Cisco Meeting Server

Deployments with Cisco Expressway X12.6 and later

Planning and Preparation Guide

April 20, 2022

Contents

Change History 4

1 Introduction 5
1.1 Configuring the Meeting Server 8
1.1.1 New tools to ease configuring Meeting Server 8
1.2 Managing conferences 11
1.3 Using the Cisco Expressway-E as the edge device in Meeting Server deployments 12
1.4 Using the Cisco Expressway-C with the Meeting Server in the core network 13
1.5 Using Call Control 14

2 Single server deployment 15
2.1 Overview of Meeting Server components 15
2.2 Deployment considerations 17
2.2.1 Summary of devices required 17
2.2.2 Licensing 18
2.2.3 Certificate requirements 19
2.2.4 Security 19
2.2.5 Port requirements 21
2.2.6 What Can Be Branded 21

3 Scalable and resilient server deployments 22
3.1 Overview 22
3.2 Features supporting scaling Meeting Server deployments 22
3.2.1 Call Bridge Clustering 22
3.3 Features supporting resiliency in Meeting Server deployments 23
3.3.1 Database Clustering 23
3.3.2 Call Bridge Grouping 24
3.4 Deployment considerations 25
3.4.1 Additional certificate requirements for scalable and resilient deployments 25
3.4.2 Additional devices required for scalable and resilient deployments 26

Appendix A Technical specifications 27
A.1 Video standards 27
A.2 Audio standards 27
A.3 Resolution and frame rate 27
A.4 Bandwidth 27

A.5 Call capacity 28

Appendix B Call capacities by Cisco Meeting Server platform 29
B.1 Cisco Meeting Server web app call capacities 30
B.1.1 Cisco Meeting Server web app call capacities — external calling 30
B.1.2 Cisco Meeting Server web app capacities — mixed (internal + external) calling 31
B.2 Number of users supported on Cisco Meeting Server 31

Cisco Legal Information 32

Cisco Trademark 33

Change History

Date	Change Summary
April 20, 2022	Updated for version 3.5.
December 15, 2021	Updated for version 3.4.
August 24, 2021	Updated for version 3.3.
May 19, 2021	Updated the document for web app call capacities and recommendations for Medium OVA Expressway.
April 08, 2021	Updated for version 3.2. Call capacities by Cisco Meeting Server platforms updated.
November 30, 2020	Updated for version 3.1.
October 07, 2020	Minor correction.
September 11, 2020	Updated for version 3.0.
April 21, 2020	Updated for version 2.9. Added section on new tools to help configuring and deploying Meeting Server.
September 25, 2019	Minor correction to include Cisco Expressway as a supported call control system for Call Bridge Grouping.
August 05, 2019	Title change to X8.11 and later
June 03, 2019	Minor corrections.
January 31, 2019	Clarification added to Streamer component support information.
January 28, 2019	Minor correction to a link.
January 16, 2019	Minor changes for clarification.
January 08, 2019	Minor corrections to appendix on scaling deployments
January 03, 2019	Added appendix on scaling deployments
December 18, 2018	Minor additions for clarification.
December 14, 2018	New guide

1 Introduction

The Cisco Meeting Server software can be hosted on specific servers based on Cisco Unified Computing Server (UCS) technology and on specification-based VM servers. Cisco Meeting Server is referred to as the Meeting Server throughout this document.

Note: Cisco Meeting Server software version 3.0 (and later) does not support X-Series servers.

Note: Cisco Meeting Management version 3.0 (or later) is mandatory in Cisco Meeting Server version 3.0 – Meeting Management reads the Meeting Server license file, and can handle the product registration and interaction with your Smart Account (if set up).

Note: Cisco Meeting App for WebRTC (Web Bridge 2) is removed from Cisco Meeting Server version 3.0. If using software version 3.0 or later, you will need to use Cisco Meeting Server web app instead of Cisco Meeting App for WebRTC. To do this, you need to deploy Web Bridge 3 – for details on deploying and configuring Web Bridge 3, see the 3.0 or later Deployment Guides.

The Meeting Server can be deployed as a single server providing a single instance of the conference bridge, or on multiple servers either co-located or located in different geographies. The flexibility of the Meeting Server architecture enables your deployment to expand as your video conferencing requirements grow; call capacity can be increased by adding Meeting Servers, and resiliency introduced by clustering the Call Bridges.

This guide covers planning a Meeting Server deployment when Cisco Expressway is used as the edge device, in place of the TURN server component within the Meeting Server.

Expressway (Large OVA or CE1200) is the recommended solution for deployments with medium web app scale requirements (i.e. 800 calls or less). Expressway (Medium OVA) is the recommended solution for deployments with small web app scale requirements (i.e. 200 calls or less). However, for deployments that need larger web app scale, from version 3.1 we recommend Cisco Meeting Server web edge as the required solution.

For more information on using Cisco Meeting Server web edge solution, see 3.1 or later Deployment Guides.

In addition, Cisco has simplified the Cisco Meeting Server and Meeting app interaction, and as a result the app dependence on XMPP has been removed. From version 3.0, the XMPP and associated components (XMPP Load Balancer and trunk) are removed from the Cisco Meeting Server software. The Cisco Meeting Server web app and Cisco Jabber are the supported apps to join Meeting Server hosted conferences, in addition to SIP endpoints, and Lync/Skype for Business clients in dual homed conferences.

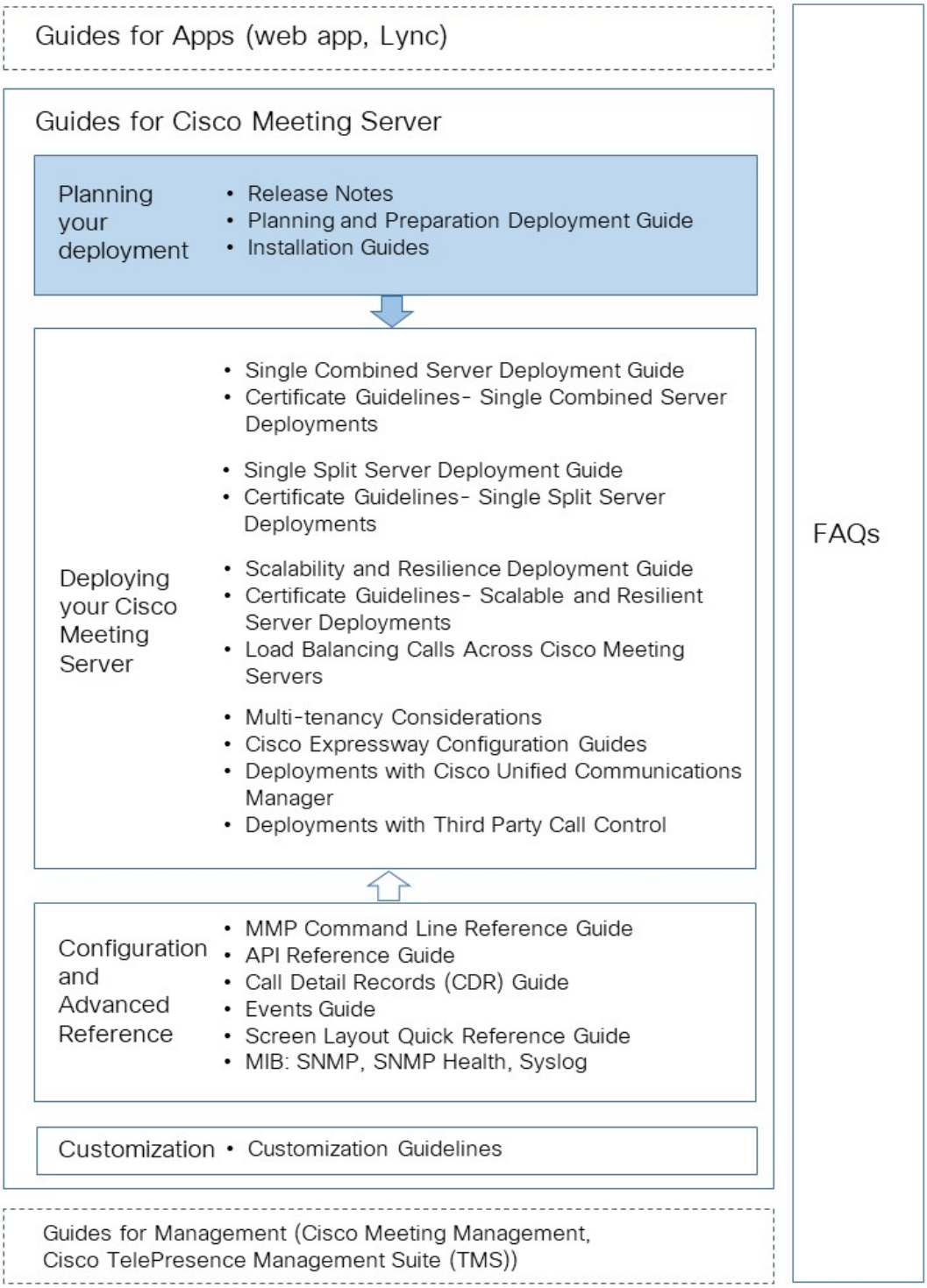
Chapter 2 of this guide provides an overview of the single server deployment model, it identifies the other network components required in the deployment (e.g. NTP servers), and

lists the requirements for the components to work together (e.g. certificates). Chapter 3 covers multiple Meeting Servers in a deployment, we call this the scalable and resilient deployment model. Both chapters reference other documents for the detailed configuration steps.

Figure 1 provides an overview of the documentation covering the Cisco Meeting Server. The guides are available on cisco.com, click on these links:

- Release notes
- Installation Guides
- Deployment Guides
- Configuration and Advanced Reference Guides
- Customization Guide

Figure 1: Overview of guides covering the Cisco Systems Solution



Documentation covering the Cisco Meeting App can be found here.

See Section 1.2 for documentation covering Cisco TelePresence Management Suite and Cisco Meeting Management.

1.1 Configuring the Meeting Server

There are two layers to the Cisco Meeting Server software: a Platform and an Application.

- **The Platform** is configured through the Mainboard Management Processor (MMP). The MMP is used for low level bootstrapping, and configuration via its command line interface. For example, the MMP is used to enable the Web Bridge, Database clustering, and for various other components.
- **The Application** runs on the MMP platform. Administration of the application level (call and media management) can be done via the Call Bridge's Web Admin interface or through the Application Programming Interface (API) if you prefer. The API uses HTTPS as a transport mechanism and is designed to be scalable in order to manage the potentially very large numbers of active calls and spaces available in a deployment.

  From version 2.9, the application level administration can all be done via the Call Bridge's Web Admin Interface both for single and clustered Meeting Servers.

Refer to the deployment guides for configuration details. The MMP and API guides are also useful reference material.

1.1.1 New tools to ease configuring Meeting Server

The following tools are available to help administrators configure and deploy Meeting Server:

- Installation Assistant Simplifies the creation of a simple Cisco Meeting Server installation for demonstrations, lab environments, or as the starting point for basic installations. From version 3.3 onwards, Installation Assistant is not longer a standalone tool. It is integrated with Meeting Management and can be used from the Meeting Management UI.
- Provisioning Cisco Meeting Server web app users through Cisco Meeting Management, available from version 2.9.
- API access through the Meeting Server web interface. From version 2.9, the Meeting Server API can be accessed via the **Configuration** tab of the Meeting Server Web Admin interface. Some examples in this guide have been changed from using API methods POST and PUT, to using API access through the web interface.

Installation Assistant tool

Use the Installation Assistant to simplify the creation of a single Cisco Meeting Server installation for demonstrations, lab environments, or as the starting point for basic installations. The tool configures Meeting Server based on the best practice deployment described in the Cisco Meeting Server Single Server Simplified Deployment guide. From version 3.3 onwards, it is integrated with Meeting Management to collect information about your setup and then

pushes that configuration to the server without you needing to use utilities to access the API, SFTP or the Meeting Server's command line interface. The Installation Assistant can be run from the Meeting Management UI. Refer to the Meeting Management Installation Guide for the software requirements for the client computer, details on installing and running the software, and the steps to configuring a Meeting Server.

Installation Assistant configures Meeting Server to be a SIP MCU capable of making and receiving calls and optionally enables the Cisco Meeting Server web app.

Installation Assistant is intended to be used on an empty, non-configured Meeting Server. It is not a management tool for Meeting Server, nor is it for re-configuring existing Meeting Server installations. The tool is built for configuring Meeting Server virtual machines only. It is not for use with the Cisco Meeting Server 2000 platform.

Using Cisco Meeting Management to provision Cisco Meeting Server web app users

Cisco Meeting Management connected to a Meeting Server or Meeting Server cluster, provides the facility to provision LDAP authenticated Cisco Meeting Server web app users, rather than needing to use the Meeting Server API. The feature also allows admins to create space templates that can be used by web app users to create their own space.

Refer to the Cisco Meeting Management User Guide for Administrators for information on connecting LDAP servers to Meeting Server clusters, how to add one or more user imports, how to create a space template, reviewing and committing the changes and finally running the LDAP sync.

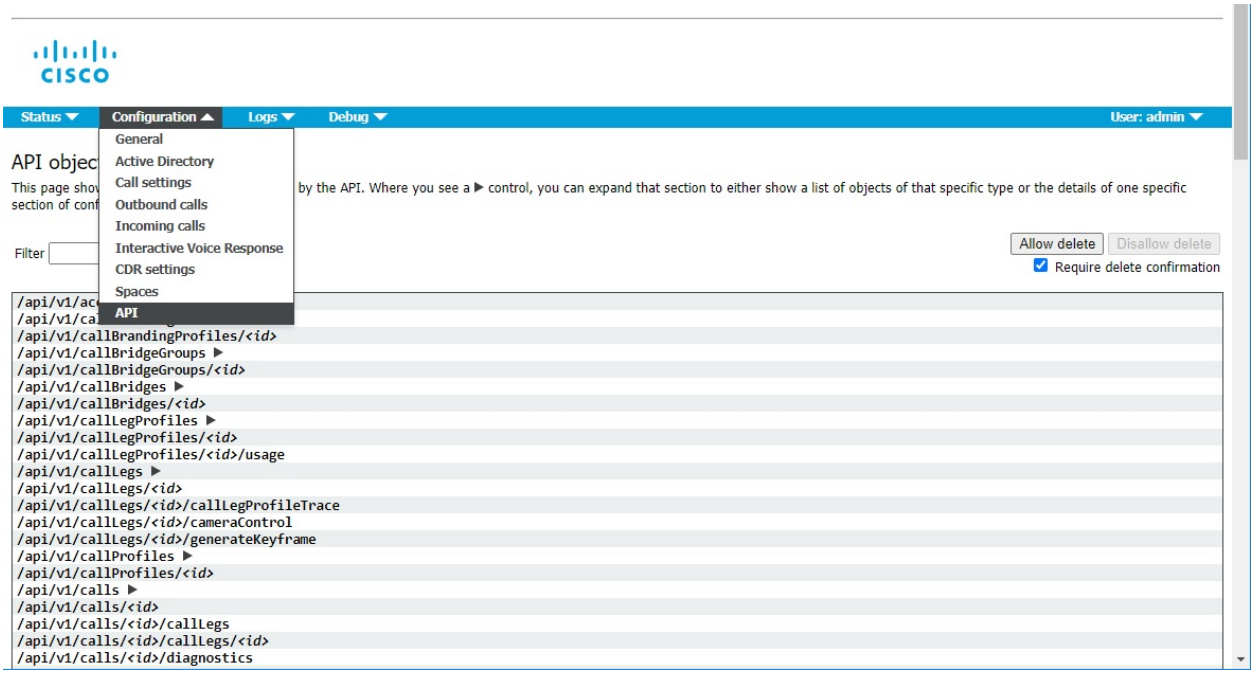
API access on the web interface

To simplify using the Call Bridge API without the need for third-party applications, version 2.9 introduced a user interface for the Call Bridge API that can be accessed via the **Configuration** tab of the Meeting Server web interface, as shown in Figure 2.

The Scheduler APIs introduced in version 3.3 are not supported via this interface. See Accessing Scheduler APIs.

Note: To access the API via the web interface you still need to do the initial Meeting Server configuration settings and authentication using the MMP as you would if you were using a third party application. See the MMP Command reference guide for details.

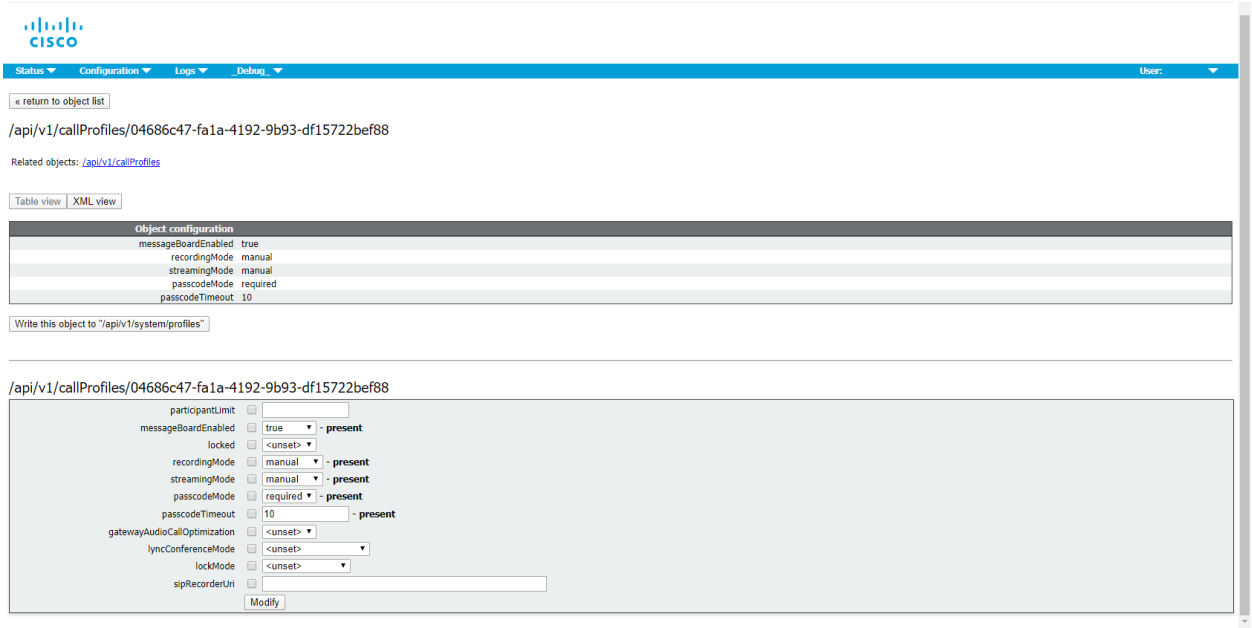
Figure 2: Accessing the Call Bridge API via the Meeting Server web interface



Note: If you wish to delete any configured API objects, select **Allow delete** on the right-hand side of the screen. By default, deletion is disallowed and **Require delete confirmation** is checked to help prevent unintentional deletions.

Using the API via the web interface offers a user-friendly way to work with the API as it gives a more visual approach to configuring your Meeting Server. For example, configuring callProfiles can be achieved using the check boxes and fields shown in Figure 3.

Figure 3: Configuring callProfiles using API access on the web interface



1.2 Managing conferences

Cisco offers several methods for managing conferences hosted on the Meeting Server.They include:

- Cisco TelePresence Management Suite (TMS) version 15.4 onwards,
- Cisco Meeting Management,
- using an Events client,
- using the API of the Meeting Server or the Web Admin Interface (limited functionality).

Cisco TelePresence Management Suite (TMS) version 15.4 onwards supports scheduling calls with Cisco Meeting Server. Scheduled meetings can be setup by each user in the organization using different methods to meet different customers needs, including: Microsoft Outlook with Exchange integration, Web based scheduling using Smart Scheduler, TMS admin interface for help desk booking, and third party applications including Google calendar or Domino Notes. Refer to the Cisco TMS documentation for more details.

Cisco Meeting Management is a management tool for the Meeting Server. It provides a user-friendly browser interface for you to monitor and manage meetings that are running on the Meeting Server, and is currently included within existing Cisco Meeting Server licensing. If you combine Cisco Meeting Management with Cisco TMS (TelePresence Management Suite), you can both schedule and manage meetings that run on Meeting Server Call Bridges. Refer to the Cisco Meeting Management documentation for more details.

Meeting Server can notify an "events client" in real-time of changes that are occurring on the Meeting Server. The Meeting Server acts as a server for the events, and the events client could be for example, a web-based management application. Cisco Meeting Management acts as an events client.

Note: You can construct your own events client, which is similar to constructing an API client. The events client needs to support HTTP and WebSocket libraries, both are available in common scripting languages like Python. The events port on the Meeting Server is the same port as you configured for the Web Admin, typically TCP port 443 on interface A.

Rather than continually poll an API resource on the Meeting Server, an events client can subscribe to an event resource to receive updates. For example, after establishing a WebSocket connection between the events client and the Meeting Server, the events client can subscribe to the event resource **`callRoster`** and receive updates on the participant list of an active conference to find out when a new participant joins, or an existing participant changes layout etc.

1.3 Using the Cisco Expressway-E as the edge device in Meeting Server deployments

Expressway (Large OVA or CE1200) is the recommended solution for deployments with medium web app scale requirements (i.e. 800 calls or less). Expressway (Medium OVA) is the recommended solution for deployments with small web app scale requirements (i.e. 200 calls or less). However, for deployments that need larger web app scale, from version 3.1 we recommend Cisco Meeting Server web edge as the required solution.

For more information on using Cisco Meeting Server web edge solution, see 3.0 or later Deployment Guides.

Cisco Expressway software edge features have been developed to enable the Cisco Expressway-E to be used as the edge device in Meeting Server deployments with small to medium web app scale requirements. Use the TURN server capabilities in Cisco Expressway-E to enable:

- participants using the browser based Meeting Server web app to join conferences hosted on the Meeting Server,
- remote Lync and Skype for Business clients to join conferences hosted on the Meeting Server.

In addition, the Cisco Expressway-E can be used as a SIP Registrar to register SIP endpoints or to proxy registrations to the internal call control platform (Cisco Unified Communications Manager or Cisco Expressway-C).

CAUTION: Important notes for Expressway users
If you are deploying Web Bridge 3 and web app you must use Expressway version X12.6 or later, earlier Expressway versions are not supported by Web Bridge 3.

Table 1 below indicates the configuration documentation that covers setting up Cisco Expressway-E to perform these functions. Table 2 below shows the introduction of the features by release.

Note: If you are configuring dual homed conferencing between on-premises Meeting Server and on-premises Microsoft Skype for Business infrastructure, then the Meeting Server automatically uses the TURN services of the Skype for Business Edge.

Table 1: Documentation covering Cisco Expressway as the edge device for the Meeting Server

Edge feature	Configuration covered in this guide
Connect remote browser based Meeting Server web apps	Cisco Expressway Web Proxy for Cisco Meeting Server Deployment Guide
Connect remote Lync and Skype for Business clients	Cisco Meeting Server with Cisco Expressway Deployment Guide
SIP Registrar or to proxy registrations to the internal call control platform	Cisco Expressway-E and Expressway-C Basic Configuration (X12.6)

Table 2: Expressway edge support for the Meeting Server

Cisco Expressway-E version	Edge feature	Meeting Server version
X12.6	Supports Cisco Meeting Server web app. See Cisco Expressway Web Proxy for Cisco Meeting Server (X12.6)	2.9 and later

1.4 Using the Cisco Expressway-C with the Meeting Server in the core network

In addition to deploying Cisco Expressway-E at the edge of the network, Cisco Expressway-C can be deployed in the core network with the Meeting Server. If deployed between the Meeting Server and an on-premises Microsoft Skype for Business infrastructure, the Cisco Expressway-C can provide IM&P and video integration. In addition the Cisco Expressway-C can provide the following functionality:

- a SIP Registrar,
- an H.323 Gatekeeper,

- Call control in Meeting Server deployments with Call Bridge groups configured to load balance conferences across Meeting Server nodes.

Table 3:Additional documentation covering Cisco Expressway-C and the Meeting Server

Feature	Configuration covered in this guide
Call control device to load balance clustered Meeting Servers	Cisco Meeting Server Load Balancing Calls Across Cisco Meeting Servers
SIP Registrar	Cisco Expressway-E and Expressway-C Basic Configuration (X12.6)
H.323 Gatekeeper	Cisco Expressway-E and Expressway-C Basic Configuration (X12.6)

1.5 Using Call Control

The Meeting Server can be used with Cisco Unified Communications Manager, Cisco Expressway-C or a third party call control platform.

The Cisco Meeting Server with Cisco Unified Communications Manager Deployment Guide details how to configure a SIP trunk between the Meeting Server and Cisco Unified Communications Manager. It explains how to set up scheduled, rendezvous and ad hoc calls between the two devices. The guide also covers support for ActiveControl on the Meeting Server.

The Cisco Meeting Server with Cisco Expressway Deployment Guide details how to configure an Expressway-centric deployment with the Meeting Server.

The Cisco Meeting Server Deployments with Third Party Call Control Guide provides examples of how to configure the Meeting Server to work with third party call control devices from Avaya and Polycom.

2 Single server deployment

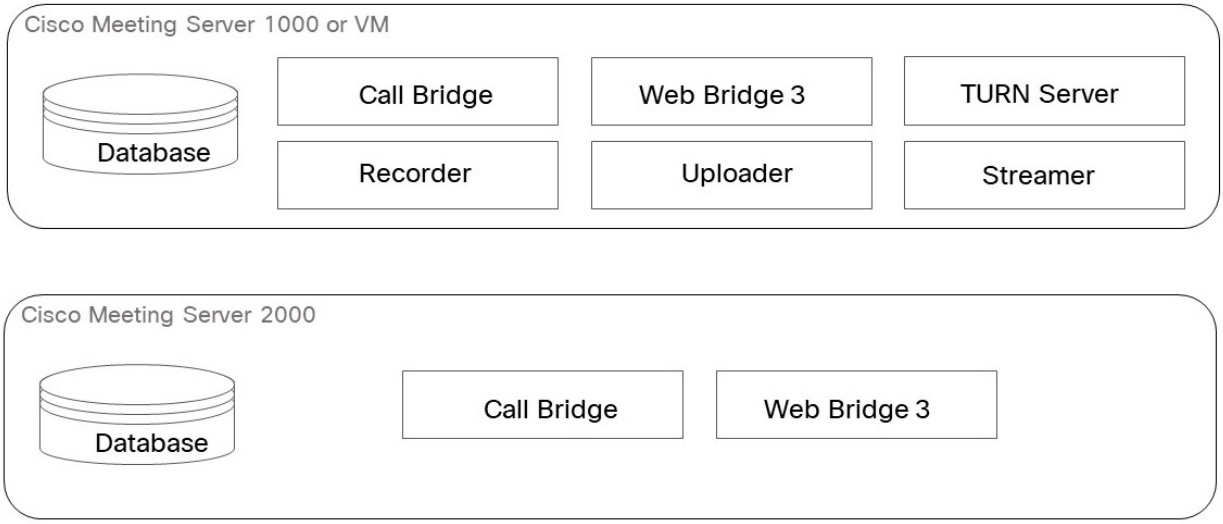
2.1 Overview of Meeting Server components

The Meeting Server comprises a number of components which can be “pick and mixed” to adapt the solution to your video conferencing needs. Figure 4 shows schematically the components on a Meeting Server.

Depending on your deployment you may find that not all of these components need to be enabled and configured.

Expressway (Large OVA or CE1200) is the recommended solution for deployments with medium web app scale requirements (i.e. 800 calls or less). Expressway (Medium OVA) is the recommended solution for deployments with small web app scale requirements (i.e. 200 calls or less). However, for deployments that need larger web app scale, from version 3.1 we recommend Cisco Meeting Server web edge as the required solution which will scale up to SIP capacity.

Figure 4: Components on a Meeting Server



Call Bridge bridges the conference connections, enabling multiple participants to join meetings hosted on the Meeting Server or Lync/Skype for Business AVMCUs. The Call Bridge exchanges audio and video streams so that participants can see and hear each other. The Call Bridge requires a license installed on the Meeting Server before any media calls can be made.

Database The Call Bridge reads from and writes to the database storing the space information, for example the members of spaces, recent activity within a space. In a single server deployment the database is created and managed automatically by the Call Bridge and does not require a specific license or to be enabled.

Web Bridge 3 required if using the Cisco Meeting Server web app. Using the Web Bridge 3 does not require an activation key, but it does require an enabled Call Bridge.

TURN server optional, provides firewall traversal technology, allowing the Meeting Server to be deployed behind a Firewall or NAT if using Cisco Meeting Server web edge solution. To connect to the deployment from Meeting Server web app, external Lync clients, or SIP endpoints registered to a SIP or voice call control device, you need to enable the TURN server.

For more information on using Cisco Meeting Server web edge solution, see 3.1 or later Deployment Guides.

Recorder optional. The internal SIP Recorder component (from version 3.0) on the Meeting Server adds the capability of recording meetings and saving the recordings to a document storage such as a network file system (NFS).

The Recorder should be enabled on a different Meeting Server to the server hosting the conferences, see 2. Only locate the Recorder on the same Meeting Server as the Call Bridge which is hosting the conferences (local) for the purposes of testing the deployment.

Where possible it is recommended that the Recorder is deployed in the same physical locality as the target file system to ensure low latency and high network bandwidth. It is expected that the NFS is located within a secure network.

Note: Depending on the mechanism you use to store the recordings you may need to open external firewall ports so that the recorder, uploader and storage system can communicate. For example: NFS running version 2 or 3 of the port mapper protocol uses TCP or UDP ports 2049 and 111.

Note: Do not use the Firewall component on the Meeting Server if using either the Recorder or Uploader.

Note: At the end of recording a meeting, the recording is automatically converted to MP4. The converted file is suitable for placing within a document storage/distribution system, for example, in a network file system (NFS) they are stored in the NFS folder spaces/<space ID; tenant spaces are stored in tenants/<tenant ID>/spaces/<space ID>.

For VM sizing requirements, see the Installation Guides for Cisco Meeting Server x.x Virtualized Deployments.

Uploader optional, only enable if you are deploying the VBrick Rev portal to enable users to easily identify and download their conference recordings.

Once the Uploader component is configured and enabled, recordings are pushed from the NFS to Vbrick, and an owner is assigned to the recording; no manual importing of recordings is required. The Rev portal applies security configured by your administrator to your video content, only allowing a user to access the content that they are permitted to access. Vbrick

emails the owner when the recording is available in the owner's Rev portal. Owners of a recording access video content through their Rev portal, and can edit and distribute as necessary.

Streamer optional.

The internal SIP Streamer component (from version 3.0) adds the capability of streaming meetings held in a space to the RTMP URL configured on the space.

An external streaming server needs to be configured to be listening on this RTMP URL. The external streaming server can then offer live streaming to users, or it can record the live stream for later playback.

Note: The Streamer component supports the RTMP standard in order to work with third party streaming servers that also support the RTMP standard. Vbrick is the officially supported external streaming server, however, other servers have also been tested.

For VM sizing requirements, see the Installation Guides for Cisco Meeting Server x.x Virtualized Deployments.

2.2 Deployment considerations

The remainder of this chapter outlines the areas to consider before deploying the Meeting Server as a single server deployment. Further details for setting up the Meeting Server for this type of deployment,are provided in the Cisco Meeting Server Single Combined Server Deployment Guide and Cisco Meeting Server with Cisco Expressway Deployment Guide (2.4/X8.11.1).

2.2.1 Summary of devices required

This section provides an overview of the servers typically deployed within a Meeting Server deployment:

- the Meeting Server (for instance the Cisco Meeting Server 2000, or the Cisco Meeting Server 1000). If you are using a VM host it must comply with the host server requirements provided in the Installation Guides for Cisco Meeting Server x.x Virtualized Deployments. Sizing guidelines are also provided in the document.Note: you will need an additional Cisco Meeting Server if you intend to deploy the Recorder or Streamer.
- 1 Network File System (NFS) server if you are deploying the Recorder
- 1 Cisco Expressway pair. Replace the Meeting Server edge components by deploying the Cisco Expressway-E in the DMZ and the Cisco Expressway-C in the internal network, see 1.3 and 1.3 for example deployments.
- 1 Syslog server. The Meeting Server creates Syslog records for troubleshooting issues, these records are stored locally, but can also be sent over TCP to a remote location, for

example a Syslog server. Syslog records are useful during troubleshooting as they contain more detailed logging information than is available on the Meeting Server's own internal log page. The audit log of the Meeting Server, records configuration changes and significant low-level events, these logs can also be sent to the Syslog server. Typical audit log records are changes made to the dial plan or the configuration of a space using the Web Admin Interface or the API, and tagged with the name of the user that made the change along with the respective source IP address and SSH port. This enables identifying the source of events, especially in concurrent sessions.

- 1 NTP server. You must configure at least one NTP (Network Time Protocol) server to synchronize time between the Meeting Server components.
- 1 LDAP server. If you intend to use web app you must have an LDAP server (currently Active Directory, OpenLDAP or Oracle Internet Directory (LDAP version 3)). User accounts are imported from the LDAP server. You can create user names by importing fields from LDAP.
- 1 DNS (Domain Name System) server holding a database of public IP addresses and their associated hostnames. Verify that no A or SRV records already exist for any host Meeting Server before defining the DNS records on this server. Refer to Appendix A in the deployment guides for a table of DNS records needed for the deployment.
- 1 or more (maximum of 4) CDR receivers if you intend to send CDR records to a remote system for collection and analysis (optional). The Meeting Server generates Call Detail Records (CDRs) internally for key call-related events. The Meeting Server can be configured to send these records to a remote system to be collected and analyzed: there is no provision for records to be stored on a long-term basis on the Meeting Server.
- 1 web server to hold customization assets remotely from the Call Bridge which will replace the default files built into the Cisco Meeting Server (optional).

Note: Alternatively, Meeting Server can hold one set of branding files. These locally hosted branding files are available to the Call Bridge and Web Bridge 3 once the Meeting Server is operational, the images and audio prompts replace the equivalent files built into the Meeting Server software. During start up, these branding files are detected and used instead of the default files. However, to use multiple sets of branding files, you need to use an external web server that is reachable by the Call Bridge without performing any form of HTTP authentication. See the Cisco Meeting Server Customization Guidelines for details.

2.2.2 Licensing

Note: Meeting Server 3.0 introduces a mandatory requirement to have Cisco Meeting Management 3.0 (or later). Meeting Management handles the product registration and interaction with your Smart Account (if set up) for Smart Licensing support.

The following features require a license:

- Call Bridge
- Call Bridge No Encryption
- Customizations (for custom layouts)
- Recording or Streaming

In addition to feature licenses, user licenses also need to be purchased, there are 2 different types of user licenses:

- PMP Plus,
- SMP Plus,

For more information on Cisco User Licenses and Smart Licensing, refer to the section on licensing in Chapter 1 of the deployment guides.

2.2.3 Certificate requirements

Certificates and a certificate bundle (or intermediate certificate chain if automatically downloaded from the internet) are required for the:

- Call Bridge (If you are using Lync, this certificate will need to be trusted by the Lync Front End Server; the best way to achieve this is to sign the certificate on the CA (Certification Authority) server that has issued the certificates for the Lync Front End Server)
- Web Bridge 3
- Web Admin Interface
- Recorder
- Streamer

For more information on the type of certificate required (signed by a public CA or signed by an internal CA), see the Certificate Guidelines for a single combined server deployment.

2.2.4 Security

If security is paramount, then consider the following:

- User access control
- Common Access Cards (CAC)
- Online Certificate Status Protocol (OCSP)
- FIPS
- TLS certificate validation with MMP commands
- DSCP
- Verifying SSH fingerprints

Details are provided in the Deployment guides.

User access control: control MMP user accounts and the password rules applied to these accounts. Note: the MMP user accounts provide different levels of access for configuring the Meeting Server, for example: admin, crypto, audit. For more details, see the Cisco Meeting Server MMP Command Line Reference guide.

Common Access Cards (CAC): The Meeting Server supports restricting administrative logins to the SSH and Web Admin Interface using CAC. You need to purchase a CAC enabled version of the Meeting Server software. CAC contains a private key which cannot be extracted but can be used by on-card cryptographic hardware to prove the identity of the card holder.

Online Certificate Status Protocol (OCSP): OCSP is a mechanism for checking the validity and revocation status of certificates. You can use the MMP command **`tls <service> verify ocsp`** to determine whether the CAC used for a login is valid and, in particular, has not been revoked.

FIPS: The Meeting Server provides a FIPS 140-2 level 1 certified software cryptographic module. By enabling FIPS mode, cryptographic operations are carried out using this module and cryptographic operations are restricted to the FIPS approved cryptographic algorithms.

TLS certificate verification: From version 2.3, the Meeting Server uses a minimum of TLS 1.2 and DTLS 1.2 for all services: SIP, LDAP, HTTPS (inbound connections: API, Web Admin and Web Bridge,outbound connections: CDRs). Use the MMP to enable or disable TLS certificate verification. When enabled, if the Meeting Server fails to verify the remote service's certificate, then the connection will be aborted.

Note: If needed for interop with older software that has not implemented TLS 1.2, a lower version of the protocol can be set as the minimum TLS version for the SIP, LDAP and HTTPS services. For more details, see the Cisco Meeting Server MMP Command Line Reference guide.

DSCP: The Meeting Server allows DSCP values to be set for DSCP traffic categories to support Quality of Service (QoS) on IPv4 and IPv6 networks.

For more information on these security measures, see the Cisco Meeting Server Deployment guides.

Verifying SSH fingerprints: Administrators connecting to the Meeting Server for the first time via SSH or SFTP, can verify the keys prompted by the Meeting Server by retrieving the fingerprints of the keys installed on the meeting server before logging in. Use the command **`ssh server_key list`** to retrieve the list of keys installed in the Meeting Server. For more details, see the Cisco Meeting Server MMP Command Line Reference guide.

2.2.5 Port requirements

Appendix B of the Deployment guides shows the required ports between each component of the Meeting Server, and between them and external components.

2.2.6 What Can Be Branded

Some aspects of the participant experience of meetings hosted on Meeting Servers can be branded, they include :

- the web app sign-in background image, sign-in logo, text below sign-in logo, icon, and the text on the browser tab,
- IVR messages,
- SIP and Lync participant's splash screen images and all audio prompts/messages,
- text on the meeting invitation.

If you apply a single brand with only a single set of resources specified (one web app sign-in page, one set of voice prompts, one invitation text), then these resources are used for all spaces, IVRs and Web Bridges in the deployment. Multiple brandings allow different resources to be used for different spaces, IVRs and Web Bridges. Resources can be assigned at the system, tenant, space or IVR level using the API.

3 Scalable and resilient server deployments

3.1 Overview

The flexibility of the Meeting Server architecture enables your deployment to expand as your video conferencing requirements grow. Call capacity can be increased by adding Meeting Servers and clustering the Call Bridges to increase the conference capacity and enable more participants to join a conference. Resiliency can be introduced by siting the Meeting Servers in different locations and geographies, configuring database clustering, and load balancing across Call Bridge groups to ensure an even load distributed across the Call Bridges configured within the group.

Depending on your deployment you may find that not all of the components need to be enabled and configured on all of the Meeting Servers. Typically, Cisco Meeting Server 2000 or Cisco Meeting Server 1000 are used to host the conferencing components - Call Bridge, Web Bridge and Database and VMs are used to host the Recorder, Uploader and Streamer components; but this is not mandatory and the databases can be hosted on a VM.

3.2 Features supporting scaling Meeting Server deployments

Features that support the scaling of deployments include:

- Call Bridge clustering

3.2.1 Call Bridge Clustering

Within a scalable and resilient Meeting Server deployment, you can enable Call Bridge clustering which will allow multiple Call Bridges to operate as a single entity and scale beyond the capacity of any single Call Bridge.

Note: Cisco recommends a maximum of 8 Call Bridges in a single cluster.

You have a choice whether to setup the Call Bridges in the cluster to link peer-to-peer, or for calls to route via call control devices between the clustered Call Bridges.

Linking Call Bridges peer-to-peer:

- reduces call complexity as the call will go from Call Bridge A to Call Bridge B directly, with nothing in the middle to interfere with the routing of the call.
- reduces load on the call control device, and frees up resources to handle calls that need to route through the call control device. This may be important if the call control device is licensed on a per call basis.

Routing via call control device(s):

- creates a consistent call flow for your Meeting Server and Local SIP devices. This can make network configuration a little simpler, particularly if there are firewalls between networks with fixed “allow rules” which only allow calls routed through call control devices.

For more information on how calls are routed in deployments with clustered Call Bridges, refer to the Cisco Meeting Server Scalability and Resilience Deployment Guide.

Note: Clustered Call Bridges cannot use the same database (or database cluster) as a nonclustered Call Bridge.

3.3 Features supporting resiliency in Meeting Server deployments

Features that support resiliency in multi-server deployments include:

- Database clustering
- Call Bridge grouping

3.3.1 Database Clustering

Database clustering works differently to Call Bridge clusters. A database cluster creates what is essentially an 'online' backup of the running database which is maintained as the system runs. It also provides the ability to move to using the backup in an automated fashion in the event of a failure being detected.

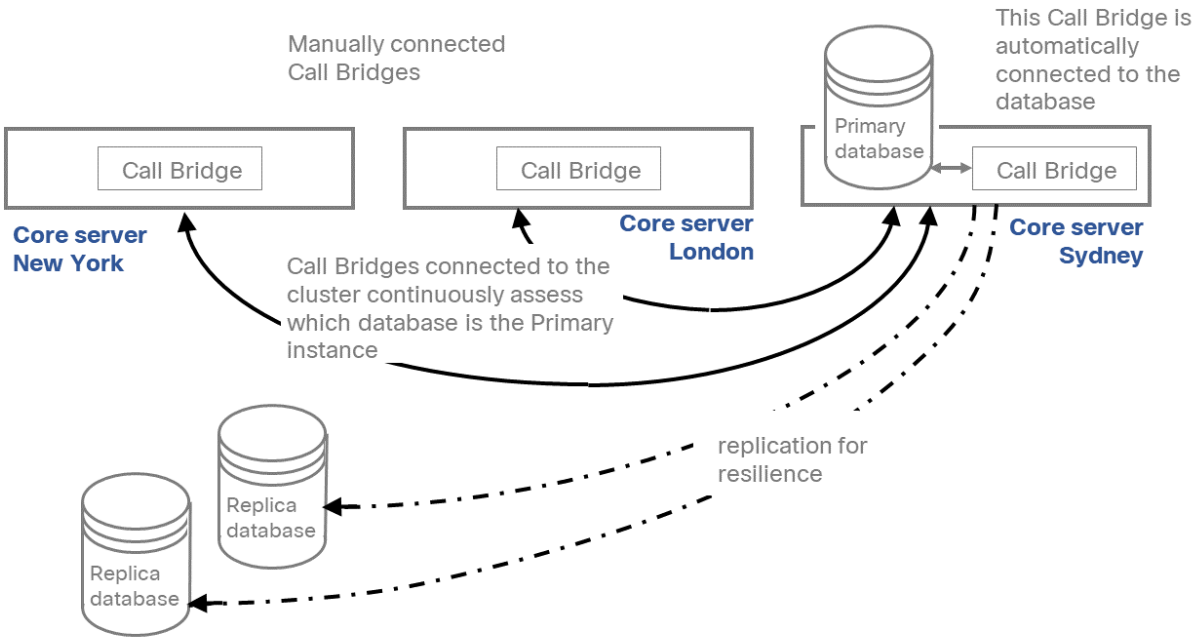
Within a database cluster, only one database is used at any time by all the Call Bridges; this is the “primary”database. All reads and writes are performed on this database instance. The contents of the primary database is replicated to the “replicas/hot-standbys” for resilience. In case of failure of the primary database, a replica database will be "promoted" to being the new primary database, and other replicas will reregister with the new primary database. After the failure has been corrected, the old primary database will assign itself as a replica and will also register with the new primary database.

Database clustering does not do any kind of load balancing, caching, nor sharding of data for more efficient local access within any kind of geographically distributed arrangement. All queries are directed at the primary database, where ever it is. The replicas are not available as read-only instances.

Note: Using an odd number of nodes aids resiliency if a network partitions, and Cisco recommends running a database cluster of 3 nodes. Do not create a database cluster of 2 nodes, as it reduces resiliency rather than increasing it.

For more information on database clustering see the Scalability and Resilience Deployment Guide.

Figure 5: Example of database clustering and Call Bridge connections



3.3.2 Call Bridge Grouping

Deployments with Cisco Unified Communications Manager and clustered Meeting Servers can use the Call Bridge Grouping feature in version 2.1 to load balance calls on the Meeting Servers. Load balancing aims to avoid overloading individual Meeting Servers in the cluster.

Using Call Bridge groups, a Meeting Server cluster can intelligently load balance calls across the Call Bridges within the same location or across nodes in different locations. The intelligent decision making behind where calls end up, is handled by the Meeting Servers. The call control system needs to be able to handle SIP messages from the Meeting Servers, in order to move calls to the correct location. This functionality has been tested using Cisco Unified Communications Manager and Cisco Expressway as call control systems.These are the only Cisco supported call control systems for this functionality. For load balancing with Cisco Expressway, use Cisco Expressway release X8.11 or later with Cisco Meeting Server release 2.4 or later.

For more information on load balancing calls, see the Cisco white paper "Load Balancing Calls Across Cisco Meeting Servers".

Note: There are different call capacities for Meeting Servers in a Call Bridge Group compared to a single or cluster of Meeting Servers. Appendix B provides an overview of the difference in call capacities.

Figure 6: Two example deployments for load balancing incoming calls using Expressway

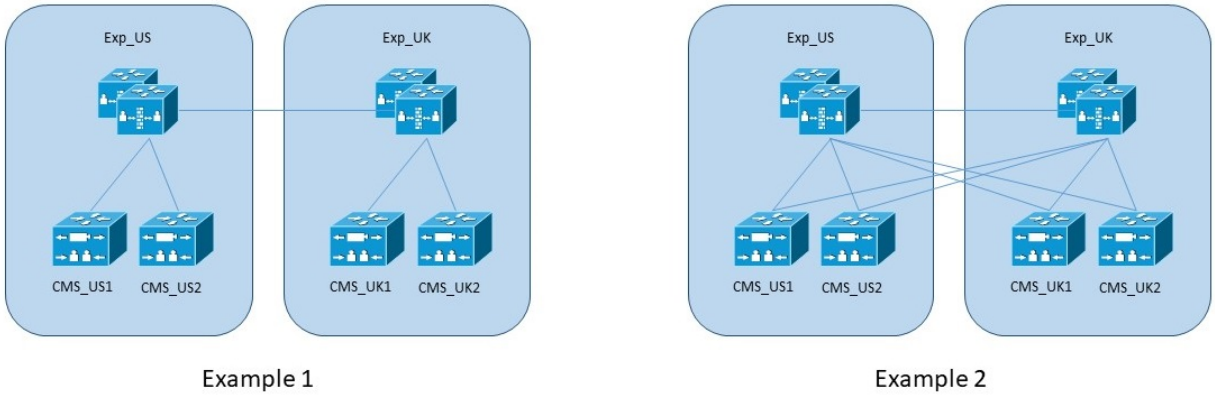
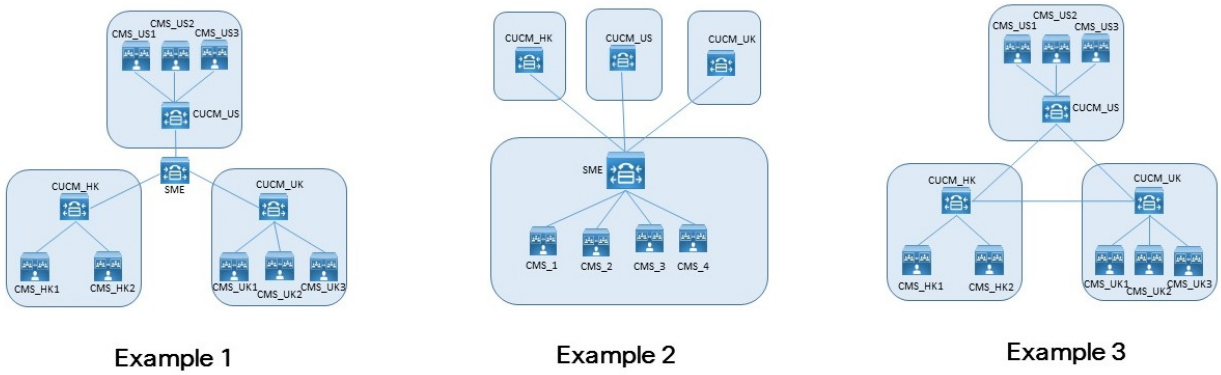


Figure 7: Three example deployments for load balancing incoming calls using Cisco Unified Communications Manager



3.4 Deployment considerations

In addition to the deployment considerations outlined for the single server deployment in Section 2.2, the following points are relevant to multiple Meeting Server deployments.

Further details for setting up the Meeting Server within a scalable and resilient deployment, are provided in the Cisco Meeting Server Scalability and Resilience Deployment Guide and Cisco Meeting Server with Cisco Expressway Deployment Guide (2.4/X8.11.1).

3.4.1 Additional certificate requirements for scalable and resilient deployments

- Host servers for the database. Database clustering uses public/private key encryption for both confidentiality and authentication. Each server hosting the database requires a set of certificates signed by the same CA.

For more information on the type of certificates required (signed by a public CA or signed by an internal CA), see the Certificate Guidelines for Scalable and Resilient Server Deployments.

3.4.2 Additional devices required for scalable and resilient deployments

In addition to the servers mentioned in Section 2.2.1, the deployment will require:

- Multiple Meeting Servers to host conferences. It is not necessary, to have the same number of Web Bridges enabled as Call Bridges. For example, one Call Bridge can manage multiple Web Bridges; those Web Bridges can be reachable externally with a single DNS name resolving to potentially multiple separate units.

  Note: If your deployment design uses more than 8 servers running Meeting Server software, irrespective of which components are running on those servers, contact your Cisco sales representative to have the design validated.

- Additional Meeting Server to host instances of the database. It is not necessary to have a database instance for every Call Bridge. Cisco recommends a maximum of 3 databases in a cluster.
- 1 or 2 NTP servers. Depending upon the configuration of your deployment it might be appropriate to use 2 NTP servers.

Appendix A Technical specifications

A.1 Video standards

Supported video standards:

- H.263+ and H.263++
- H.264 AVC (baseline and high profile)
- H.264 SVC
- WebM, VP8
- Microsoft RTV
- SIP,TIP, H.323 (via Expressway)

A.2 Audio standards

Supported audio standards:

- AAC-LD
- Speex
- Opus
- G.722, G.722.1, G.722.1c, G.728, G.729a, G.711a/u

A.3 Resolution and frame rate

Supported resolution with frame rate:

- Main video : up to 1080p at 60fps
- Content: up to1080p at 30fps

A.4 Bandwidth

Bandwidth consumed:

- Up to 6Mbps

A.5 Call capacity

Table 1 provides a comparison of the call capacities across the platforms hosting Cisco Meeting Server software version 3.0 and later.

Table 4: Call capacities across Meeting Server platforms

Type of calls	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M5v2
Full HD calls 1080p60 video 720p30 content	24	24	30	175	218
Full HD calls 1080p30 video 1080p30/4K7 content	24	24	30	175	218
Full HD calls 1080p30 video 720p30 content	48	48	60	350	437
HD calls 720p30 video 720p5 content	96	96	120	700	875
SD calls 448p30 video 720p5 content	192	192	240	1000	1250
Audio calls (G.711)	1700	2200	2200	3000	3000

Appendix B Call capacities by Cisco Meeting Server platform

Table 5 below details maximum call capacities on Meeting Servers by upgrading to later software versions. Note that there are different capacities for a single or cluster of Meeting Servers compared to load balancing calls within a Call Bridge Group.

Table 5:Evolution in Meeting Server call capacity

Software version		2.9			3.0, 3.1, and 3.2			3.2	
Cisco Meeting Server platform		1000 M4	1000 M5	2000	1000 M4	1000 M5	2000	1000 M5v2	2000 M5v2
Meeting Servers - Individual or in a cluster (notes 1,2 3 and 4) and Meeting Servers in a Call Bridge group	1080p30 720p30 SD Audio	48 96 192 1700	48 96 192 2200	350 700 1000 3000	48 96 192 1700	48 96 192 2200	350 700 1000 3000	60 120 240 2200	437 875 1250 3000
	HD participants per conference per server	96	96	450	96	96	450	120	450
	web app call capacities (internal calling from 3.0 & external calling on CMS web edge from 3.1):								
	Full HD HD SD Audio calls				48 96 192 500	48 96 192 500	350 700 1000 1000	60 120 240 500	437 875 1250 1250
Meeting Servers in a Call Bridge Group	Call type supported	Inbound SIP Outbound SIP Cisco Meeting App							
	Load limit	96,000	96,000	700,000 (note 5)	96,000	96,000	700,000	120,000	875,000

Note 1: Maximum of 24 Call Bridge nodes per cluster; cluster designs of 8 or more nodes need to be approved by Cisco, contact Cisco Support for more information.

Note 2: Clustered Cisco Meeting Server 2000's without Call Bridge Groups configured, support integer multiples of maximum calls, for example integer multiples of 700 HD calls.

Note 3: Up to 16,800 HD concurrent calls per cluster (24 nodes x 700 HD calls) applies to SIP or web app calls.

Note 4: A maximum of 2600 participants per conference per cluster depending on the Meeting Servers platforms within the cluster.

Note 5: From version 3.2, Meeting Server supports increased call capacities on Meeting Server 1000 M5v2 and Meeting Server 2000 M5v2 hardware variants.

- The load limit for Meeting Server 1000 M5v2 has increased from 96,000 to 120,000. The Meeting Server 1000 call capacity for 720p video calls has increased from a maximum of 96 to 120 on the new platform.
- The load limit for Meeting Server 2000 M5v2 has increased from 700,000 to 875,000. The Meeting Server 2000 call capacity for 720p video calls has increased from 700 to 875 on the new platform.

Note 6: Table 5 assumes call rates up to 2.5 Mbps-720p5 content for video calls and G.711 for audio calls. Other codecs and higher content resolution/framerate will reduce capacity. When meetings span multiple call bridges, distribution links are automatically created and also count against a server's call count and capacity. Load limit numbers are for H.264 only.

Note 7: The call setup rate supported for the cluster is up to 40 calls per second for SIP calls and 20 calls per second for Cisco Meeting Server web app calls.

B.1 Cisco Meeting Server web app call capacities

This section details call capacities for deployments using Web Bridge 3 and web app for external and mixed calling. (For internal calling capacities, see Table 5.)

B.1.1 Cisco Meeting Server web app call capacities – external calling

Expressway (Large OVA or CE1200) is the recommended solution for deployments with medium web app scale requirements (i.e. 800 calls or less). Expressway (Medium OVA) is the recommended solution for deployments with small web app scale requirements (i.e. 200 calls or less). However, for deployments that need larger web app scale, from version 3.1 we recommend Cisco Meeting Server web edge as the required solution which will scale up to SIP capacity.

External calling is when clients use Cisco Expressway as a reverse proxy and TURN server to reach the Web Bridge and Call Bridge.

When using Expressway to proxy web app calls, the Expressway will impose maximum calls restrictions to your calls as shown in Table 6.

Note: If you are deploying Web Bridge 3 and web app you must use Expressway version X12.6 or later, earlier Expressway versions are not supported by Web Bridge 3.

Table 6: Cisco Meeting Server web app call capacities – external calling

Setup	Call Type	CE1200 Platform	Large OVA Expressway	Medium OVA Expressway
Per Cisco Expressway (X12.6 or later)	Full HD	150	150	50
	Other	200	200	50

The Expressway capacity can be increased by clustering the Expressway pairs. Expressway pairs clustering is possible up to 6 nodes (where 4 are used for scaling and 2 for redundancy), resulting in a total call capacity of four times the single pair capacity.

Note: The call setup rate for the Expressway cluster should not exceed 6 calls per second for Cisco Meeting Server web app calls.

B.1.2 Cisco Meeting Server web app capacities – mixed (internal + external) calling

Both standalone and clustered deployments can support combined internal and external call usage. When supporting a mix of internal and external participants the total web app capacity will follow Appendix B for Internal Calls, but the number of participants within the total that can connect from external is still bound by the limits in Table 6.

For example, a single standalone Meeting Server 2000 with a single Large OVA Expressway pair supports a mix of 1000 audio-only web app calls but the number of participants that are external is limited to a maximum of 200 of the 1000 total.

B.2 Number of users supported on Cisco Meeting Server

From version 3.3, a Cisco Meeting Server cluster can support up to 300,000 users depending on the servers where the databases are located. All databases in the cluster must be on the same specification server.

Cisco Meeting Server	Maximum number of users
Meeting Server 2000 M5v2	300,000
Meeting Server 2000 M5v1	200,000
Meeting Server 2000 M4, Meeting Server 1000 M4, M5v1, M5v2, and Specification based servers	75,000

Note: LDAP sync for a large number of users can cause an increase in call join times. We advise adding new users/coSpaces onto the Meeting Server during a maintenance window or during off peak hours.

Cisco Legal Information

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

© 2022 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)