Cisco Meeting Server and web app

Release 3.12.2

Release Notes

26 February, 2026

Cisco Systems, Inc.www.cisco.com

Contents

What's changed

Version	Change
February 26, 2026	Maintenance release for 3.12.2 See Resolved issues.

1 Introduction

This document describes the changes in version 3.12.2 of the Cisco Meeting Server software and Cisco Meeting Server web app.

1.1 Cisco Meeting Server

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 , 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 3.12 is required with Meeting Server 3.12.

- **Upgrade**: The recommended work flow is to first upgrade Meeting Management, complete Smart Licensing, and then upgrade Meeting Server.

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.

1.2 Cisco Meeting Server web app

Cisco Meeting Server web app (web app) is a browser-based client for Cisco Meeting Server that lets users join meetings (audio and video) and share what is on their screen.

1.2.1 Using the web app

Web app allows you to join meetings with audio and video in a space. You can also share a screen or presentation in your meeting.

You can add or remove members to a space. You can also invite people both inside and outside of your organization to meetings.

Note: A space is a persistent virtual meeting room that a group of users can use at any time for a meeting. For more details refer to the Online Help or User Guide for web app.

You can use the web app on desktop, mobile or tablet from any of the supported browsers . See list of browsers for details.

Refer to the online help or User Guide for Cisco Meeting Serverweb app for detailed instructions on how to use the web app.

You can choose from the following options based on what you want to do:

- Sign in to the web app - You can sign in to web app, join meetings, view a list of all spaces you are a member of and view joining methods and copy the invitation details to invite someone to your meeting. You can create a space using pre-configured templates, edit or delete a space if you have appropriate permissions.
- Join a meeting - Use this option if you have been invited to a meeting. The invitation should include some details such as a meeting ID, passcode (optional), or a video address (URI).
- Schedule a meeting - To schedule a meeting, click Schedule meeting on the home page. Type a name and the select the space you want to use for the meeting. The meeting can be scheduled for one instance or to recur daily, weekly or monthly. You can add all the members of the selected space or add selected participants and configure their roles for the meeting.

1.3 Smart Licensing

From the 3.4 release onwards, Smart licensing is mandatory for Meeting Server. The support for traditional licensing has been deprecated from 3.4 and later releases. Customers are advised to move to Smart licensing.

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

1.4 End of Software Maintenance

On release of Cisco Meeting Server software version 3.12.2, 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 3.10	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.10.x is April, 2026

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

1.5 Deprecation Notice

Cisco has initiated the process of deprecating support for Skype for Business and TelePresence Interoperability Protocol in the Meeting Server. Support for these features will be removed in a future release. We recommend preparing for the transition to supported alternatives to avoid any disruption in the service.

2 What's new in Cisco Meeting Server

This section of the document lists the following new features and changes implemented in the following Meeting Server releases:

New feature and enhancements in 3.12.1:

- Passcode requirements and validation for coSpaces
- Reintroduction and update of ‘callbridge wc3jwt expiry’ command

New features and changes in 3.12:

- Improved connection resiliency between Meeting Server and Cisco Unified Communications Manager/IMP Server
- Security improvements - Securely storing user data
- API enhancement to rename participants on web app
- Configuring web app user identification
- API enhancements to save chat messages on web app
- API enhancements to apply audio gain at participant level
- Improvements in audio prompt
- Tracking coSpace creation time
- Adding customized help links in web app

2.1 Passcode requirements and validation for coSpaces

Meeting Server now enforces a minimum passcode length of 8 digits for coSpaces. In previous versions, there was no minimum passcode length; for example, if the `minPasscodeLength` parameter was set to 0, no passcode length was enforced.

Setting a **coSpace** passcode remains optional; administrators are not required to configure a passcode unless desired. However, if a passcode is set, it must be between 8 and 63 digits. An error message will be displayed if the passcode does not meet these criteria.

If the minimum passcode length in the **dial-in security profile** was set to less than 8 in the previous version, it is recommended to update it to a value between 8 and 63 digits after upgrading to ensure a seamless workflow.

CAUTION: When upgrading to Meeting Server 3.12.1, all meeting access PINs must have at least 8 digits. If Cisco TelePresence Management Suite scheduled meetings use PINs shorter than 8 digits, they will fail to launch on Meeting Server after the upgrade.

Points to note:

- The minimum passcode length of 8 digits applies to **coSpaces** and **dialInSecurityProfiles**, only when a passcode is configured or modified.
- Existing **coSpaces** and configurations are unaffected unless their passcodes are changed.

The table below outlines the workflows for various scenarios when the passcode is updated.

Scenario	Workflow
Using API	
Created in 3.12 - **coSPace** API with dial-in profiles and passcode set to a length of 6 digits (for example)	After upgrade - **Existing space** – No change until passcode is edited. If the edited passcode is less than 8 digits, an error message is displayed, and passcode rule is applied. **New Spaces** using existing dial- in security profile - The passcode rule is applied with the required minimum passcode length of 8 digits.
coSpace API with new dial-in security profiles	Requires 8 digit minimum passcode length.
coSpace API Without dial-in profiles	**Existing coSpaces** – remains unaffected until the passcode is edited. If Passcode is edited to less than 8, error msg is displayed, and passcode rule is applied. **New coSpaces** - Requires 8 digit minimum passcode/empty passcode
Using portals like CMM/webapp	
coSpaces created using **webapp/CMM** with old template less than 8 digits	Templates use old dial-in profile, and passcode is automatically created based on the specified values. Therefore, passcode rule is not enforced.
coSpaces created using **webapp/CMM** with new template less than 8 digits	Requires 8 digit minimum passcode length.
Meeting Server meetings scheduled via Cisco TelePresence Management Suite	Requires 8 digit minimum passcode length. PINs shorter than 8 digits, will fail to launch on Meeting Server after the upgrade.

The minimum passcode length is enforced on the following API methods:

- Creation/modification of coSpaces
- Creation/modification of accessMethods
- Creation/modification of dialInSecurityProfiles

2.1.1 API Additions

API method	Parameter	Type/value	Description/Notes
POST/PUT on /dialInSecurityProfiles	minPasscodeLength	Number	The minimum allowed passcode length: between 8 to 63 digits in length (inclusive).
POST/PUT on /coSpaces/accessMethods	passcode	Number	The security code for the access method. The minimum allowed passcode length: between 8 to 63 digits in length (inclusive).
POST/PUT on /coSpaces	passcode	Number	The security code for the coSpace. The minimum allowed passcode length: between 8 to 63 digits in length (inclusive).

The above-mentioned passcode also applies to the web app, ensuring consistent passcode validation across all access methods. If a user enters a passcode outside the allowed length range of 8 to 63 digits, the web app displays an appropriate error message.

2.2 Reintroduction and update of ‘callbridge wc3jwt expiry’ command

In Meeting Server version 3.12.1, the **`callbridge wc3jwt expiry`** command has been reintroduced after its earlier removal. This command allows administrators to configure the web app session expiry by setting the timeout value in hours (from 1 to 24). If unset, the default expiry is now 1 hour (previously 24 hours).

CAUTION: This command must be used with caution and only under the guidance of an administrator.

2.2.1 MMP Modifications

Command/Examples	Description/Notes
`callbridge wc3jwt expiry <expiry time in hours>`	Sets the web app session timeout in hours. Accepts integers from 1 to 24. When unset defaults to 1. **Note:** Restart call bridge for the changes to be applied.

Note: Some browsers may pause or stop background tasks after prolonged inactivity, depending on device performance and browser features such as tab-sleeping. If the session expiry is set beyond one hour, the 5-minute " extend session" pop-up may not always appear as expected. The session will still expire at the configured expiry time, but the pop-up notification is subject to browser and system resource management, which cannot be controlled or modified by web app.

2.3 Improved connection resiliency between Meeting Server and Cisco Unified Communications Manager/IMP Server

This release of Meeting Server introduces improvements in connection resiliency between Meeting Server and Cisco Unified Communications Manager (CUCM)/IMP Server, for Jabber users.

When a Jabber user signs into a Cisco Meeting Server web app meeting, Meeting Server dynamically updates the user's presence status in the call using the application user session key. Previously, when an invalid response was received for the presence updates, the Meeting Server failed to update the presence status for the Jabber user and required a manual restart to resume presence updates.

To minimize service disruption and ensure continuous presence updates, the Meeting Server now proactively validates the application session key every 12 hours. Additionally, administrators can configure this validation interval using the new MMP command: **`callbridge imps app_session_refresh_timer`**, where the value can be set between 1 and 24 hours.

2.3.1 MMP additions

Command	Description
callbridge imps app_session_refresh_timer	This command allows Meeting Server to periodically validate the application session in CUCM. Accepted values range from 1 hour to 24 hours. If it is unset, it defaults to 12 hours.

Further, this release significantly enhances Meeting Server's scalability and responsiveness, particularly with CUCM and IMP Server integration. Previously, when users signed in to a meeting from one browser and later joined another meeting from a different browser, it could cause excessive load on the IMPS server and result in 499 timeout errors.

These enhancements reduce HTTP 499 errors and ensure that Presence resets no longer delay user joins, delivering a more stable and scalable meeting experience.

2.4 Security improvements - Securely storing user data

Version 3.12 adds further enhancements to the Meeting Server’s security specifications. Secure storage enhancements continue to be implemented as a configurable option on VM deployments (specification based/ Meeting Server 1000/Small) and can be enabled using the **`secure_ storage enable`**, MMP command.

Note: If upgrading from version 3.11 with secure storage enabled, it is recommended to take a backup of the configuration, to avoid any risk of losing the configuration.

CAUTION: Once enabled, **Secure Storage cannot be disabled** using any command. This operation is **irreversible**. Only a **`<factory_reset full>`** command will reset the secure storage settings, and all the corresponding changes in the system will be reset. Therefore, it is recommended to **take a backup of the configuration** settings using the **`backup snapshot <filename>`** command before enabling secure storage. See the MMP Command Reference document for complete details on taking a backup.

The secure storage improvements introduced in this release include the following improvements:

Character limit on Passphrase to encrypt private keys

Version 3.12 introduces a minimum limit of 14 characters for passphrases on private key encryption using the **`pki encrypt <key> <encrypted-key>`** command. Passphrases may include any combination of letters, numbers, special characters, symbols, or spaces. An error message is displayed if the passphrase is less than 14 characters.

Encrypting backup files

Secure storage enforces encryption of backup files created with the **`backup snapshot <name>`** command. When using **`backup snapshot <name>`**, users are now prompted to encrypt the backup file with a passphrase. The passphrase must be at least 14 characters long and may include any combination of letters, numbers, special characters, symbols, or spaces. These files can be decrypted using the same passphrase during rollback.

Note: Once Secure Storage is enabled, the backup file is automatically encrypted by default, so no further encryption is necessary.

Additionally, if the user chooses to download the backup files using SFTP, secure storage enforces encryption for backup file downloads. A new MMP command, **`backup encrypt <name> <encrypted-name>`**, has been added to encrypt the backup files before downloading; else, permission to download these files will be denied.

Support for FIPS mode

With this release Secure Storage supports FIPS, when enabled.

Note that when FIPS is enabled, private key files created in the previous release (3.11) with a shorter passphrase must be regenerated using a minimum 14-character passphrase.

2.4.1 MMP additions and modifications

The following command is added as part of this implementation:

Command	Description
`backup encrypt <name> <encrypted-name>`	This command encrypts the backup files while downloading them using SFTP. The command prompts the user to enter a minimum 14-character passphrase that may include any combination of letters, numbers, special characters, symbols, or spaces. It is recommended to use a new file name rather than reusing an existing file name.

The below mentioned backup command is modified to provide additional details accordingly.

Command	Description
`backup list`	The command is modified to include encryption status and the original file name from which it is encrypted.

2.5 API enhancement to rename participants on web app

Version 3.12 introduces a new API that will authorize web app participants to modify the display names during an ongoing meeting. With the new permission controls, authorized participants can rename themselves or other participants, including those waiting in the lobby.

2.5.1 API Additions

A new API, `renameParticipantAllowed`, has been introduced and is managed through **callLegProfile** on the following API methods.

POST to **/callLegprofiles**

PUT to **/callLegprofiles/<callLegprofileID>**

Parameter	Value	Description
`renameParticipantAllowed`	none	Participants cannot rename display names. If unset defaults to **none**.
	self	Participants can rename their own display name.
	participants	Participants can rename themselves and others, including those in the lobby.

Refer Rename participants for details on using the feature in web app.

2.6 Configuring web app user identification

In Cisco Meeting Server web app version 3.11, visual indicators were introduced in the **Participant list** to identify the joining methods of each participant, such as ✓ for signed-in users, ? for non-signed-in users, and 💻 for SIP users.

In version 3.12, Meeting Server adds configurability to this feature by introducing a new API parameter, `showParticipantIndicator`. This parameter enables administrators to control the visibility of the user identification icons in the web app participant list.

2.6.1 API additions

API parameter, `showParticipantIndicator`, is introduced on `webBridgeProfiles` at the global level. This parameter enables administrators to display or hide the user identification icons.

- POST to **/webBridgeProfiles**
- PUT on **/webBridgeProfiles/<web bridge profile id>**
- GET on **/webBridgeProfiles/**

Parameter	Type/value	Description
`showParticipantIndicator`	**True**/False	Displays or hides the user identification icons in the Participant list. **True** – Displays the user identification icons. **False** – Hides the user identification icons.

2.7 API enhancements to save chat history on web app

From version 3.12, web app participants with required permission can download and save their chat messages during a web app meeting. Administrators can assign the required permission using the new API, `allChatSave`.

2.7.1 API additions

The `allChatSave` parameter is introduced on the following **callLegs** and **callLegprofiles** API methods:

- POST to **/calls/<call ID>/callLegs**
- PUT to **/callLegs/<callLegID>**

- POST to **/callLegprofiles**
- PUT to **/callLegprofiles/<callLegprofileID>**

Parameter	Type/value	Description
allChatSave	True/**False**	**True** – Web app participant can download and save chat messages in .txt format. **False** – Web app participant cannot download and save chat messages.

Refer *Save chat history* for details on using the feature in web app.

2.8 API enhancements to apply audio gain at participant level

Meeting Server now supports applying fixed audio gain for specific participants during an ongoing meeting. Administrators can control the audio output of endpoints with very low or high audio levels.

A new **audioGainDb** parameter has been introduced on **callLegs** and **callLegProfile** API methods, as well as in the **callRoaster** resource of subscribable events. This parameter accepts positive and negative values, where positive represents increase in volume and negative represents decrease in volume.

The gain from the **audioGainDb** parameter operates independently of the **audioGainMode** parameter. However, the effective volume depends on whether **audioGainMode** parameter is enabled in the **callLeg** profile. If set to AGC, the fixed gain from the **audioGainDb** is applied after the automatic gain control.

API additions

A new **audioGainDb** parameter is introduced on the following **callLegs** and **callLegprofiles** API methods:

- POST to **/calls/<call ID>/callLegs**
- PUT to **/callLegs/<callLegID>**
- POST to **/callLegprofiles**
- PUT to **/callLegprofiles/<callLegprofileID>**

Parameter	Type/value	Description
audioGainDb	Numeric/Integer	This parameter sets the Gain value in decibels for a specific participant. The value must be entered in multiples of ten. For example, enter 60 to achieve a gain value of 6 dB. It accepts positive (volume increase) and negative (volume decrease) values, within a range of +60 to – 60. Note: **audioGainDb** when modified via **callLegProfile** will not be applied unless and until modified after the **callLeg** has been established.

Events record changes

The **audioGainDb** parameter is added to **callRoster** resource of subscribable events.

Parameter	Type/value	Description
audioGainDb	Numeric/Integer	The Gain value applied for a particular participant.

2.9 Improvements in audio prompt

Meeting Server has been improved for better audio prompt handling to ensure the co-space join prompt is only played once when users connect via IVR or join PIN-protected Spaces.

2.10 Tracking coSpace creation time

From version 3.12, the GET operation on a coSpace retrieves its creation time and owner details, which helps in tracking when the coSpace was created and by whom. This information is also displayed on the Spaces page under Configuration menu option in WebAdmin.

Note: For coSpaces created before the version 3.12 upgrade, the **creationTime** will display the upgrade date. However, the **ownerJid** will not be included.

API modifications

The following response elements will be returned in the GET operation on coSpace.

Response elements	Type/value	Description/Notes
creationTime	String	Date and time when the space is created; displayed in yyyy-mm-dd hh:mm:ss format based on the Coordinated Universal Time (UTC) regardless of the selected time zone.
ownerJid	String	The owner of the coSpace identified by their specific Jid.

2.11 Adding customized help links in web app

Version 3.11 introduced the ability to configure the Meeting Server to redirect web app’s default help link to display the custom pages. This was introduced as a beta feature. From this release of Meeting Server, this is a fully supported feature and will not require customization license.

This feature is supported on the web app only.

To redirect the help pages to external custom help pages, add **brand_external_help_link** in the **text_strings_xx_XX.json** file. When the user clicks on the ⍰ help icon, they are directed to the custom help link provided in this file. However, if the link to the external help pages is not added, then the help icon directs to the default online help pages.

Note: The custom help page configured in the Meeting Server will replace every help link across the web app. This includes the sign-in page, in-meeting page, and cookie notification page. Therefore, when the custom help link is set in the Meeting Server, the administrators must ensure it has all the required information. In case of an invalid URL or multiple URLs, the custom help page displays an error message.

2.12 Summary of API additions and changes

API functionality for Meeting Server 3.12 includes the following new API parameters.

The following API parameter is added to rename participants:

`renameParticipantAllowed` is introduced on the callLegProfile:

- POST to /callLegprofiles
- PUT to /callLegprofiles/<callLegprofileID>

The following API parameter is added to display or hide the user identification icons.

`showParticipantIndicator` is introduced `webBridgeProfiles` at the global level:

- POST to **/webBridgeProfiles**
- PUT on **/webBridgeProfiles/<web bridge profile id>**
- GET on **/webBridgeProfiles/**

The following API parameter is added to download and save the chat messages during a web app meeting.

The `allChatSave` parameter is introduced on the following **callLegs** and **callLegprofiles** API methods:

- POST to **/calls/<call ID>/callLegs**
- PUT to **/callLegs/<callLegID>**
- POST to **/callLegprofiles**
- PUT to **/callLegprofiles/<callLegprofileID>**

The following API parameter is added to apply fixed audio gain for specific participants during an ongoing meeting.

A new **`audioGainDb`** parameter is introduced on the following **callLegs** and **callLegprofiles** API methods:

- POST to **/calls/<call ID>/callLegs**
- PUT to **/callLegs/<callLegID>**
- POST to **/callLegprofiles**
- PUT to **/callLegprofiles/<callLegprofileID>**

The GET operation on a coSpace retrieves its creation time and owner details.

The following response elements will be returned in the GET operation on coSpace.

2.13 Summary of MMP additions and changes

The following command is added to improve connection between Cisco Meeting Server and Cisco Unified Communications Manager/IMP Server, where the value can be set between 1 and 24 hours.

Command	Description
`callbridge imps app_session_refresh_timer`	This command allows Meeting Server to periodically validate the application session in CUCM. Accepted values range from 1 hour to 24 hours. If it is unset, it defaults to 12 hours.

The following commands are added as part of the **Secure storage** enhancement:

CAUTION: Once enabled, **Secure Storage cannot be disabled** using any command. This operation is **irreversible**. Only a **`<factory_reset full>`** command will reset the secure storage settings, and all the corresponding changes in the system will be reset. Therefore, it is recommended to **take a backupof the configuration** settings using the **`backup snapshot <filename>`** command before enabling secure storage.

The following command is added to regenerate private key files, when FIPS is enabled, with shorter passphrase using a minimum 14-character passphrase.

Command	Description
`backup encrypt <name> <encrypted-name>`	This command encrypts the backup files while downloading them using SFTP. The command prompts the user to enter a minimum 14-character passphrase. It is recommended to use a new file name rather than reusing an existing file name.

The following backup command is modified to provide additional details accordingly.

Command	Description
`backup list`	The command is modified to include encryption status and the original file name from which it is encrypted.

2.14 Summary of Event record Changes

The `audioGainDb` parameter is added to callRoster resource of subscribable events.

Parameter	Type/value	Description
`audioGainDb`	Numeric/Integer	The Gain value applied for a particular participant.

2.15 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

3 What's new in Cisco Meeting Server web app

This version of the web app software introduces the following new features and changes:

Enhancements in 3.12.1:

- Edge browser support for web app session timeout

New features and changes in 3.12:

- Web app session timeout
- Rename participants
- Refreshed user interface
- Save chat history
- Meeting invite links for members-only space

3.1 Edge browser support for web app session timeout

Version 3.12 introduced a web app session expiry of 60 minutes if participants are inactive or switch to another tab. This feature was initially supported only on Chrome, Firefox, and Safari browsers. From version 3.12.1, it is also supported on Edge browser.

3.2 Web app session timeout

From version 3.12 web app sessions are set to expire after 60 minutes. At the 55-minute mark, if the participant is inactive or active in another tab, a notification pop-up will appear, allowing the participant to choose either stay signed in or sign out. If the participant becomes active in the web app tab after the pop-up appears and before the session expires, the session will automatically refresh, and the pop-up will be dismissed.

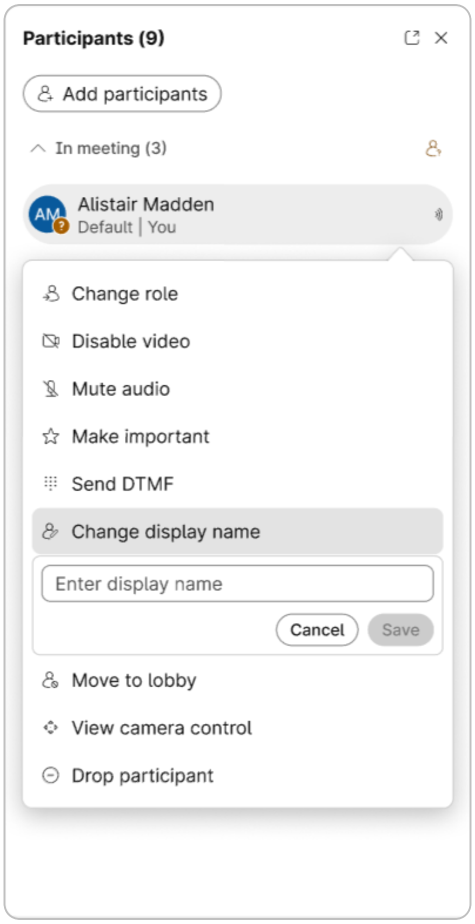
Note:

- The pop-up notification will appear only on desktop browsers for Windows or macOS and will not be shown on mobile devices.
- This feature is supported on Chrome, Firefox and Safari browsers only.
- In macOS, when the Firefox window is maximized in a separate window, the pop-up notification may appear in another tab. However, the user will not be automatically redirected to the Firefox window where the pop-up is shown. As a result, if the user is not actively engaged with that window, they may remain unaware of the pop-up notification.

- The behavior described above is determined by the system's functionality when in full screen mode and cannot be controlled or modified by the web app.

3.3 Rename participants

From version 3.12, meeting hosts or participants with appropriate permissions can now modify their display names or those of other participants during a meeting, including participants waiting in the lobby. A new option, **Change display name**, has been added to the Participants list window. Participants will receive a notification whenever their display name is changed.



Note:

- Display name is limited to a maximum of 80 characters.
- The name change is also reflected in the video layout label.
- Participants are notified of name changes only while in the meeting, not while in the lobby.
- The display name does not update if a user changes the name only by altering the letter case. For example, " sally wood" to " Sally Wood" or vice versa.

- If a participant gets disconnected, their display name is reverted to the original name even if the participant gets reconnected automatically by the web app. Such participants will need to be renamed again upon reconnection.
- The **Change display name** option will not appear for participants without necessary permissions. Refer *API enhancements to rename participants on web app* for details on providing permissions in the Meeting Server.

3.4 Refreshed user interface

From version 3.12, web app introduces a refreshed user interface with enhanced visual appearance like updated colors, fonts, and icons.

3.5 Save chat history

Web app now allows participants with the appropriate permissions to export meeting chat history as a .txt file. The export functionality helps participants save and review chat content locally.

During an active meeting, participants can click the **Save** button in the **Chat** window; upon clicking, a .txt file is downloaded containing all chat messages visible to the participant up to that moment. The **Save** button will be accessible at any time during the meeting.

The exported file name follows the naming convention:

```
<SpaceName>-<Chat History>-<Day Date Time Timezone>.txt
```

The exported file includes:

- **Sender** and **receiver** names
- **Timestamps** for each message
- **Message content**

Note:

- Only participants with the **`allChatSave`** permission enabled (at callLegProfile level) in the Meeting Server can see the **Save** button and export the chat.
- Participants can export the chat history multiple times; each export reflects the chat content visible at the point of export.

3.6 Meeting invite links for members-only space

In previous versions of the web app, signed-in space members could not join a meeting scheduled in a members-only space directly via the meeting invite link. Instead, they were required to click the 'Join meeting' button within the respective space in the web app.

From version 3.12, clicking on the link will take the signed-in space members directly to the meeting lobby page. No additional sign-in steps are needed if they’re already logged in. However, when non-members use the invite link to join a space meeting, web app notifies with appropriate message that the access is restricted to members only.

3.7 Browser versions tested

Table 2 lists the browsers tested for web app at the time of release of a specific version of web app.

We always recommend using the latest version of browsers.

Note: Please note certain browsers such as Google Chrome and Mozilla Firefox automatically update to the latest version. The following table shows the version of browsers tested at the time of the official release of a version of Cisco Meeting Server. This means we have not tested this particular release with previous versions of those browsers.

We endeavor to test the latest maintenance release of each major release of Cisco Meeting Server against the latest public versions of all the browsers to keep them compatible and if we detect any issues we will endeavor to fix them as soon as possible.

Table 2: Cisco Meeting Server web app tested on browsers and versions

Browsers	Versions
Google Chrome (Windows, and Android)	141.0.7390.107
Google Chrome (macOS)	141.0.7390.78
Mozilla Firefox (Windows)	144.0
Chromium-based Microsoft Edge (Windows)	141.0.3537.7
Apple Safari for macOS	26.0.1
Apple Safari for iOS	18.4

Note: Web app is not supported on the legacy Microsoft Edge.

Note: Web app is not supported on virtual machines (VMs) running these supported browsers.

Important note for users using iOS 13 or later and macOS 10.15 or later

In order for users to be able to use web app on Safari on iOS 13 or later and macOS 10.15 or later, webbridge3 needs to be properly configured to comply with requirements stated here : https://support.apple.com/en-us/HT210176.

Users will not be able to open the app on Safari if these requirements are not met.

Important note about screen sharing on Chrome on macOS 10.15 or later

From macOS version 10.15 (Catalina) or later, to share the screen or application from the app running on Chrome, users need to enable permissions. Follow these steps:

1. From the Apple menu, open **System Preferences**.
2. Click on **Security & Privacy**.
3. Click on the **Privacy** tab at the top.
4. In the column on the left hand side, scroll down and click on **Screen Recording**.
5. Make sure Chrome is selected. Restart Chrome.

3.7.1 Important note about accessibility settings in Safari browsers

By default, Safari browsers do not allow navigation of UI elements via the 'Tab' key but via Option + Tab instead. This can be configured in Safari's Preferences as follows:

From your Safari browser menu, go to **Safari** > **Preferences** > **Advanced** > **Accessibility** > **Press Tab to highlight each item on a web page** to change your preference.

3.7.2 Important note about audio and video issues observed in Safari browsers

CSCwp32445 - In Safari version 18.5 on MacBook systems, users experience intermittent audio issues during screen sharing sessions. When other participants share screens with content audio using a different browser, Safari users initially hear the audio but then lose both the shared content audio and participant audio.

Workaround: The issue is resolved if the user rejoins the meeting. In some cases, it also resolves on its own after a few minutes.

3.7.3 Important note about group policy settings in Microsoft Edge

If `WebRtcLocalhostIpHandling` - **Restrict exposure of local IP address by WebRTC** group policy is applied to Microsoft Edge browser, make sure to only use one of the following policy options:

- `AllowAllInterfaces` (default) or
- `AllowPublicAndPrivateInterfaces` (default_public_and_private_interfaces)

Any other option could cause connection issues.

3.8 Product documentation

The end-user guides such as User Guide, and visual 'How to' guides for web app are available in the following location:

https://www.cisco.com/c/en/us/support/conferencing/cisco-meeting-app/products-user-guide-list.html

4 Upgrading, downgrading and deploying Cisco Meeting Server software version 3.12.2

This section assumes that you are upgrading from Cisco Meeting Server software version 3.11. If you are upgrading from an earlier version, then you must first upgrade to 3.11 following the instructions in the 3.11 release notes, before following any instructions in this Cisco Meeting Server 3.12 Release Notes. This is particularly important if you have a Cisco Expressway connected to Meeting Server.

Note: Cisco has not tested upgrading from a software release earlier than 3.11.

To check which version of Cisco Meeting Server software is installed on a Cisco Meeting Server 2000, Cisco Meeting Server 1000/Small, 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.

4.1 Upgrading to Release 3.12.2

The instructions in this section apply to Meeting Serverdeployments 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 complete 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.

Note: If you have deployed a clustered database, remove all nodes from the cluster using the **`database cluster remove`** command before upgrading your Meeting Servers. After the upgrade, re-add the nodes to the cluster using the appropriate MMP commands. See Cluster upgrade FAQ for detailed instructions.

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: If upgrading from version 3.11 with secure storage enabled, it is recommended to take a backup of the configuration, to avoid any risk of losing the configuration.

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_12_2_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:1f9178294766cfa6c5f30d8c08ee213027d79d2a7249eac21f16fd896e126a58

   `Cisco_Meeting_Server_3_12_2_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:b240992ddd153a2e7ab41092714d0479ad22473a2b5f9f85057ad0d709bb8fd6

   `Cisco_Meeting_Server_3_12_2_vSphere-8_0.ova`

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

   For vSphere8.0 and higher, hash (SHA-512) for Cisco_Meeting_Server_3_12_vSphere-8_0.ova:
   e89aaf982237d5ebf24df65e09275e593f7d4cd900355645a2e609e86d01a6b664257224f03ee8dff0f2938
   e6d6e53e43aa2ec95e2e8507d76a172ce64857b41

2. To validate the OVA file, the checksum for the 3.12.2 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.

   Note: Version 3.12 of Meeting Server and Meeting Management supports ESXi 8.0 Update 3e.

   ---

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 <image_name>.img. For example: upgrade upgrade_spa.img
    ```

    b. The Server/ virtualized server restarts automatically: allow 10 minutes for the process to complete.
7. Verify that 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. You have completed the upgrade.

4.2 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" Meeting Server to the required version using the MMP **`upgrade`** command.

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 complete 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.

Note: If you are downgrading from version 3.12.2 with secure storage enabled, the process will be aborted. To proceed, perform a **`<factory_reset full>`** to clear secure storage settings, then downgrade to the desired version.

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 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 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. Finally, check that:
   - the Web Admin interface on each Call Bridge can display the list of coSpaces.
   - dial plans are intact,
   - 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.

4.3 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, Web Bridge 3, and MeetingApps 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.

4.3.1 Points to note

4.3.1.1 Cisco Meeting Server 2000

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.

4.3.1.2 Cisco Meeting Server 1000 and specification-based VM server

- 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.
- When uploading OVA to Vcenter and deploying, the Publisher field should show (Trusted certificate). If you see a warning for an invalid certificate and not-trusted cert when importing the OVA, see this article: https://kb.vmware.com/s/article/84240. You may have to add the intermediate and root certificates corresponding to the certificate used to sign the OVA, to the VECS Store. To procure intermediate or root certificates or any other issues, contact Cisco Technical Support.

5 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 and web app, 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 3.12.2.
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.

5.1 Resolved issues in Cisco Meeting Server

Issues seen in previous versions that are fixed in 3.12.2.

Cisco identifier	Summary
CSCws62493	Users experienced one-way audio after a session refresh, following a transfer into a Meeting Server meeting via the Cisco Unified Communications Manager intercluster.
CSCwt00859	An isolated instance of segmentation fault occurred in the management process due to a race condition while handling a presence or session-related REST request due to unexpected or incomplete data.
CSCwt00875	Multiple Meeting Server 2000 servers experienced repeated segmentation fault crashes within a short time window. The crashes occurred during REST-based presence and session update operations together and were frequently reported inside the Curl library.
CSCws27917	The logo for the standard screen layout does not appear on SIP devices when the user connects and disconnects multiple times. This issue occurs specifically with SIP endpoints during repeated connection attempts.

Issues seen in previous versions that are fixed in 3.12.1.

Cisco identifier	Summary
CSCwo73532	Cisco has evaluated the impact of vulnerability, identified by CVE-1999-0524 involving timestamp requests and replies. Meeting Server 1000 and virtual deployments are impacted by this vulnerability, which has been addressed by implementing firewall modifications in the Meeting Server software to resolve the issue.
CSCwq92494	Meeting Server 2000 crashes with the error: " server-!ServerMediaVideoComposition::configureContributors." The Media module in Meeting Server 2000 experiences intermittent crashes when 'per participant pane placement' is applied during an ongoing conference that has more than 100 participants, and the 'roll pane' feature is intermittently toggled.
CSCwr28875	Meeting Server 2000 crashes with the error: " server-!ServerMediaCall::writeVideoLayoutContributors" . The Media module in Meeting Server 2000 experiences intermittent crashes when 'per participant pane placement' is applied during an ongoing conference that has more than 100 participants, and the 'roll pane' feature is intermittently toggled.
CSCws26193	Meeting Server crashes with the error: " mf_remote_media!dav1d_decoder_flush_frame_buffer [dav1d_interface.cpp. " Intermittent issues with content quality and media framework restarts are observed during meetings under high utilization with multiple concurrent meetings and many participants. This issue affects users sharing content using the AV1 video codec on Meeting Server, regardless of their location.

Cisco identifier	Summary
CSCwr77696	The warning message displayed when the `secure_storage enable` command is executed has been modified to the following: **This command enables virtual TPM protection for the internal filesystem ensuring stronger protection of sensitive data. Warning: This operation is irreversible. Ensure you create a " backup" before proceeding. System will reboot to initialise the secure storage. Are you sure you want to proceed to reboot now? (Y/n)**

Issues seen in previous versions that are fixed in 3.12.

Cisco identifier	Summary
CSCwq11063	Meeting Server 1000 occasionally crashes in a rare scenario, displaying the following error: " server!ServerApp1Cmgr::getCallSummary(SfGuid const*, Server-CallOverallSummaryImplementation*)" .
CSCwr82907	LDAP sync fails with a " duplicate cospace URI" error when a user is deleted from one LDAP group and later re-added to a different group without an intermediate sync. This prevents synchronization for other LDAP users, as the duplicate URI blocks the sync process for the new group.
CSCwr82906	Sharing content at 4096x4097 resolution in Chrome causes unexpected codec negotiation (CN) and does not display the correct error message.
CSCwp22989	Meeting Server 1000 is crashing intermittently with the error reason " server-!ServerControlCmgrCall::updateConfiguration(ServerCallConfigurationImplementation const*)" when participants are disconnected from an ongoing meeting.
CSCwp16290	In rare scenarios, Meeting Server crashes when a participant joins a meeting.
CSCwp67146	Outbound SIP calls are not evenly distributed when Meeting Server dials out calls in quick succession.
CSCwo68125	The Meeting Server’s media module crashes when content is shared using AV1 codec at resolutions above 4K from a Firefox browser.
CSCwn13502	The numeric fonts in the participant’s display name are not displayed appropriately in a Meeting Servermeeting.
CSCwk11099	When a Meeting Server conference has over 16 participants with longer display names, SIP URI (directory URI) and directory number (DN) exceeding 64 bytes, and a SIP endpoint or Jabber clients joins with Active Control enabled, the endpoint may not see other participants in the conference. **Note:** When configuring the SIP Trunk for Jabber calls as part of Cisco Unified Communications Manager (CUCM) integration with Cisco Meeting Server, while setting '**Calling and Connected Party Info Format**' to '**Deliver URI and DN in connected party, if available**', it is highly recommended to keep the combined **SIP URI (directory URI)** and **directory number (DN)** to less than 64 bytes. This is important to ensure Jabber can accurately display the participant list, improving the calling experience.
CSCvw10678	The cospace_join.wav file (" You are entering the meeting now") is played twice when joining a CoSpace protected by a PIN or when users joined via IVR.

5.2 Open issues in Cisco Meeting Server

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
CSCwq73418	A signed-in tenant user who is not a member of a cospace cannot join a meeting even when non-member access is allowed; the user receives a " Meeting join failed. Unable to find the scheduled meeting." error message.
CSCwr81825	When a meeting includes only webapp participants, the participants in rotating pane do not rotate every 20 seconds as expected. Instead, pane rotation may take up to a minute.
CSCwn81355	When 'Video Mute on Entry' and 'Audio Mute on Entry' are enabled in a meeting, SIP participants are unable to unmute their video or audio after joining.
CSCwn27875	The **`joinToneParticipantThreshold`** and **`leaveToneParticipantThreshold`** parameters accepts values more than the set maximum value of 100.
CSCwh41791	Failed to access webbridge intermittantly, on Meeting Server 2000.
CSCwd89530	If the packet capture is not stopped gracefully using Ctrl+C and the terminal is closed abruptly, further packet captures are not possible until CMS reboot.
CSCwb77929	In a deployment with multiple Web Bridge, web app participants can see the Meeting notes only if they are connected to the same webbridge where the notes was saved and published initially.
CSCwa83782	A conference is booked on TMS as Automatic connect type and one of the participants is joining the conference through an unmanaged device. When the conference starts, the participant is called by CMS/TMS, but Meeting Serverdisconnects the call after some time.
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.
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.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.

5.2.1 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.

5.3 Resolved issues in Cisco Meeting Server web app

The table below lists issues seen in previous versions that are fixed in 3.12.1.

Cisco Identifier	Summary
CSCws38615	The title on the web app homepage is misaligned and the phone numbers in the call information section are displayed in inconsistent font size.

The table below lists issues seen in previous versions that are fixed in 3.12.

Cisco Identifier	Summary
CSCwo81653	In a web app meeting, the participant names from the Chat window's To: drop-down list overflow into the message section.

5.4 Open issues in Cisco Meeting Server web app

Cisco Identifier	Summary
CSCwp96170	On the 'Email or copy invite' screen, some language names in the 'Language' drop-down are not displayed correctly.
CSCwi05238	Web app briefly shows an error message ‘Sign in failed’ when participant is logging in.
CSCwh48464	When a web app participant applies virtual background to their video and then refreshes the browser tab, the virtual background appears black on Google Chrome and Mozilla Firefox browsers.
CSCwc76769	In Google Chrome browser, when a participant applies blur to their video and leaves the web app meeting, the camera is still on and does not close.
CSCwa17363	In web app, the participants who are moved to lobby from Meeting Management can see the list of participants in the meeting even if they are waiting in the lobby.
CSCvz01888	If the role of a member was changed in the space before the meeting, a role change notification appears when the member joins the meeting.

Cisco Identifier	Summary
CSCvu98805	Whilst in a meeting from web app on Firefox browser, if you open the presentation received in a second window, occasionally the content becomes non-responsive if the presenter stops and restarts the sharing or if another participant in the meeting starts sharing content at the same time. This is an issue with Firefox browser, for details see https://bugzilla.mozilla.org/show_bug.cgi?id=1652042. Work around: Maximize the second window or alternatively, close the presentation window and reopen it.
CSCvt71069	If the video layout 'speaker large' is selected, window does not re size correctly.

Appendix A: 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.

Cisco Meeting Server 1000/ Small and other virtualized platforms

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

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

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.

Cisco Meeting Server Medium

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.

Call capacities

The following table provides a comparison of the call capacities across the platforms hosting Cisco Meeting Server software.

ides a comparison of the call capacities across the platforms hosting Cisco Meeting Server software.

Table 3: Call capacities across Meeting Server platforms

Type of calls	Cisco Meeting Server Small M7 (VM)	Cisco Meeting Server M8 Medium
Full HD calls 1080p60 video 720p30 content	60	150

Type of calls	Cisco Meeting Server Small M7 (VM)	Cisco Meeting Server M8 Medium
Full HD calls 1080p30 video 720p30 content	120	225
HD calls 720p30 video 720p5 content	240	450
SD calls 480p30 video 720p5 content	480	850
Audio calls (G.711)	3000	3000

Meeting Server M8 platform supports a maximum load limit of 450,000.

Meeting Server Small M7 variant support a maximum of 94 vCPU and 128 GBRAM.

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

Table 4: Meeting Server call capacity for clusters and Call Bridge groups

Cisco Meeting Server platform		Cisco Meeting Server 1000 M6 (per node)	Cisco Meeting Server 1000 M7 (per node)	Cisco Meeting Server 2000 M6 (per node)
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	80 160 320 3000	120 240 480 3000	648 1296 1875 3200
	HD participants per conference per server			
	web app call capacities (internal calling & external calling on CMS web edge):			
	Full HD HD SD Audio calls	80 160 320 500		648 1296 1875 1875
Meeting Servers in a Call Bridge Group	Call type supported			
	Load limit	160,000		1,296,000

Points to Note:

- Maximum of 24 Call Bridge nodes per cluster; cluster designs of 8 or more callbridge nodes need to be approved by Cisco, contact Cisco Support for more information.
- 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.
- Up to 21,000 HD concurrent calls per cluster (24 nodes x 875 HD calls) applies to SIP or web app calls.
- A maximum of 2600 participants per conference per cluster depending on the Meeting Servers platforms within the cluster.
- Table 4 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.

- 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.

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 4.)

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 Deployment Guides.

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 the table below.

Note: If you are deploying Web Bridge 3 and web app you must use Expressway version X14.3 or later, earlier Expressway versions are not supported by Web Bridge 3.

Table 5: 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 (X14.3 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.

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 4 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 5.

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.

Note: You cannot move a call to an external endpoint or move the audio to a regular phone during a call.

Appendix B: Apps feature comparison

Table 6:Feature comparison for Cisco Meeting Server web app

Feature	Web app 3.12	Web app 3.11	Web app 3.10	Web app 3.9
General				
Cisco Meeting Serverversion	3.12	3.11	3.10	3.9
Managing access for members	Yes	Yes	Yes	Yes
User-level permissions (e.g. can create space)	Yes	Yes	Yes	Yes
Support for localization	Yes	Yes	Yes	Yes
Branding	Yes	Yes	Yes	Yes
Online help	Yes	Yes	Yes	Yes
Encryption	Yes	Yes	Yes	Yes
Single sign on	Yes	Yes	Yes	Yes
Support for custom pages in online help	Yes	Yes	No	No
Refreshed user interface (color, font, and icons)	Yes	No	No	No
Join using video address (URI)	Yes	Yes	Yes	Yes
Notifications				
Audio notification when participant joins/leaves	Yes	Yes	Yes	No
Connection resiliency (Auto reconnect in bad network)	Yes	Yes	Yes	Yes
Web app session timeout	Yes	No	No	No
Schedule a meeting				
View list of scheduled meeting	Yes	Yes	Yes	Yes
Schedule a meeting	Yes	Yes	Yes	Yes
Modify a scheduled meeting	Yes	Yes	Yes	Yes

Feature	Web app 3.12	Web app 3.11	Web app 3.10	Web app 3.9
Delete a scheduled meeting	Yes	Yes	Yes	Yes
Space Management				
Space member roles	Yes	Yes	Yes	Yes
Meeting invite links for members-only space	Yes	No	No	No
Restrict access of non-members to space	Yes	Yes	Yes	No
Create / edit space	Yes	Yes	Yes	Yes
Activate newly provisioned spaces	Yes	Yes	Yes	Yes
Add / edit / delete space members	Yes	Yes	Yes	Yes
Directory look up for Add Members feature	Yes	Yes	Yes	Yes
View information for space	Yes	Yes	Yes	Yes
Send invitation	Yes	Yes	Yes	Yes
Audio and video				
Audio	OPUS	OPUS	OPUS	OPUS
Video	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8
Mic/camera configuration controls	Yes	Yes	Yes	Yes
Speaker configuration controls	Yes	Yes	Yes	Yes
Blur your background	Yes	Yes	Yes	Yes
Virtual background	Yes	Yes	Yes	Yes
Far end camera control	Yes	Yes	Yes	Yes
Auto prioritization of audio and video	Yes	Yes	Yes	Yes
Screen share				
Content magnification	Yes	Yes	Yes	Yes
Reset content zoom	Yes	Yes	Yes	Yes

Feature	Web app 3.12	Web app 3.11	Web app 3.10	Web app 3.9
View screen share	Yes	Yes	Yes	Yes
Desktop sharing	Yes	Yes	Yes	Yes
Application sharing	Yes	Yes	Yes	Yes
View screen share in a new window	Yes	Yes	Yes	Yes
Re-size the video pane	Yes	Yes	Yes	Yes
Share content audio	Yes	Yes	Yes	Yes
Optimize for Text (Share screen in 1080p)	Yes	Yes	Yes	Yes
Chat				
Chat (Broadcast to all participants in the meeting)	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only
Chat (Private)	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only
Export chat history	Yes	No	No	No
In-call				
On-screen messages	Yes	Yes	Yes	Yes
Full-screen view	Yes	Yes	Yes	Yes
Layout control	Yes	Yes	Yes	Yes
Name labels	Yes	Yes	Yes	Yes
Recording	Yes	Yes	Yes	Yes
Streaming	Yes	Yes	Yes	Yes
Active speaker label (Beta support)	Yes	Yes	Yes	Yes
Self-view	Yes	Yes	Yes	Yes
Pin self-view	Yes	Yes	Yes	Yes
Mirror self-view	Yes	Yes	Yes	Yes
Move self-view	Yes	Yes	Yes	Yes
HD/SD selection	Yes	Yes	Yes	Yes
Pin presentation preview	Yes	Yes	Yes	Yes

Feature	Web app 3.12	Web app 3.11	Web app 3.10	Web app 3.9
Move presentation preview	Yes	Yes	Yes	Yes
Meeting notes	Yes	Yes	Yes	Yes
Closed captioning	Yes	Yes	Yes	Yes
Share files	Yes	Yes	Yes	Yes
Network health indicator and media statistics	Yes	Yes	Yes	Yes
Content share metrics	Yes	Yes	Yes	Yes
Logo support	Yes	Yes	Yes	Yes
Surveys	Yes	Yes	Yes	Yes
Participants				
Rename participants	Yes	No	No	No
Increased character limit for participant names	Yes	Yes	No	No
User identification in Participants list	Yes	Yes	No	No
Configurable user indicators in Participants list	Yes	No	No	No
Move participant	Yes	Yes	Yes	Yes
Add participant	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)
Remove participants	Yes	Yes	Yes	Yes
Admit participants to a locked meeting	Yes	Yes	Yes	Yes
Change a participant's role	Yes	Yes	Yes	Yes
Make participant important	Yes	Yes	Yes	Yes
Mute/Unmute other participants' audio and video individually	Yes	Yes	Yes	Yes
Mute/Unmute all participants' audio and video	Yes	Yes	Yes	Yes
Send diagnostics during a meeting	Yes	Yes	Yes	Yes

Feature	Web app 3.12	Web app 3.11	Web app 3.10	Web app 3.9
Send invite	Yes	Yes	Yes	Yes
View call info	Yes	Yes	Yes	Yes
Mic / Camera controls during call	Yes	Yes	Yes	Yes
Raise hand	Yes	Yes	Yes	Yes
Move call				
Use this device for screen share and call management only (while another device is used for audio and video)	Yes	Yes	Yes	Yes

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

Accessibility Support Features

Keyboard navigation

You can use your keyboard to navigate through web app.

- Use **Tab** to navigate between areas in web app. You'll know an area is in focus when it's surrounded by an outline.
  Use **Shift + Tab** to move to the previously focused area.
- Use the **Spacebar** or **Enter** key to select items.
- Use arrow keys to scroll through lists or drop-down menus.
- Use **Esc** to close or dismiss opened screens/menus.

Screen reader support

You can use the JAWS screen reader version 18 or later.

The screen reader announces focused areas/buttons, relevant information like notifications, warnings, status messages appearing on the screen, and the actions you can perform.

For example: When you focus on **Add participant** area in a web app meeting, the screen reader will announce " Add participant" and to enter a participant's SIP address.

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