Cisco Meeting Server

Deployments with Cisco Expressway X8.11
Planning and Preparation Guide

January 31, 2019
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change History</td>
<td>4</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>5</td>
</tr>
<tr>
<td>1.1 Configuring the Meeting Server</td>
<td>7</td>
</tr>
<tr>
<td>1.2 Managing conferences</td>
<td>7</td>
</tr>
<tr>
<td>1.3 Using the Cisco Expressway-E as the edge device in Meeting Server deployments</td>
<td>8</td>
</tr>
<tr>
<td>1.4 Using the Cisco Expressway-C with the Meeting Server in the core network</td>
<td>10</td>
</tr>
<tr>
<td>1.5 Using Call Control</td>
<td>12</td>
</tr>
<tr>
<td>2 Single server deployment</td>
<td>13</td>
</tr>
<tr>
<td>2.1 Overview of Meeting Server components</td>
<td>13</td>
</tr>
<tr>
<td>2.2 Deployment considerations</td>
<td>15</td>
</tr>
<tr>
<td>2.2.1 Summary of devices required</td>
<td>15</td>
</tr>
<tr>
<td>2.2.2 Licensing</td>
<td>16</td>
</tr>
<tr>
<td>2.2.3 Certificate requirements</td>
<td>16</td>
</tr>
<tr>
<td>2.2.4 Security</td>
<td>17</td>
</tr>
<tr>
<td>2.2.5 Port requirements</td>
<td>18</td>
</tr>
<tr>
<td>2.2.6 What Can Be Branded</td>
<td>18</td>
</tr>
<tr>
<td>2.4 Deployment considerations</td>
<td>15</td>
</tr>
<tr>
<td>2.4.1 Additional certificate requirements for scalable and resilient deployments</td>
<td>24</td>
</tr>
<tr>
<td>2.4.2 Additional devices required for scalable and resilient deployments</td>
<td>24</td>
</tr>
<tr>
<td>2.4.3 Other considerations</td>
<td>25</td>
</tr>
<tr>
<td>2.4.4 API tool</td>
<td>25</td>
</tr>
<tr>
<td>3 Scalable and resilient server deployments</td>
<td>20</td>
</tr>
<tr>
<td>3.1 Overview</td>
<td>20</td>
</tr>
<tr>
<td>3.2 Features supporting scaling Meeting Server deployments</td>
<td>20</td>
</tr>
<tr>
<td>3.2.1 Call Bridge Clustering</td>
<td>20</td>
</tr>
<tr>
<td>3.3 Features supporting resiliency in Meeting Server deployments</td>
<td>21</td>
</tr>
<tr>
<td>3.3.1 Database Clustering</td>
<td>21</td>
</tr>
<tr>
<td>3.3.2 Call Bridge Grouping</td>
<td>22</td>
</tr>
<tr>
<td>3.3.3 XMPP resiliency</td>
<td>23</td>
</tr>
<tr>
<td>3.4 Deployment considerations</td>
<td>24</td>
</tr>
<tr>
<td>3.4.1 Additional certificate requirements for scalable and resilient deployments</td>
<td>24</td>
</tr>
<tr>
<td>3.4.2 Additional devices required for scalable and resilient deployments</td>
<td>24</td>
</tr>
<tr>
<td>3.4.3 Other considerations</td>
<td>25</td>
</tr>
<tr>
<td>3.4.4 API tool</td>
<td>25</td>
</tr>
<tr>
<td>Appendix A Technical specifications</td>
<td>26</td>
</tr>
<tr>
<td>A.1 Video standards</td>
<td>26</td>
</tr>
<tr>
<td>A.2 Audio standards</td>
<td>26</td>
</tr>
<tr>
<td>A.3 Resolution and frame rate</td>
<td>26</td>
</tr>
</tbody>
</table>
A.4 Bandwidth ..............................................................................................................26
A.5 Call capacity .........................................................................................................27

Appendix B Growth in scaling deployments ..............................................................28

Cisco Legal Information .............................................................................................30

Cisco Trademark .........................................................................................................31
## Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 31, 2019</td>
<td>Clarification added to <a href="#">Streamer component support information</a>.</td>
</tr>
<tr>
<td>January 28, 2019</td>
<td>Minor correction to a link.</td>
</tr>
<tr>
<td>January 16, 2019</td>
<td>Minor changes for clarification.</td>
</tr>
<tr>
<td>January 08, 2019</td>
<td>Minor corrections to appendix on scaling deployments</td>
</tr>
<tr>
<td>January 03, 2019</td>
<td>Added appendix on scaling deployments</td>
</tr>
<tr>
<td>December 18, 2018</td>
<td>Minor additions for clarification.</td>
</tr>
<tr>
<td>December 14, 2018</td>
<td>New guide</td>
</tr>
</tbody>
</table>
1 Introduction

The Cisco Meeting Server software can be hosted on specific servers based on Cisco Unified Computing Server (UCS) technology as well as on the Acano X-Series hardware, or on a specification-based VM server. Cisco Meeting Server is referred to as the Meeting Server throughout this document.

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 SIP edge and TURN server components within the Meeting Server. Customers are encouraged to start planning their transition to using Expressway at the edge of their network and the Meeting Server in the core of their network. The SIP edge, TURN server, internal Firewall and H.323 gateway components will be removed from the Meeting Server software at some point in the future.

In addition, Cisco is simplifying the Cisco Meeting Server and Cisco Meeting App interaction, and as a result the app dependence on XMPP will be removed. Once this development is complete, Cisco will remove XMPP from the Cisco Meeting Server product line. Customers are encouraged to start planning the migration to the Cisco Meeting WebRTC app rather than using the Cisco Meeting App thick clients (Windows, Mac and iOS). In the future, the Cisco Meeting WebRTC App and Cisco Jabber will be the supported apps to join Meeting Server hosted conferences, in addition to SIP endpoints, and Lync/Skype for Business clients in dual homed conferences. On withdrawal of the native Cisco Meeting Apps, the XMPP server and Load Balancer components will be removed from the Cisco Meeting Server software.

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
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 components.

- The Application runs on this managed platform with configuration interfaces of its own. The application level administration (call and media management) is done via either the Call Bridge’s Web Admin Interface, or through the API. The Web Admin interface is suitable for configuring a single Call Bridge. To configure multiple Call Bridges you will need to use the API.

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

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.
From version 2.4, the 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

Over the previous few releases of 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. Use the TURN server capabilities in Cisco Expressway-E to connect:

- participants using the WebRTC app to conferences hosted on the Meeting Server,
- remote Lync and Skype for Business clients to 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).

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:** Cisco Expressway-E can not be used to connect remote Cisco Meeting App thick clients (Windows/Mac desktop or iOS) to conferences hosted on the Meeting Server. Nor can the Cisco Expressway-E be used between on-premises Microsoft infrastructure and the Meeting Server. In deployments with on-premises Microsoft infrastructure and the Meeting Server, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization.
**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

<table>
<thead>
<tr>
<th>Edge feature</th>
<th>Configuration covered in this guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect remote WebRTC apps</td>
<td>Cisco Expressway Web Proxy for Cisco Meeting Server Deployment Guide</td>
</tr>
<tr>
<td>Connect remote Lync and Skype for Business clients</td>
<td>Cisco Meeting Server with Cisco Expressway Deployment Guide</td>
</tr>
<tr>
<td>SIP Registrar or to proxy registrations to the internal call control platform</td>
<td>Cisco Expressway-E and Expressway-C Basic Configuration (X8.11)</td>
</tr>
</tbody>
</table>

### Table 2: Expressway edge support for the Meeting Server

<table>
<thead>
<tr>
<th>Cisco Expressway-E version</th>
<th>Edge feature</th>
<th>Meeting Server version</th>
</tr>
</thead>
<tbody>
<tr>
<td>X8.11</td>
<td>Supported:</td>
<td>2.4</td>
</tr>
<tr>
<td></td>
<td>- load balancing of clustered Meeting Servers,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft clients on Lync or Skype for Business infrastructure in other organizations, or Skype for Business clients on Office 365 (not &quot;consumer&quot; versions of Skype),</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- interoperability between on-premise Microsoft infrastructure and on-premise Meeting Server, where no Microsoft calls traverse into or out of the organization,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- standards based SIP endpoints,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- standards based H.323 endpoints,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Cisco Meeting App thin client (Web RTC app) using TCP port 443.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not supported:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- off premise Cisco Meeting App thick clients (Windows/Mac desktop or iOS),</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- interoperability between on-premise Microsoft infrastructure and Meeting Server;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in this scenario, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See [Cisco Meeting Server with Cisco Expressway Deployment Guide (2.4/X8.11.1)]</td>
<td></td>
</tr>
</tbody>
</table>
From version 2.4, you should start migrating your Meeting Server deployments from using the Meeting Server SIP edge component (SIP and Lync Call Traversal feature) and the Meeting Server TURN server, to using the Expressway X8.11 TURN server.

You are encouraged to migrate your Meeting Server deployments from using the Meeting Server edge components to using the Expressway X8.11 (or later) TURN server. The SIP edge, TURN server, internal Firewall and H.323 gateway components will be removed from the Meeting Server software at some point in the future.

### 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration covered in this guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call control device to load balance clustered Meeting Servers</td>
<td>Cisco Meeting Server 2.4+, Load Balancing Calls Across Cisco Meeting Servers</td>
</tr>
<tr>
<td>SIP Registrar</td>
<td>Cisco Expressway-E and Expressway-C Basic Configuration (X8.11)</td>
</tr>
<tr>
<td>H.323 Gatekeeper</td>
<td>Cisco Expressway-E and Expressway-C Basic Configuration (X8.11)</td>
</tr>
</tbody>
</table>

Figure 2 and Figure 3 illustrate recommended Meeting Server deployments. The deployments are discussed in the Cisco Meeting Server deployment guides version 2.4 and later.

Figure 2: Cisco Unified Communications Manager-centric deployment example
Note: When planning the dial plan on Expressway, each Meeting Server in a cluster requires its own neighbour zone on the Cisco Expressway. For more information see Appendix A in the white paper Load Balancing Calls Across Cisco Meeting Servers.

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. The greyed out components will be removed from the Meeting Server software at some future date, they are not discussed in this guide.

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

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** required if using the Cisco Meeting App WebRTC client. Using the Web Bridge does not require an activation key, but it does require an enabled Call Bridge.

- **Recorder** optional, only enable if you intend to allow conferences to be recorded within your deployment and the recordings saved on a document storage system such as a network file system (NFS). The Recorder can be deployed on the same Meeting Server for testing purposes, but must be deployed on a different Meeting Server in production networks. Requires a recording license installed on the Meeting Server hosting the Call Bridge.

The recommended deployment for production usage of the Recorder is to run it on a dedicated VM with a minimum of 4 physical cores and 4GB. In such a deployment, the Recorder should support 2 recordings per physical core, so a maximum of 8 simultaneous recordings. 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.

The recorder uses variable bit rate, so it is not possible to accurately predict how much storage a recording will take. Our testing has shown that the size of 720p30 recordings ranges between 300MB to 800MB for 1 hour. In terms of budgeting it would be safe to assume 1GB per hour.

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, only enable if you intend to allow conferences to be streamed to a streaming service, such as YouTube. The Streamer can be deployed on the same Meeting Server for testing purposes, but must be deployed on a different Meeting Server in production networks. Requires a streaming license installed on the Meeting Server hosting the Call Bridge.

The Streamer component adds the capability of streaming meetings held in a space to the URI configured on the space.

An external streaming server needs to be configured to be listening on this URI. 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. However, we have only tested against Vbrick as an external streaming server.

The recommended deployment for production usage of the Streamer is to run it on a separate VM. This VM should be sized with 1 vCPU and 1GB of memory per 6 concurrent streams, with a minimum of 4 vCPUs and a maximum of 32vCPUs.

**Note:** If you intend to deploy the Recorder and Streamer on the same Meeting Server, you will need to size the server appropriately for both uses.

**XMPP server** optional. The XMPP server handles the XMPP signaling between the Call Bridge and XMPP clients. XMPP clients include the Cisco Meeting Apps, including the WebRTC Client, the Recorder and the Streamer components. If you are planning to use any of these XMPP clients then you will need to configure and enable the XMPP server. However, Cisco is simplifying the Cisco Meeting Server and Cisco Meeting App interaction, and as a result the app dependence on XMPP will be removed. Once this development is complete, Cisco will remove
XMPP from the Cisco Meeting Server product line. Customers are encouraged to start planning the migration to the Cisco Meeting WebRTC app rather than using the Cisco Meeting App thick clients (Windows, Mac and iOS). In parallel, the Recorder and Streamer components will cease to use XMPP to communicate with the Call Bridge.

### 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 (either hosted on a specified UCS server for instance the Cisco Meeting Server 1000, Cisco Meeting Server 2000 or a specified VM host or an Acano X series server). If you are using a VM host it must comply with the host server requirements provided in the [Installation Guides for Cisco Meeting Server 2.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 Figure 2 and Figure 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.

- 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 any of the Cisco Meeting Apps 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, from version 2.5, the Meeting Server can hold one set of branding files. These locally hosted branding files are available to the Call Bridge and Web Bridge 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

You will need activation keys or licenses to use these components on the Meeting Server:

- Call Bridge
- Recording
- Streaming

The XMPP license activation key is now included in the Cisco Meeting Server software.

In addition to the licenses mentioned above, you will also need to purchase Cisco User Licensing. Refer to the section on licensing in Chapter 1 of the deployment guides.

**Note:** From version 2.4 of the Cisco Meeting Server software, you no longer need a branding license if you wish to rebrand the WebRTC, voice prompts and invitation text.

### 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
- XMPP server
- 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

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) and XMPP. 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.

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 WebRTC app sign in background image, sign in logo, text below sign in logo and the text on the browser tab,
- IVR messages,
- SIP/Lync call messages,
- some text on the meeting invitation.

From version 2.4, no license is required to apply single or multiple brands to these customizable features. If you apply a single brand with only a single set of resources specified (one WebRTC 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, the resources can be assigned at the system, tenant, space or IVR level.

Either use the API to apply a single branding or multiple brandings, or use the Web Admin interface if you only wish to apply a single brand to the IVR messages, SIP/Lync call messages or meeting invites. The Customization Guidelines describes the elements that can be branded and explains how to apply the branding files.
Note: The WebRTC app sign in page cannot be rebranded using the Web Admin interface, nor can multiple brandings be applied via the Web Admin Interface.
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, specified UCS servers hosting the software or X-Series servers 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
- XMPP resiliency

#### 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 “master”. All reads and writes are performed on this database instance. This master database’s contents are replicated to the “slaves/hot-standbys” for resilience. In case of master failure, a slave database will be "promoted" to being the new master, and other slaves will reregister with the new master database. After the failure has been corrected, the old master will assign itself as a slave and will also register with the new master.

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 current master, where ever it is. The replicas are not available as read-only instances.

**Note:** Do not create a database cluster of 2 nodes, as it reduces resiliency rather than increase it. Using an odd number of nodes aids resiliency in the case of network partitions, and Cisco recommends running at least 3 database nodes. There is currently a limit of 5 database nodes in a cluster.
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 as a call control system, which is the only Cisco supported call control system 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.
3.3.3 XMPP resiliency

XMPP resiliency provides fail-over protection for a client being unable to reach a specific XMPP server. XMPP resiliency can be configured in multi-server deployments where there are at least three XMPP servers in the deployment.

When setup in resilient mode, the XMPP servers within a deployment are loaded with the same configuration. Each knows the location of the others and they establish links between them. They use keep-alive messages to monitor each other and elect a master. XMPP messages can be sent to any server, messages will be forwarded to the master XMPP server. The XMPP servers continue to monitor each other, if the master fails then a new master is elected and the other XMPP servers forward traffic to the new master.

**Note:** Deployments with only two XMPP servers will not benefit from resiliency, and if one fails it will cause an outage, effectively doubling the risk of failure versus stand-alone mode. This is due to the failover algorithm requiring more than half of the nodes to be available in order for the system to make good decisions about which XMPP server is the master.
Note: Cisco is simplifying the Cisco Meeting Server and Cisco Meeting App interaction, and as a result the app dependence on XMPP will be removed. Once this development is complete, Cisco will remove XMPP from the Cisco Meeting Server product line. Customers are encouraged to start planning the migration to the Cisco Meeting WebRTC app rather than using the Cisco Meeting App thick clients (Windows, Mac and iOS).

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; rather we recommend one at every point of presence.

  Note: There is currently a limit of 5 database nodes in a database cluster.
- 1 or 2 NTP servers. Depending upon the configuration of your deployment it might be appropriate to use 2 NTP servers.

### 3.4.3 Other considerations

**CAUTION:** The maximum number of concurrent XMPP clients supported by the current Meeting Server software is 500. This maximum is a total number of all different clients (Cisco Meeting App, WebRTC Sign-in and WebRTC Guest clients) registered at the same time to clustered Meeting Servers. If the number of concurrent XMPP registrations exceeds 500 sessions, some unexpected problems with sign in may occur or it may lead to a situation where all currently registered users need to re-sign in, this can cause a denial of service when all users try to sign in at the same time.

### 3.4.4 API tool

If your deployment has more that one Meeting Server we strongly recommend using the API to configure them, rather than the Web Admin interface. You will need a web API tool, such as POSTMAN, and a login account and password for the Meeting Server API. The API login password is set up using the MMP command `user add <username> api`. 
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 to 1080p at 30fps

A.4 Bandwidth

Bandwidth consumed:
- Up to 6Mbps
A.5 Call capacity

Table 4: Call capacities on supported servers

<table>
<thead>
<tr>
<th>Supported server</th>
<th>Full HD (1080p30) calls (see note 1)</th>
<th>HD (720p30) calls (see note 1)</th>
<th>SD (448p30) calls (see note 1)</th>
<th>Audio calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Meeting Server 2000</td>
<td>For single or clustered Meeting Servers: 350 (from version 2.4), 250 (prior to version 2.4)</td>
<td>For single or clustered Meeting Servers: 700 (from version 2.4), 500 (prior to version 2.4)</td>
<td>1000</td>
<td>3000 this includes a maximum of 1000 escalated Ad Hoc calls (note 2)</td>
</tr>
<tr>
<td></td>
<td>For a Meeting Server in a Call Bridge group: 250</td>
<td>For a Meeting Server in a Call Bridge group: 500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Meeting Server 1000</td>
<td>48</td>
<td>96</td>
<td>192</td>
<td>3000, this includes a maximum of 1000 escalated Ad Hoc calls (note 2)</td>
</tr>
<tr>
<td>Cisco Meeting Server 2.x running on Multiparty Media 410v</td>
<td>64</td>
<td>128</td>
<td></td>
<td>2000</td>
</tr>
<tr>
<td>Cisco Meeting Server 2.x running on Multiparty Media 400</td>
<td>36</td>
<td>72</td>
<td></td>
<td>1000</td>
</tr>
</tbody>
</table>

Notes:
1) Given call capacities assume 720p5 content, and up to 2.5 Mbps bandwidth
2) Assuming 3 participants (call legs) in an Ad Hoc call. If you create new call legs and destroy them very rapidly, you may find the maximum Ad Hoc calls reduces to 100.
2) Lync video calls into the Call Bridge consume the same resources as SIP calls.
Appendix B  Growth in scaling deployments

Table 5 below demonstrates the expansion in maximum call capacities on Meeting Servers by upgrading to later software versions. Bold indicates a new feature in that software version. Note 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

<table>
<thead>
<tr>
<th>Software version</th>
<th>2.0</th>
<th>2.1</th>
<th>2.2</th>
<th>2.3</th>
<th>2.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Meeting Servers or Meeting Servers in a cluster (notes 1, 2, 3 and 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1080p30</td>
<td>48</td>
<td>NA</td>
<td>48</td>
<td>NA</td>
<td>48</td>
</tr>
<tr>
<td>720p30</td>
<td>96</td>
<td>NA</td>
<td>96</td>
<td>NA</td>
<td>96</td>
</tr>
<tr>
<td>SD Audio</td>
<td>192</td>
<td>NA</td>
<td>192</td>
<td>NA</td>
<td>192</td>
</tr>
<tr>
<td>3000</td>
<td>3000</td>
<td>NA</td>
<td>3000</td>
<td>NA</td>
<td>3000</td>
</tr>
<tr>
<td>HD participants per conference per server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>NA</td>
<td>96</td>
<td>NA</td>
<td>96</td>
<td>100</td>
</tr>
<tr>
<td>WebRTC connections per Web Bridge</td>
<td>100</td>
<td>NA</td>
<td>100</td>
<td>NA</td>
<td>100</td>
</tr>
</tbody>
</table>
## Appendix B  Growth in scaling deployments

<table>
<thead>
<tr>
<th>Software version</th>
<th>Cisco Meeting Server platform</th>
<th>2.0</th>
<th>2.1</th>
<th>2.2</th>
<th>2.3</th>
<th>2.4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1000</td>
<td>2000</td>
<td>1000</td>
<td>2000</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>Meeting Servers in a Call Bridge Group</td>
<td>Call type supported</td>
<td>NA</td>
<td>NA</td>
<td>Inbound SIP</td>
<td>NA</td>
<td>Inbound SIP Outbound SIP</td>
</tr>
<tr>
<td>1080p30 720p30 SD Audio Load limit</td>
<td>NA</td>
<td>NA</td>
<td>48 96 192 3000 96,000</td>
<td>NA</td>
<td>48 96 192 3000 96,000</td>
<td>250 500 1000 3000 500,000</td>
</tr>
<tr>
<td>Note 5</td>
<td></td>
<td></td>
<td>(note 5)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of HD participants per conference per server</td>
<td>NA</td>
<td>NA</td>
<td>96</td>
<td>NA</td>
<td>96</td>
<td>100</td>
</tr>
<tr>
<td>WebRTC connections per Web Bridge</td>
<td>NA</td>
<td>NA</td>
<td>100</td>
<td>NA</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

**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).

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

**Note 5:** A Cisco Meeting Server 2000 with Call Bridge Groups enabled only supports 500 HD calls. The loadLimit for a Cisco Meeting Server 2000 is set at 500,000 due to the total number of video calls supported remaining at 1,000. The Meeting Server does not offer a way to limit the minimum resolution of calls, so it will always be possible to have a mix of HD and lower resolution calls. There is no mechanism to make use of the increased scale in HD or full HD in a load balanced configuration.
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.

© 2018–2019 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)