Cisco Meeting Server

Cisco Meeting Server Release 3.4.1

Release Notes

28 February 2022

Contents

What's changed

Version	Change
February 28, 2022	Maintenance release 3.4.1 See Resolved Issues.
December 17, 2021	Updated Resolved issues section
December 15, 2021	First release for version 3.4.

1 Introduction

This document describes the new features, improvements and changes in version 3.4 of the Cisco Meeting Server software.

The Cisco Meeting Server software can be hosted on:

- Cisco Meeting Server 2000, a UCS 5108 chassis with 8 B200 blades and the Meeting Server software pre-installed as the sole application.
- Cisco Meeting Server 1000, a Cisco UCS server pre-configured with VMware and the Cisco Meeting Server installed as a VM deployment.
- Or on a specification-based VM server.

Throughout the remainder of these release notes, the Cisco Meeting Server software is referred to as the Meeting Server.

Note: Cisco Meeting Management handles the product registration and interaction with your Smart Account for Smart Licensing support. Meeting Management 3.4 is required with Meeting Server 3.4.

- **Upgrade**: The recommended work flow is to first upgrade Meeting Management, complete Smart Licensing, and then upgrade Meeting Server.
- **Smart Licensing**: From the 3.4 release onwards, Smart licensing is mandatory for Meeting Server. The support for traditional licensing has been deprecated. The existing traditional licenses will still be supported until the validity expires. Once the license expires you must migrate to Smart licensing.

For more information on Smart Licensing and upgrading Meeting Management, see Meeting Management Release Notes .

If you are upgrading from a previous version, you are advised to take a configuration backup using the **`backup snapshot <filename>`** command, and save the backup safely on a different device. See the MMP Command Reference document for full details.

Note about Microsoft RTVideo: support for Microsoft RTVideo and consequently Lync 2010 on Windows and Lync 2011 on Mac OS, will be removed in a future version of the Meeting Server software. However, support for Skype for Business and Office 365 will continue.

1.1 Cisco Meeting Server web app Important Information

If you are using Cisco Meeting Server web app (i.e. you have deployed Web Bridge 3), see Cisco Meeting Server web app Important Information for details on when features are released and issues resolved for the web app. These details are not included in the Meeting Server release notes.

The Important Information guide describes the following:

- Any new or changed feature in the web app, and details of fixed issues and open issues associated with the web app with an indication of the version of Meeting Server where this feature/fix is available.
- Any upcoming changes in browsers affecting the web app, and the affected versions of the web app with recommended workarounds.

1.2 End of Software Maintenance

On release of Cisco Meeting Server software version 3.4, Cisco announced the time line for the end of software maintenance for the software in Table 1.

Table 1: Time line for End of Software Maintenance for versions of Cisco Meeting Server

Cisco Meeting Server software version	End of Software Maintenance notice period
Cisco Meeting Server version 2.9.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 2.9.x is March 1, 2022.
Cisco Meeting Server version 3.2.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.2.x is April 17, 2022.

For more information on Cisco's End of Software Maintenance policy for Cisco Meeting Server click here.

2 New features and changes in version 3.4

Version 3.4 of the Meeting Server software introduces the following new features and changes

2.1 Meeting Notes

Version 3.4 introduces the **Meeting Notes** feature that enables web app participants to view and/ or take notes during a meeting and publish it to all other web app participants. This feature is enabled at call level. With this feature:

- In a web app meeting, the participants with appropriate permissions can take and publish notes and other participants can view the published notes.
- Notes can be viewed only during the meeting. Participants joining after a meeting has started can view the recent published note, if any.
- A meeting can have only one published note. Any subsequent changes to the note must be made by editing the published note and republishing it. This will overwrite the previous note and the updated note is sent to all the participants again.
- Notes that are not published are saved as drafts and can be edited and published anytime during the meeting.
- The participant who is taking notes can download and save the notes on their systems during the meeting.

Note:

- This feature is supported only on web app. Participants joining through SIP end points or Lync/Skype cannot view or take notes.
- Though multiple participants can be given permission to take notes on a particular call, we recommend to give permission to only one participant to take the notes to avoid multiple concurrent edits.

2.1.1 API additions

A new API parameter **notesAllowed** is introduced in 3.4 to enable/disable notes at a call level. The acceptable range of values are **true**, **false**. The parameter is supported on the following API methods:

- POST to **/callProfiles**
- GETon **/callProfiles/<call profile id>**
- PUT to **/callProfiles/<call profile id>**
- POST to **/calls**
- GET on **/calls/<call id>**
- PUT to **/calls/<call id>**

Parameter	Type/Value	Description/ Notes
notesAllowed	true| **false**	• true – Indicates that notes is allowed in the call. • false – Indicates that notes is not allowed in the call. The usual rules for the hierarchy of calls and call profiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to false.

Additionally, the administrator can control the participants who are allowed to take the notes in a given call. This is enabled by the new parameter **noteContributionAllowed**. A participant can publish a note if the notes feature is enabled for the call and the participant is allowed to contribute to the notes. The new parameter **noteContributionAllowed** is introduced on the following API methods:

- POST to **/callLegProfiles**
- GET on **/callLegProfiles/<call leg profile id>**
- PUT to **/callLegProfiles/<call leg profile id>**
- POST to **/calls/<call ID>/callLegs**
- GET on **/callLegs/<callLeg id>**

- PUT to **`/callLegs/<callLeg id>`**
- POST to **`/calls/<call id>/participants`**

Note: Even when **`noteContributionAllowed`** is set to **`true`**, if **`notesAllowed`** is set to **`false`** at the call level (or because the call inherited it from the **`callProfile`** hierarchy) then notes will still not be allowed.

Parameter	Type/Value	Description/ Notes
noteContributionAllowed	true| **false**	Determines whether or not the participant can publish notes. If unset at all levels of the hierarchy, then it defaults to false.

For more information on APIs, see *Meeting Server 3.4 API Reference Guide*.

2.2 Security enhancement to validate the certificate name between Call Bridge and Web Admin

The Call Bridge when connecting with their peers in a clustered deployment, are validated using the Web Admin certificates. Web Admin certificates which do not present a trusted chain are rejected, however the certificate names were not validated.

As a security improvement to these existing Call Bridge validations, TLS certificate name verification is implemented between peers. As part of this verification, when **`Call Bridge trust cluster`** is enabled, peers configured on the clustering must match an exact FQDN on its corresponding Web Admin certificate. A mismatch in the configuration will result in Call Bridge failure.

2.3 Rejecting blast dial calls

With Blast dial feature, when any participant dials in to a space, all the other contacts from a preset list in the space are dialed out simultaneously. In earlier releases, when a participant rejects the call, Meeting Management would not stop re-dialing the participant. From version 3.4, the participants can reject the call and Meeting Management will stop re-dialing the participant. A new audio prompt guides the participants with DTMF key options to accept or reject the call. The participants can press DMTF key **1** to enter the meeting or ***** to reject the call. Any other DMTF inputs will be ignored.

Meeting Management will stop re-dialing when:

- The participant accepts the incoming call by clicking **Accept** button and then press DTMF key *****.

- The participant declines the call by clicking **Decline** or **Reject** buttons on a SIP device.
- The participant accepts the incoming call and ends the call by clicking **End call**.

Note: If the user declines the call using **Decline** or **End call** buttons on the PSTN devices, Meeting Management might not stop redialing the participant. It is recommended to use * key to reject calls.

2.3.1 CDR changes

The **`confirmationStatus`** field supported on **`callLegStart`** and **`callLegUpdate`** CDRs is now added to **`callLegEnd`** CDR.

Name	Type	Description
confirmationStatus	required/notRequired/confirmed/rejected	• required: means that confirmation=true was configured and the user has not yet provided the DTMF confirmation to join the call. • notRequired: means that confirmation=true was not configured. • confirmed: means that a DTMF sequence was entered to confirm that the participant wants to join the call. • rejected: means that a DTMF sequence was entered to reject call. The Meeting Management will stop re-dialing the participant.

For more information on the CDRs, see *Meeting Server 3.4 Call Detail Records Guide*.

2.4 Generating log bundle using MMP command

The Meeting Server log bundle is generated when the admin initiates the download process by connecting the SFTP client to the MMP IP address using the MMP admin user credentials. In addition to the existing process, version 3.4 introduces the option to generate the log bundle before initiating the download.

A new MMP command is added to generate the log bundle with a specific file name on the respective Meeting Server. Each time this command is executed the latest log bundle replaces the log bundle that was generated earlier, using this command. The generated log bundle can be downloaded when required.

You can also generate and download log bundle for Call bridges and edge servers using Meeting Management. Refer to *Meeting ManagementRelease notes* for information.

2.4.1 MMP Addition

The following MMP command is added to generate the log bundle for the Meeting Server:

Command/Example	Description/ Notes
`generate_logbundle`	The Meeting Server generates the log bundle file with specific file name, **`generatedlogbundle.tar.gz`** which can be downloaded using the **`SFTP get generatedlogbundle.tar.gz`** command.

For information on using the MMP command, see *Meeting Server 3.4 MMP Command Line Reference Guide*.

2.5 Cisco Meeting Server Scheduler

The Scheduler component was introduced as a beta feature in version 3.3. It was added as a new component that enabled Web app users to schedule meetings, modify the scheduled meetings, and notify participants via email. From version 3.4, Scheduler is fully supported on Meeting Server 1000 and Meeting Server on Virtualized deployments. It is included in the base multiparty licensing (PMP Plus and SMP Plus) and does not require a separate feature license.

Version 3.4 also allows scheduler meeting invites to be sent from a common email address and you can also include the organizer's name as a display name beside the email address to identify the sender. Refer to Configuring email server for Scheduler and Include display name in Scheduler meeting invites for more details on these features.

Note: The scheduler component is not supported on Meeting Server 2000. Call Bridges running on the Meeting Server 2000 are supported in the deployment, but the Scheduler component must run on Meeting Server 1000 or a Meeting Server on VM.

2.5.1 Overview

The Scheduler supports meetings with single and recurring instances. If the meeting template has different roles (such as host and guest), then participants can be assigned to these roles. Web app users can schedule meetings in a persistent space or in a temporary space that is created for the purpose of the meeting. The temporary spaces that are created at the time of scheduling the meeting are deleted by the scheduler component 24 hours after the end of the scheduled meeting, whilst taking meeting recurrences into account. A meeting participant or space member can dial in to this space at any time during the lifetime of the space, even if it is outside the hours of the scheduled meeting. Meeting Server supports multiple meeting series per space.

Email notifications are sent to the participants when a meeting is scheduled or canceled, or the list of participants is modified. If a scheduled meeting is updated, then the updated invitation is sent only to the invitees included by the Scheduler. Email invites can be sent using a common email address. If the common email address is not configured, authentication with the SMTP server requires an email address to be configured using the MMP command **`scheduler email username`**. This account configured on the MMP must have appropriate permissions to be able to send emails on behalf of web app users.

Meeting invitation emails consist of the following:

- Conference join information, which is retrieved by the scheduler using an API call to the Call Bridge. This information is present in the body of the email.
- Meeting details in an industry standard iCalendar (.ics) file attached to the email. The ICS file can be saved by participants to their calendar.

For information on how to customize the email invitation text, see *Meeting Server 3.4 Customization Guidelines*.

Web app users can invite two types of participants to the scheduled meetings:

- Web app participants: The scheduled meetings are visible to web app users when they are signed into the web app. An email invitation will be sent, provided the user's email address was successfully imported during the Call Bridge LDAP sync.
- Email participants: An email address can be specified, for example, to invite someone who does not have a web account. In this case an email invitation will be sent.

The scheduler does not support proposing new times and does not track acceptance or rejection of invitations. For more information on using the Scheduler through web app, see *Meeting Server 3.4 web app User Guide*.

2.5.2 Configuring the email sever for Scheduler

The Scheduler component is supported on Meeting Server 1000 and Meeting Server on VM deployments. For Meeting Server on specification-based VM platforms, an additional 4 GB of RAM is required for running the scheduler component. There is no additional RAM requirement for Meeting Server1000.

In this release, IPv6 is not supported on the Scheduler.

Scheduler supports the following types of email configurations:

1. SMTP
2. SMTP with Authenticated Login (Auth Login)
3. SMTP and STARTTLS
4. SMTP with Auth Login and STARTTLS

5. SMTPS (end to end TLS Encryption for the entire SMTP transaction)
6. SMTPS with Auth Login

For more information about configuration of the email server and types of email configuration, see *Meeting Server 3.4 Installation Guide*.

2.5.3 Deploying the Scheduler

The scheduler is deployed as a new component using the Meeting Server MMP. When the scheduler is enabled, it makes API requests to the Call Bridge over the loopback interface. It is therefore a requirement that the scheduler is deployed on a Meeting Server which is also hosting a Call Bridge. It is not possible to configure the scheduler to use a remote Call Bridge.

It is not necessary to deploy a scheduler alongside every Call Bridge. One scheduler supports 150,000 meetings; two or three schedulers can be added to provide resiliency, but the capacity remains at 150K scheduled meetings. Scheduled meeting data is stored in the Meeting Server database and both clustered and single box database deployments are supported. For more information on deploying the Scheduler, see Meeting Server 3.4 Deployment Guide.

2.5.3.1 API and MMP additions

New API nodes and MMP commands are introduced to support the Scheduler component. See Meeting Server 3.4 API Reference Guide and Meeting Server 3.4 MMP Command Line Reference Guide for more details.

2.5.4 Configure common email address for Scheduler meeting invites

In Version 3.3, when a meeting was scheduled using the Scheduler, the meeting invite was sent to participants from the organizer's email address. This requires that the scheduler can send emails on behalf of users. For organizations that do not want to enable this authority, from version 3.4 meeting invites can be sent to all the participants from a common email address.

A new MMP command is added to configure the common email address on the Meeting Server. Besides configuring the common email address, the command also provides the option to set a display name for the common email address. A name of interest can be configured to be displayed beside the common email address in the email header. The common email address and the display name can have a maximum length of 320 characters and 78 characters respectively.

Further, a new MMP command is added to remove the common email address that is configured on the Meeting Server.

When the meeting invites are sent from a common email address, the recipients would not know the organizer/ host details. Therefore, the organizer/ host name is included in the email invitation text template. A new variable is added in the email invitation template to include the organizer's name or email address in the email invite.

When the Scheduler sends the API request to fetch the email text and meeting joining instructions, the organizer detail is included in the request. This is achieved by including a new request parameter in the Email invitation API.

2.5.4.1 API Additions

The existing API has been modified to include a new request parameter **`organizer`**. This is an optional parameter which can be passed to the API to include the organizer details in the email invitation text.

- GET on **`/api/v1/coSpaces/<coSpace id>/accessMethods/<access method id>/emailInvitation`**
- GET on **`/api/v1/coSpaces/<coSpace id>/emailInvitation`**

Parameter	Type/Value	Description/ Notes
organizer (optional)	String	If provided, includes the organizer details in the email invitation text. The organizer details could be name or email address of the organizer/host as included in the API.

For more information on APIs, see *Meeting Server 3.4 API Reference Guide*.

2.5.4.2 MMP Additions

The following commands are added to configure and remove the common email address on the Meeting Server.

Command/Example	Description/ Notes
`scheduler email common-address <address@mail.domain> "<Display name>"`	Configures the common email address and a display name on the Meeting Server. The Scheduler sends the meeting invites from the common email address to the participants. If the common email address is left blank, the Scheduler sends the email invites from the organizer's email address.
`scheduler email common-address none`	Removes the common email address and display name that has been configured.

For more information on using the MMP command, see *Meeting Server 3.4 MMP Command Line Reference Guide*.

2.5.4.3 Addition to email invitation template text file

A new variable **`organizername`** is added in the email invitation template. The following variable should be added in the **invitation_template_xx_XX.txt** file to include organizer's name in the email invite.

```
#if organizername
Organisator: %organizername%
#endif
```

See *Meeting Server 3.4 Customization Guidelines document* for details.

2.5.5 Include display name in Scheduler meeting invites

In version 3.3, when a meeting invite was sent from the scheduler, the sender details in the email header included only the email address of the organizer. From this version, the organizer's name can be included to appear as display name beside the email address to identify the sender.

When a meeting is scheduled using web app, web app sends the name of the user scheduling the meeting as the organizer display name, to the scheduler. A name of choice can be set as display name by including the new optional parameter in the scheduler API. The display name should not exceed 78 characters.

2.5.5.1 API Additions:

The new **`organizerDisplayName`** API parameter is introduced to include the organizer/ sender's display name in the email header. This parameter is supported on the following method:

- POST to **`/scheduler/meetings`**.

Parameter	Type/Value	Description/ Notes
organizerDisplayName (optional)	String	Meeting organizer's name to be displayed in the email.

For more information on APIs, see *Meeting Server 3.4 API Reference Guide*.

2.6 Move participants to lobby

Earlier versions of Meeting Server provided APIs to admit participants waiting in the lobby in a locked meeting. From version 3.4, Meeting Server provides API to move a participant back to the lobby from a locked meeting.

The existing API parameter **`deactivated`** can be used to move the participants back to the lobby. Additionally, a new parameter **`canMoveToLobby`** is added to indicate if a participant can be moved to lobby or not.

This feature is also supported in Meeting Management 3.4. Refer to CMM Release notes for information.

2.6.1 API Addition

The existing API parameter **`deactivated`** is modified to take both **`true`** and **`false`** values. It is supported on the following methods:

- PUT to **/participants/<participant id>**
- POST to **/calls/<call id>/participants**
- PUT to **/calls/<call id>/participants/***

Parameter	Type/Value	Description
deactivated	true/false	• true - Participant will wait in the lobby or can be moved to the lobby. • false - Participants are allowed into the meeting from the lobby.

A new API parameter **canMoveToLobby** is added to GET on **/participants/<participant id>**.

Response elements	Type/Value	Description/Notes
canMoveToLobby	true/false	• true - Participant can be moved to lobby. • false - Participant cannot be moved to lobby.

The value of the **lockMode** parameter set at the call profile also determines if the admin can move the participants to or from lobby:

- **all**- when the meeting is locked, participants will wait in the lobby if they join after the meeting is locked or participants can be moved to lobby anytime during the meeting. This includes participants who don't need activation.
- **needsActivation** - when the meeting is locked, new participants who don't need activation will enter the meeting and cannot be moved to lobby during the meeting. However new participants who need activation will wait in the lobby and can be moved to lobby anytime during the meeting. Members of a cospace will bypass the lock and enter the meeting even if they require activation as long as there is an activator in the meeting.

For more information on APIs, see *Meeting Server 3.4 API Reference Guide*.

2.7 Closed Captioning

From version 3.4, Meeting server allows web app participants to view and publish closed captions in a meeting. With closed captions, meetings become more accessible for the participants who are deaf or hard-of-hearing. The closed captions published in real time during the meeting are sent by a participant configured as captionist by the Meeting Server admin.

Note: We recommend you to give permission to only one participant in a meeting to publish closed captions.

In a web app meeting, the captions are displayed on the participants screen when the captionist types the captions and presses Enter. Participants can also view the closed caption history in web app on the Closed captions window, which is available as an in-meeting menu option.

Closed captions are not saved on the server and hence are available only during the meeting and lost when it ends. The captionist can download and save the captions to their local drive during the meeting using the UI option on the web app screen.

Note: This feature is supported only on web app. Participants joining through SIP end points or Lync/Skype cannot view closed captions.

2.7.1 API Additions

The new parameter **`captionsAllowed`** is introduced to enable or disable captions at the call level. It is supported on the following methods:

- POST to **`/callProfiles`**
- GET on **`/callProfiles/<call profile id>`**
- PUT to **`/callProfiles/<call profile id>`**
- POST to **`/calls`**
- GET on **`/calls/<call id>`**
- PUT to **`/calls/<call id>`**

Parameter	Type/Value	Description
captionsAllowed	true/false	• true - Indicates that captions are allowed in the call. • false - Indicates that captions are not allowed in the call. The usual rules for the hierarchy of calls and call profiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to false.

Additionally, the new parameter **`captionContributionAllowed`** is added to allow a participant to send captions in a meeting. It is supported on the following methods:

- POST to **`/callLegProfiles`**
- GET on **`/callLegProfiles/<call leg profile id>`**
- PUT to **`/callLegProfiles/<call leg profile id>`**
- POST to **`/calls/<call id>/callLegs`**

- GET on **`/callLegs/<callLeg id>`**
- PUT to **`/callLegs/<callLeg id>`**
- POST to **`/calls/<call id>/participants`**

Parameter	Type/Value	Description
captionContributionAllowed	true/false	Determines whether or not the participant can send captions in a meeting. The usual rules for the hierarchy of callLeg and callLeg profiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to false. Note: If **`captionsAllowed`** is set to **false** at the call level, the participant cannot send closed captions even if **`captionContributionAllowed`** is set as **true**.

Note: Closed captions are always displayed at the bottom of the web app screen. If you are sending both closed captions and message text for the meeting, we recommend that you configure the **`messagePosition`** as **top** or **middle**.

A new API, POST to **`calls/<call id>/captions/`** is introduced to allow third party API tools to send captions in the meeting. Only web app participants can view these captions.

Parameter	Type/Value	Description
captionsText	string	The text to be displayed as caption on the screen in the meeting.

For more information on APIs, see Meeting Server 3.4 *API Reference Guide*.

2.8 Blur your background (Beta Support)

Version 3.4 allows web app participants to blur their background in a meeting. Blurring the background makes the surroundings appear out of focus hence hiding the details behind the participant and emphasizing the participant. Participants can blur their background only after they have joined the meeting and not on the preview page. A new option **Blur** is included in the web app in meeting camera settings. As this is a beta feature, this option is disabled by default.

Note: Cisco does not guarantee that a beta feature will become a fully supported feature in the future. Beta features are subject to change based on feedback, and functionality may change or be removed in the future.

Background Blur is supported only on Mac and Windows with Google Chrome and Mozilla Firefox browsers. This feature is not supported on other browsers and Android or iOS devices.

Note:

- It is recommended to disable HD when background blur is enabled. There might be audio and video sync issues if HD is enabled with background blur.
- Background Blur works best with systems having Graphic Processing Unit (GPU).
- The following minimum system configuration is required to use the Background blur feature:
  - For Windows systems: Memory - 16 GB and CPU - 1.60 GHz
  - For Mac systems: Memory - 16 GB and CPU - 2.30 GHz

2.8.1 API Additions

A New API parameter **`backgroundBlurAllowed`** is introduced to enable or disable background blur at the call level. It is supported on the following methods:

- POST to **`/callProfiles`**
- GET on **`/callProfiles/<call profile id>`**
- PUT to **`/callProfiles/<call profile id>`**
- POST to **`/calls`**
- GET on **`/calls/<call id>`**
- PUT to **`/calls/<call id`**

Parameter	Type/Value	Description
backgroundBlurAllowed	true | **false**	• true - Indicates that background blur is allowed in the call. • false - Indicates that background blur is not allowed in the call. The usual rules for the hierarchy of calls and call profiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to false

For more information on APIs, see *Meeting Server 3.4 API Reference Guide*.

2.9 Far end camera control

Sometimes manual control over camera is required to frame the correct participant in the meeting. Version 3.4 introduces capabilities to control camera of other participants that supports far end camera control (FECC). Only participants with appropriate permissions can control other participant's camera using the new option **View Camera Control** in web app. This option is included for the participants whose camera supports FECC. A participant can only control the camera of a single participant at a time.

The existing API parameters **controlRemoteCameraAllowed** and **cameraControlAvailable** are used to support this feature on web app.

For more information on APIs, see *Meeting Server 3.4 API Reference Guide*.

2.10 Summary of API additions and changes

API functionality for the Meeting Server 3.4 includes the following new and modified API parameters.

New API parameters to support Meeting Notes feature.

- **notesAllowed** is introduced on
  - POST to **/callProfiles**
  - GET on **/callProfiles/<call profile id>**
  - PUT to **/callProfiles/<call profile id>**
  - POST to **/calls**
  - GET on **/calls/<call id>**
  - PUT to **/calls/<call id>**
- **noteContributionAllowed** is introduced on
  - POST to **/callLegProfiles**
  - GET on **/callLegProfiles/<call leg profile id>**
  - PUT to **/callLegProfiles/<call leg profile id>**
  - POST to **/calls/<call id>/callLegs**
  - GET on **/callLegs/<call leg id>**
  - PUT to **/callLegs/<call leg id>**
  - POST to **/calls/<call id>/participants**

New API parameter to include organizer details in the Scheduler meeting invite text when common email address is used

- **organizer** is introduced on
  - GET on **/coSpaces/<coSpace id>/accessMethods/<access method id>/emailInvitation**
  - GET on **/coSpaces/<coSpace id>/emailInvitation**

New API parameter to support display names in Scheduler meeting invites

- **organizerDisplayName** is introduced on
  - POST to **/scheduler/meetings**

New API parameter to show if participant can be moved to lobby or not.

- **canMoveToLobby** is introduced on
  - GET on **/participants/<participant id>**.

New API parameter to support Closed Captions feature.

- **captionsAllowed** is introduced on
  - POST to **/callProfiles**
  - GET on **/callProfiles/<call profile id>**
  - PUT to **/callProfiles/<call profile id>**
  - POST to **/calls**
  - GET to **/calls/<call id>**
  - PUT to **/calls/<call id>**
- **captionContributionAllowed** is introduced on
  - POST to **/callLegProfiles**
  - GET to **/callLegProfiles/<call leg profile id>**
  - PUT to **/callLegProfiles/<call leg profile id>**
  - POST to **/calls/<call id>/callLegs**
  - GET to **/callLegs/<call leg id>**
  - PUT to **/callLegs/<call leg id>**
  - POST to **/calls/<call id>/participants**

New API parameter to support Background Blur feature.

- **backgroundBlurAllowed** is introduced on
  - POST to **/callProfiles**
  - GET on **/callProfiles/<call profile id>**
  - PUT to **/callProfiles/<call profile id>**
  - POST to **/calls**
  - GET on **/calls/<call id>**
  - PUT to **/calls/<call id**

Modification to API objects and parameters

- The maximum limit of the existing API parameter **passcode** on the **/cospace** object has now been modified to accept 63 digits.
- Moving participants to lobby

  The existing API parameter **deactivated** is modified to take both **true** and **false** values. It is supported on the following methods:

  - PUT to **/participants/<participant id>**
  - POST to **/calls/<call id>/participants**
  - PUT to **/calls/<call id>/participants/***

Parameter	Type/Value	Description
deactivated	true/false	• true - Participant will wait in the lobby or can be moved to the lobby. • false - Participants are allowed into the meeting from the lobby.

- Far end camera control

  The existing API parameters **controlRemoteCameraAllowed** and **cameraControlAvailable** are used to support this feature on web app.

New API objects

A new API, POST to **calls/<call id>/captions/** is introduced to allow third party API tools to send captions in the meeting.

2.11 Summary of MMP additions and changes

Version 3.4 supports the MMP additions described in this section.

- Common email address for Scheduler meeting invites

  New MMP commands **scheduler email common-address <address@mail.domain> "<Display name>"** and **scheduler email common-address none** are added to configure and remove common email address from the Meeting Server.

- Generating log bundle using the MMP command

  A new MMP command **generate_logbundle** is added to generate the log bundle with a specific file name **generatedlogbundle.tar.gz**, on the respective **Meeting Server.**

2.12 Summary of CDR Changes

Version 3.4 introduces the following addition to Call Detail Records of the Meeting Server.

- The **`confirmationStatus`** field supported on **`callLegStart`** and **`callLegUpdate`** CDRs is now added to **`callLegEnd`** CDR.

.

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 3.4.1

This section assumes that you are upgrading from Cisco Meeting Server software version 3.3. If you are upgrading from an earlier version, then you must first upgrade to 3.3 following the instructions in the 3.3.x release notes, before following any instructions in this Cisco Meeting Server 3.4.1 Release Notes. This is particularly important if you have a Cisco Expressway connected to the Meeting Server.

Note: Cisco has not tested upgrading from a software release earlier than 3.3.

To check which version of Cisco Meeting Server software is installed on a Cisco Meeting Server 2000, Cisco Meeting Server 1000, or previously configured VM deployment, use the MMP command **`version`**.

If you are configuring a VM for the first time then follow the instructions in the Cisco Meeting Server Installation Guide for Virtualized Deployments.

3.1 Upgrading to Release 3.4.1

The instructions in this section apply to Meeting Server deployments which are not clustered. For deployments with clustered databases read the instructions in this FAQ, before upgrading clustered servers.

CAUTION: Before upgrading or downgrading Meeting Server you must take a configuration backup using the **`backup snapshot <filename>`** command and save the backup file safely on a different device. See the MMP Command Reference document for full details. Do **not** rely on the automatic backup file generated by the upgrade/downgrade process as it may be inaccessible in the event of a failed upgrade/downgrade.

Upgrading the firmware is a two-stage process: first, upload the upgraded firmware image; then issue the upgrade command. This restarts the server: the restart process interrupts all active calls running on the server; therefore, this stage should be done at a suitable time so as not to impact users – or users should be warned in advance.

Note:
Meeting Server 3.0 introduced 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.

To install the latest firmware on the server follow these steps:

1. Obtain the appropriate upgrade file from the software download pages of the Cisco website:

   `Cisco_Meeting_Server_3_4_1_CMS2000.zip`

   This file requires unzipping to a single upgrade.img file before uploading to the server. Use this file to upgrade Cisco Meeting Server 2000 servers.

   Hash (SHA-256) for upgrade.img file:
   2f8a7de6178d98b700ce59f69d73035d3cea0be239d87c5d53f1506face3d6a6

   `Cisco_Meeting_Server_3_4_1_vm-upgrade.zip`

   This file requires unzipping to a single upgrade.img file before uploading to the server. Use this file to upgrade a Cisco Meeting Server virtual machine deployment.

   Hash (SHA-256) for upgrade.img
   file:cba0b5800cc9089b8d29afcc0e5ca9b80d5a54bc02694c6de539ba18ffd942a0

   `Cisco_Meeting_Server_3_4_1.ova`

   Use this file to deploy a new virtual machine via VMware.

   For vSphere6, hash (SHA-512) for Cisco_Meeting_Server_3_4_1.ova: 6.0:
   86d825e3348d98c2fe4e3f2574626126ab71483d8ff48f608ef091dea91470cd10751781e37db881257c78b8d46c830563b0f2bd7f1b56cab29c5fd30ac43d0f

   For vSphere6.5 and higher, hash (SHA-512) for Cisco_Meeting_Server_3_4_1_vSphere-6_5.ova:
   1fdae9fb1bc43ec9d8c9ce1aeefcb442ea01c63b1371868eec5f4e090c9f40a44dde3b56d98e37cea2aa0db5aec18cac1cae3c11662695299139dc49d1f647aa

2. To validate the OVA file, the checksum for the 3.4.1 release is shown in a pop up box that appears when you hover over the description for the download. In addition, you can check the integrity of the download using the SHA-512 hash value listed above.
3. Using an SFTP client, log into the MMP using its IP address. The login credentials will be the ones set for the MMP admin account. If you are using Windows, we recommend using the WinSCP tool.

   Note: If you are using WinSCP for the file transfer, ensure that the Transfer Settings option is 'binary' not 'text'. Using the incorrect setting results in the transferred file being slightly smaller than the original and this prevents successful upgrade.

   Note:
   a) You can find the IP address of the MMP's interface with the **`iface a`** MMP command.
   b) The SFTP server runs on the standard port 22.

4. Copy the software to the Server/ virtualized server.

5. To validate the upgrade file, issue the **upgrade list** command.
   a. Establish an SSH connection to the MMP and log in.
   b. Output the available upgrade images and their checksums by executing the upgrade list command.

      upgrade list
   c. Check that this checksum matches the checksum shown above.
6. To apply the upgrade, use the SSH connection to the MMP from the previous step and initiate the upgrade by executing the **upgrade** command.
   a. Initiate the upgrade by executing the upgrade command.
      upgrade
   b. The Server/ virtualized server restarts automatically: allow 10 minutes for the process to complete.
7. Verify that the Meeting Server is running the upgraded image by re-establishing the SSH connection to the MMP and typing:
   version
8. Update the customization archive file when available.
9. If you are deploying a scaled or resilient deployment read the Scalability and Resilience Deployment Guide and plan the rest of your deployment order and configuration.
10. If you have deployed a database cluster, be sure to run the **database cluster upgrade_schema** command after upgrading. For instructions on upgrading the database schema refer to the Scalability and Resilience Deployment Guide.
11. You have completed the upgrade.

3.2 Downgrading

If anything unexpected occurs during or after the upgrade process you can return to the previous version of the Meeting Server software. Use the regular upgrade procedure to "downgrade" the Meeting Server to the required version using the MMP **upgrade** command.

1. Copy the software to the Server/ virtualized server.
2. To apply the downgrade, use the SSH connection to the MMP and start the downgrade by executing the **upgrade <filename>** command.

   The Server/ virtualized server will restart automatically – allow 10-12 minutes for the process to complete and for the Web Admin to be available after downgrading the server.
3. Log in to the Web Admin and go to **Status > General** and verify the new version is showing under **System status**.

4. Use the MMP command **`factory_reset app`** on the server and wait for it to reboot from the factory reset.
5. Restore the configuration backup for the older version, using the MMP command **`backup rollback <name>`** command.

   Note: The **`backup rollback`** command overwrites the existing configuration as well as the cms.lic file and all certificates and private keys on the system, and reboots the Meeting Server. Therefore it should be used with caution. Make sure you copy your existing cms.lic file and certificates beforehand because they will be overwritten during the backup rollback process. The .JSON file will not be overwritten and does not need to be re-uploaded.

   The Meeting Server will reboot to apply the backup file.

   For a clustered deployment, repeat steps 1-5 for each node in the cluster.

6. a. In the case of XMPP clustering, if applicable, you need to re-cluster XMPP:
   a. Pick one node as the XMPP primary, initialize XMPP on this node
   b. Once the XMPP primary has been enabled, joining any other XMPP nodes to it.
   c. Providing you restore using the backup file that was created from the same server, the XMPP license files and certificates will match and continue to function.
7. Finally, check that:
   - the Web Admin interface on each Call Bridge can display the list of coSpaces.
   - dial plans are intact,
   - XMPP service is connected, if applicable,
   - no fault conditions are reported on the Web Admin and log files.
   - you can connect using SIP and Cisco Meeting Apps (as well as Web Bridge if that is supported).

   The downgrade of your Meeting Server deployment is now complete.

3.3 Cisco Meeting Server Deployments

To simplify explaining how to deploy the Meeting Server, deployments are described in terms of three models:

- single combined Meeting Server – all Meeting Server components (Call Bridge, Web Bridge 3, Database, Recorder, Uploader, Streamer and TURN server) are available, the Call Bridge and Database are automatically enabled but the other components can be individually enabled depending upon the requirements of the deployment. All enabled components reside on a single host server.

- single split Meeting Server – in this model the TURN server and Web Bridge 3 are enabled on a Meeting Server located at the network edge in the DMZ, while the other components are enabled on another Meeting Server located in the internal (core) network.
- the third model covers deploying multiple Meeting Servers clustered together to provide greater scale and resilience in the deployment.

Deployment guides covering all three models are available here. Each deployment guide is accompanied by a separate Certificate Guidelines document.

Points to note:

The Cisco Meeting Server 2000 only has the Call Bridge, Web Bridge 3, and database components. It is suited for deployment on an internal network, either as a single server or a cascade of multiple servers. The Cisco Meeting Server 2000 should not be deployed in a DMZ network. Instead if a deployment requires firewall traversal support for external Cisco Meeting Server web app users, then you will need to also deploy either:

- a Cisco Expressway-C in the internal network and an Expressway-E in the DMZ, or
- a separate Cisco Meeting Server 1000 or specification-based VM server deployed in the DMZ with the TURN server enabled.

The Cisco Meeting Server 1000 and specification-based VM servers have lower call capacities than the Cisco Meeting Server 2000, but all components (Call Bridge, Web Bridge 3, Database, Recorder, Uploader, Streamer and TURN server) are available on each host server. The Web Bridge 3, Recorder, Uploader, Streamer and TURN server require enabling before they are operational.

4 Bug search tool, resolved and open issues

You can now use the Cisco Bug Search Tool to find information on open and resolved issues for the Cisco Meeting Server, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a cisco.com registered username and password.

To look for information about a specific problem mentioned in this document:

1. Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**

   or,

   in the **Product** field select **Series/Model** and start typing `Cisco Meeting Server`, then in the **Releases** field select **Fixed in these Releases** and type the releases to search for example `3.2`.
2. From the list of bugs that appears, filter the list using the *Modified Date*, *Status*, *Severity*, *Rating* drop down lists.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

4.1 Resolved issues

Note: Refer to the Cisco Meeting Server web app Important information guide for information on resolved issues affecting web app.

Issues seen in previous versions that are fixed in 3.4.1.

Cisco identifier	Summary
CSCwa59076	After upgrading to Meeting Server 3.4, users are unable to join a web app meeting with microphone enabled and camera disabled from control panel or while using desktops without inbuilt cameras.
CSCvz75483	In rare cases, version 3.3.0.6 of Meeting Server 2000 crashes with the error message "sf_assert failed server/management/cmgr/server_management_cmgr.cpp:8849" in the syslog file.

Cisco identifier	Summary
CSCwa58708	On September 16, 2021 the Apache Software Foundation disclosed five vulnerabilities affecting the Apache HTTP Server (httpd) 2.4.48 and earlier releases identified by CVE IDs: CVE-2021-40438, CVE-2021-33193, CVE-2021-34798, CVE-2021-36160, CVE-2021-39275. For details on the vulnerabilities, see Apache HTTP Server Vulnerabilities. Cisco has evaluated the impact of the vulnerability on this product and concluded that the product is affected by: • CVE-2021-34798 - NULL pointer dereference in httpd core • CVE-2021-40438 - mod_proxy SSRF However, the product is not affected by the following vulnerabilities: • CVE-2021-33193 - Request splitting via HTTP/2 method injection and mod_proxy • CVE-2021-39275 - ap_escape_quotes buffer overflow • CVE-2021-36160 - mod_proxy_uwsgi out of bound read

Issues seen in previous versions that are fixed in 3.4.

Cisco identifier	Summary
CSCvz91897	Syslog or audit log events can be sent from Meeting Server to configured remote hosts without authentication. A new option **`syslog`** is added to the **`tls`** MMP command, to validate the remote host through certificate authentication.
CSCvz28881	When participants are in a distributed call setup with load balancing enabled on Meeting Server, they are unable to stop the call recording using API.
CSCvz21954	Refer messages can be used to transfer calls before joining the meeting.
CSCvz34846	Meeting Server did not perform an error check to reject alphanumeric values for CallID API parameter.
CSCvy95143	Occasionally in a SIP call, Meeting Server sends and receives an INVITE from the same call dialog at the same time, disconnecting the call due to time out.
CSCvx11659	When the TLS SIP verification is enabled on Meeting Server, it sometimes does not check validity of the received certificate and accetpts invalid or expired certificate.
CSCwa52529	The loadLimit on Meeting Server 2000v2 (M5v2 blade server) shows 700000 while the correct loadLimit for Meeting Server 2000v2 is 850000.

4.2 Open issues

Note: Refer to the Cisco Meeting Server web app Important information guide for information on open issues affecting web app.

The following are known issues in this release of the Cisco Meeting Server software. If you require more details enter the Cisco identifier into the Search field of the Bug Search Tool.

Cisco identifier	Summary
CSCwa40239	When the Email invites are sent using the Scheduler, all the email address in the participant list must be valid. Scheduler might not send emails to any of the participants from the list, even if one of the email address is invalid.
CSCvz01886	When a participant's role does not have permissions to share video and presentation, then the role is changed and they have permissions to share video and presentation, the presentation is not visible to other participants when they share content.
CSCvw61547	On very rare occasions, calls through a Meeting Server TURN component may fail to connect or may lack a media channel. An error similar to " TURN 437 allocation mismatch in state RefreshTurnAllocationPending" will be seen in the Call Bridge syslog.
CSCvt74033	When content is being shared and an event happens to trigger a Webex Room Panorama to drop from sending two video streams to one, the video frame rate being received by a remote endpoint from the Room Panorama can drop noticeably.
CSCvt52420	The mediaProcessingLoad parameter returned in the system/load API on Meeting Server does not correctly account for calls using VP8 codec. When using VP8, there may be a higher actual media load on the Meeting Server than the API reports.
CSCvn65112	For locally hosted branding, if the audio prompt files are omitted then the default built-in prompts are used instead. To suppress all audio prompts use a zero-byte file, rather than no file at all.
CSCvm56734	In a dual homed conference, the video does not restart after the attendee unmutes the video.
CSCvj49594	ActiveControl does not work after a hold/resume when a call traverses Cisco Unified Communications Manager and Cisco Expressway.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.
CSCvh23036	DTLS1.2, which is the default DTLS setting for Meeting Server 2.4, is not supported by Cisco endpoints running CE 9.1.x. ActiveControl will only be established between Meeting Server 2.4 and the endpoints, if DTLS is changed to 1.1 using the MMP command `tls-min-dtls-version 1.0`.

Cisco identifier	Summary
CSCvg62497	If the NFS is set or becomes Read Only, then the Uploader component will continuously upload the same video recording to Vbrick. This is a result of the Uploader being unable to mark the file as upload complete. To avoid this, ensure that the NFS has read/write access.
CSCve64225	Cisco UCS Manager for Cisco Meeting Server 2000 should be updated to 3.1(3a) to fix OpenSSL CVE issues.
CSCve37087 but related to CSCvd91302	One of the media blades of the Cisco Meeting Server 2000 occasionally fails to boot correctly. Workaround: Reboot the Fabric Interconnect modules.

4.2.1 Known limitations

- From version 3.1, Cisco Meeting Server supports TURN short-term credentials. This mode of operation can only be used if the TURN server also supports short-term credentials, such as the Meeting Server TURN server in version 3.1 onwards. Using Cisco Meeting Server with Expressway does not support short-term credentials.

5 Meeting Server platform maintenance

It is important that the platform that the Cisco Meeting Server software runs on is maintained and patched with the latest updates.

5.1 Cisco Meeting Server 1000 and other virtualized platforms

The Cisco Meeting Server software runs as a virtualized deployment on the following platforms:

- Cisco Meeting Server 1000
- specification-based VM platforms.

5.2 Cisco Meeting Server 2000

The Cisco Meeting Server 2000 is based on Cisco UCS technology running Cisco Meeting Server software as a physical deployment, not as a virtualized deployment.

CAUTION: Ensure the platform (UCS chassis and modules managed by UCS Manager) is up to date with the latest patches, follow the instructions in the Cisco UCS Manager Firmware Management Guide. Failure to maintain the platform may compromise the security of your Cisco Meeting Server.

5.3 Call capacities

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

Table 2: 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

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 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

Table 3 provides the call capacities for a single or cluster of Meeting Servers compared to load balancing calls within a Call Bridge Group.

Table 3: Meeting Server call capacity for clusters and Call Bridge groups

Cisco Meeting Server platform		Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M5v2
Individual Meeting Servers or Meeting Servers in a cluster (notes 1, 2, 3, and 4) and Meeting Servers in a Call Bridge Group	1080p30 720p30 SD Audio calls	48 96 192 1700	48 96 192 2200	60 120 240 2200	350 700 1000 3000	437 875 1250 3000
	HD participants per conference per server	96	96	120	450	450
	web app call capacities (internal calling & external calling on CMS web edge): Full HD HD SD Audio calls	48 96 192 500	48 96 192 500	60 120 240 500	350 700 1000 1000	437 875 1250 1250
Meeting Servers in a Call Bridge Group	Call type supported	Inbound SIP Outbound SIP				
	Load limit	96,000	96,000	120,000	700,000	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 21,000 HD concurrent calls per cluster (24 nodes x 875 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: Table 3 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 6: 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.

5.4 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 3.)

5.5 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.

For more information on using Cisco Meeting Server web edge solution, see Cisco Meeting Server 3.1 Release notes.

External calling is when clients use Cisco Meeting Server web edge, or Cisco Expressway as a reverse proxy and TURN server to reach the Web Bridge 3 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 4.

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 4: Cisco Meeting Server web app call capacities – using Expressway for 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.

5.6 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 Table 3 for Internal Calls and if using Cisco Meeting Server web edge solution for external calling. However, if using Expressway at the edge, the number of participants within the total that can connect from external is still bound by the limits in Table 4.

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.

6 Related user documentation

The following sites contain documents covering installation, planning and deployment, initial configuration, operation of the product, and more:

- Release notes (latest and previous releases): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-release-notes-list.html
- Install guides (including VM installation, Meeting Server 2000, and using Installation Assistant): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-guides-list.html
- Configuration guides (including deployment planning and deployment, certificate guidelines, simplified setup, load balancing white papers, and quick reference guides for admins): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html
- Programming guides (including API, CDR, Events, and MMP reference guides and customization guidelines): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html
- Open source licensing information: https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-licensing-information-listing.html
- Cisco Meeting Server FAQs: https://meeting-infohub.cisco.com/faq/category/25/cisco-meeting-server.html
- Cisco Meeting Server interoperability database: https://tp-tools-web01.cisco.com/interop/d459/s1790

7 Accessibility Notice

Cisco is committed to designing and delivering accessible products and technologies.

The Voluntary Product Accessibility Template (VPAT) for Cisco Meeting Server is available here:

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence

You can find more information about accessibility here:

www.cisco.com/web/about/responsibility/accessibility/index.html

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.

Cisco Trademark