Deployment Tasks for Unified CM for Cisco Meeting Server Permanent Conferences

The main function of Unified CM is to handle call routing to and from Cisco Meeting Server. Connect Unified CM to Cisco Meeting Server with a SIP trunk enabled for Early Offer. (Use the same trunk as previously configured for scheduled conferences: SIP_TRUNK_CMS1.) When a user dials the Space alias, the call is sent to call bridge on Cisco Meeting Server via the SIP trunk. Similarly, Cisco Meeting Server can send calls to Unified CM through the SIP trunk for auto-dial participants. The conference alias has two formats: SIP URI or numeric. The dial plan design should include the call routing for both the numeric alias and SIP URI for Spaces. For dial plan design details, refer to the Call Control chapter.

A Cisco Meeting Server Space can be created for each individual user, and the Space numeric alias can be based upon the user's DID number. Table 3-24 shows the Space numeric alias ranges for a deployment using the dial plan example from Call Control chapter.

Table 3-24 Space Numeric Alias Ranges

Site	+E.164 DID Range	Space Numeric Alias Range
SJC	+1 408 555 4XXX	8-004-4XXX
RTP	+1 919-555 1XXX	8-005-1XXX
RCD	+1 972 555 5XXX	8-006-5XXX

For numeric aliases, configure a route pattern for each site that routes to the Cisco Meeting Server route list for permanent conferences, as shown in Table 3-25.

Table 3-25 Route Patterns Configuration for Space Numeric Alias

Pattern	Partition	Gateway or Route List	Description
80044XXX	ESN	RL_SPACE_SCHED	Pattern to match SJC DID range
80051XXX	ESN	RL_SPACE_SCHED	Pattern to match RTP DID range
80065XXX	ESN	RL_SPACE_SCHED	Pattern to match RCD DID range

For SIP URIs, use the XMPP domain as the domain part. The XMPP domain configured in this document is cms.ent-pa.com. For example, participants can dial <*username*>**.space@cms.ent-pa.com** to join the conference on Cisco Meeting Server. Cisco Meeting App users are also reachable by dialing <*username*>**@cms.ent-pa.com**, for example, from a Unified CM registered device. Unified CM sends all calls for the XMPP domain to Cisco Meeting Server. Configure a Domain Routing SIP Route Pattern with the Cisco Meeting Server XMPP domain that routes calls to the Cisco Meeting Server route list for permanent conferences, as shown in Table 3-26.

Table 3-26 SIP Route Pattern Configuration for Space URI

Pattern	Partition	Gateway or Route List
cms.ent-pa.com	URI	RL_SPACE_SCHED

Deployment Tasks for Cisco Meeting Server to Create Spaces

Note The tasks in this section are deployed using Cisco Meeting Server API with a tool (Postman, for example) to execute the REST API. For API details, refer to the latest version of the *Cisco Meeting Server API Reference Guide*, available at https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html.

Cisco Meeting Server must have the Multiparty licenses applied before it can host conferences. Each user should be given a license if Personal Multiparty Plus (PMP+) is desired. To assign PMP+, the user should be associated with a user profile object that has the hasLicense field set to **true**. If the hasLicense field is **false** or does not exist in the user profile object, the user has no license and Shared Multiparty Plus (SMP+) will be used. User profiles specify the capabilities for the users. Use an API to create a userProfile object (POST /userProfiles) using the parameters as listed in Table 3-27, and set the hasLicense field to **true**.

Table 3-27 userProfile Object Parameters

Parameter	Value	Description
hasLicense	true	Use Personal Multiparty License
canReceiveCall	true	Allow Cisco Meeting App users to receive call

All users in Cisco Meeting Server reside in the LDAP directory. The user profile object (created previously) should be used as one of the parameters to synchronize the users from the directory to Cisco Meeting Server, and all imported users will be associated with that user profile. The ldapServers, ldapMappings, and ldapSources objects are required to create the user synchronization process.

ldapServers specifies the location, credentials, and other attributes to access the server. Use the parameters as listed in Table 3-28 to create the ldapServers object (POST /ldapServers).

Table 3-28 ldapServers Object Parameters

Parameter	Example Value	Description
address	10.192.168.10	IP address or FQDN of the directory
portNumber	636	Port number used by the directory
username	ent-pa\tmssvc	Username to access the directory
password	*<password>*	Password of the account associated with username
secure	true	Use a secure connection for directory access

ldapMappings allows you to specify the attributes related to the Space; for example, name, username, URI, and so forth. The attributes can be created based upon the attributes from Microsoft Active Directory (see Table 3-29). Use the parameters as listed in Table 3-29 to create the ldapMappings object (POST /ldapMappings).

Table 3-29 ldapMappings Object Parameters

Parameter	Example Value	Description
nameMapping	$displayName$	Display name
jidMapping	$sAMAccountName$@cms.ent-pa.com	XMPP username
coSpaceNameMapping	$displayName$'s Meeting Space	Space name
coSpaceUriMapping	$sAMAccount$.space	Space primary URI
coSpaceSecondaryUriMapping	80044$telephoneNumber\|'/.*([[:digit:]]{3})$/\1/'$	Space secondary URI

Note that the prefix for Space secondary URI varies depending on the site, and the last three digits are extracted from the user's DID number. Using the dial plan example from the Call Control chapter, the SJC site has prefix 80044, RTP site has prefix 80051, and RCD site has prefix 80065. Hence, the ldapMappings object will be created three times, one for each site.

After importing the user with the mappings in Table 3-29, the user has the username <*username*>**@cms.ent-pa.com**, which can be used to sign in to the Cisco Meeting App. The user has an associated Space with primary URI <*username*>**.space@**<*domain*> and secondary URI **80044XXX@**<*domain*>. The domain is based on the domain name configured in the call matching table for incoming calls inside Cisco Meeting Server (see Table 3-31).

LDAP Sources are used to combine the LDAP Server, LDAP Mapping, user profile, and LDAP filter into a single source so that a specific group of users can be imported into Cisco Meeting Server. Use the parameters as listed in Table 3-30 to create the ldapSources object (POST /ldapSources).

Table 3-30 ldapSources Object Parameters

Parameter	Example Value	Description
server	<*ldapServers id*>	ldapServers object ID
mapping	<*ldapMappings id*>	ldapMappings object ID
userProfile	<*userProfile id*>	userProfile object ID
baseDn	ou=enterprise,dc=ent-pa,dc=com	Top level search base
filter	memberof=cn=sjcgroup,ou,ou=enterprise,dc=ent-pa,dc=com	LDAP filter

Note that the ID of the object can be retrieved using the GET operation. For example, to retrieve the ID of the ldapMapping object, use GET /ldapMappings. Also, each site will have different filter so that users at each site will be imported based on the Active Directory group to which the users belong. For example, SJC users should belong to **sjcgroup** Active Directory group, RTP users should belong to **rtpgroup** Active Directory group, and RCD users should belong to **rcdgroup** Active Directory group. Hence, three ldapSource objects will be created using the site-specific ldapMapping and filter.

After all LDAP Sources are created, use the ldapSyncs object (POST /ldaySyncs) to start the user synchronization immediately. When the synchronization is done, users from all sites and a Space for each imported user should be created in Cisco Meeting Server.

Note Spaces can be created using an API or manually by users in the Cisco Meeting App.

Next, create dial plan rules in Cisco Meeting Server to handle incoming calls. Browse to one of the web admin interfaces and add the domains to the call matching table of incoming calls configured in the web interface (**Configuration** -> **Incoming Calls**) using the values in Table 3-31. The domains are the XMPP domain (cms.ent-pa.com), top level domain (ent-pa.com), and FQDN and IP address of all call bridges (us-cms1.ent-pa.com and us-cms2.ent-pa.com).

Table 3-31 Incoming Call Handling Configuration

Domain Name	Priority	Targets Spaces	Targets Users	Targets IVRs	Targets Lync
cms.ent-pa.com	100	yes	yes	yes	no
ent-pa.com	100	yes	no	yes	no
us-cms1.ent-pa.com	100	yes	no	no	no
us-cms2.ent-pa.com	100	yes	no	no	no
10.x.x.60	100	yes	no	yes	no
10.x.x.61	100	yes	no	yes	no

All SIP URI calls that are dialed to the XMPP domain (cms.ent-pa.com) are either for the Spaces or Cisco Meeting App users. Users calling into the Spaces using numeric dialing will hit the rules for the top level domain or the call bridge FQDNs or IP addresses. Using numeric dialing cannot reach the Cisco Meeting App users.

Summary

After you complete the deployment tasks outlined above, users can sign into their Space using Cisco Meeting App to specify PIN, add members, and customize other preferences. Users can then dial the SIP URI or numeric alias to start the meeting.

6. Deploy Cisco Meeting Management

This section describes the major deployment tasks for Cisco Meeting Management.

Overview

Deployment Tasks for Cisco Meeting Management:

1. Perform first-time setup and login to the Cisco Meeting Management portal using the one-time password.
2. Continue LDAP setup for user authentication and group mappings. Use the same directory as Cisco Meeting Server.
3. Configure CDR receiver, Cisco TMS, and NTP addresses. Use the same NTP for Cisco Meeting Server and TMS to ensure all time stamps are synchronized.
4. Add call bridges to Cisco Meeting Management.

Deployment Considerations

Cisco Meeting Management uses LDAP directory for user authentication and LDAP group to map the user group that determines the user's role. At least 2 LDAP directory groups are required for the deployment, create one group (e.g. CMMAdmin) for the administrators and another group (e.g. CMMOperator) for the video operators. Then decide on which user should belong to which group and assign users to the corresponding groups before proceeding with first-time setup.

Deployment Tasks for Cisco Meeting Management

Start the first-time setup deployment and continue until logging into the Cisco Meeting Management portal for the first-time using the one-time password. For details on first-time setup, refer to the latest version of the *Cisco Meeting Management Installation and Configuration Guide*, available at

https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-installation-guides-list.html

All users in Cisco Meeting Management reside in the LDAP directory that Meeting Management utilizes for user authentication. Therefore, after logging into the portal for the first-time, configure the LDAP server, user search base, and authentication information using the values in Table 3-32.

Table 3-32 First-Time Setup Server Configuration

Parameter	Example Value	Description
LDAP Server:		
Protocol	LDAPS	Protocol used to access the directory
Server Address	10.192.168.10	IP address or FQDN of the directory
Port	636	Port number used by the directory
Search Base:		
Base DN	OU=Enterprise, DC=ent-pa, DC=com	Top-level user search base
Search Attribute	sAMAccountName	Attribute used to identify the user

Table 3-32 First-Time Setup Server Configuration (continued)

Parameter	Example Value	Description
Authorization:		
Bind DN	CN=tmssvc, OU=Enterprise, DC=ent-pa, DC=com	Service account used to access the directory
Password	<password>	Service account password

Cisco Meeting Management uses the LDAP group to map the user group and thus determine the user access privilege in the portal. At this point, map the LDAP group (CMMGroup) created previously for the administrator so that users can login to continue the setup. Use the value shown in Table 3-33 to configure the group mapping.

Table 3-33 Group Mapping Configuration

Parameter	Example Value	Description
Group DN	CN=CMMAdmin, OU=Enterprise, DC=ent-pa, DC=com	LDAP group for administrator

After the first-time setup is complete, log into the Cisco Meeting Management portal using one of the administrator (user in CMMAdmin LDAP group) credentials. Once logged in, go to **Settings** -> **CDR** to set up the CDR receiver address using the IP address or FQDN of the Cisco Meeting Management server (for example, https://10.x.x.68). Cisco Meeting Management uses this address to construct the CDR receiver URI string in the call bridges to receive call related events. Next, go to **Settings** -> **TMS** to set up a Booking API connection with TMS to retrieve information about the upcoming scheduled meetings. Use the values shown in Table 3-34 for the configuration.

Table 3-34 TMS Configuration

Parameter	Example Value	Description
Use TMS with Meeting Management		Enable TMS integration
TMS Address	10.x.x.75	IP address or FQDN of TMS
Protocol	HTTPS	Protocol used to connect with TMS
Username	<*username*>	TMS site administrator user account
Password	<*password*>	Password of the user

Then go to **Settings** -> **NTP** and add the NTP server. The same NTP server should be used for Cisco Meeting Server and TMS in order to synchronize the time among the three components.

As mentioned previously, Cisco Meeting Management has the administrator and video operator user groups. The administrator group was added in the first-time setup steps, and video operators should be added here. Go to **Users** -> **User Groups** and use the values shown in Table 3-35 for the configuration.

Table 3-35 Video Operator Group Configuration

Parameter	Example Value	Description
LDAP Path	CN=CMMOperator, OU=Enterprise, DC=ent-pa, DC=com	LDAP group for video operators
Role	Video Operators	Role for the user group

Next, add all call bridges within the cluster into Cisco Meeting Management for monitoring and management. Go to the **Servers** page and add a call bridge (anyone within the cluster) using the values in Table 3-36 for the configuration.

Table 3-36 Add Call Bridge Configuration

Parameter	Example Value	Description
Server Address	10.x.x.60	IP address or FQDN of call bridge
Port	445	Port used by webadmin in Cisco Meeting Server
Display Name	US-CMS1	Meaningful name to represent the call bridge
Username	<*user*>	Local Cisco Meeting Server user with API access
Password	<*password*>	User password

Use the auto-discovered call bridge option to add the rest of call bridges within the cluster into Cisco Meeting Management. Cisco Meeting Management needs to know the call bridge that is added to TMS in order to show the scheduled meetings. To do so, the administrator needs to associate the Cisco Meeting Server cluster with TMS. Click on the **Associate cluster with TMS** link on top of the cluster table and use the values in Table 3-37 for the configuration.

Table 3-37 Associate Cluster with TMS Configuration

Parameter	Example Value	Description
Connected Call Bridge	US-CMS1	Name of call bridge added to TMS
TMS System ID	<*id*>	TMS ID located in the call bridge settings page inside TMS

If a second Cisco Meeting Management instance is desired to achieve high availability, repeat the tasks in this section. Then configure a network load balancer to put in front of the two Cisco Meeting Management instances.

Summary

After you complete the deployment tasks outlined above, video operators can login to the Cisco Meeting Management portal to monitor and manage meetings for Cisco Meeting Server.

Related Documentation

For additional information about Cisco Meeting Server, refer to the latest version of the following documents, available at the links provided below:

- Cisco Multiparty Licensing At-A-Glance

  https://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration/pervasive-conferencing/at-a-glance-c45-729835.pdf

- Cisco Meeting Server deployment guides and certificate guideline documents

  https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html

- Cisco Meeting Server API Reference Guide

  https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html

- Cisco Meeting Server release notes

  https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-release-notes-list.html