Cisco Meeting Server and web app

Release 4.0

Release Notes

11 November, 2026

Contents

What's changed 5

1 Introduction 6
- 1.1 Cisco Meeting Server 6
- 1.2 Cisco Meeting Server web app 6
  - 1.2.1 Using the web app 7
- 1.3 End of Software Maintenance 8
- 1.4 Deprecation Notice 8

2 What's new in Cisco Meeting Server 9
- 2.1 Enhanced logo file name validation 9
- 2.2 Updates to TLS and DTLS protocol requirements 10
- 2.3 Security improvements - Secure storage (encrypted storage) 10
  - 2.3.1 Steps to follow before upgrading to Version 4.0 10
  - 2.3.2 Steps to follow after upgrading to version 4.0 11
- 2.4 Implementing No-Index/No-Follow for Meeting Server Web App Pages 12
- 2.5 Configuring background noise removal for web app participants 13
  - 2.5.1 API addition 13
- 2.6 Configuring automatic closed captions 14
  - 2.6.1 API additions 15
  - 2.6.2 MMP additions 18
- 2.7 Enhanced virtual background capabilities 19
  - 2.7.1 Enhancements in blur/virtual background 20
  - 2.7.2 API addition 20
  - 2.7.3 Adding custom video backgrounds 20
- 2.8 Enhanced media quality and stability 21
  - 2.8.1 Resilience Indicators 21
  - 2.8.2 Media Quality Analysis 21
- 2.9 Enabling Breakout Rooms in Meeting Server 22
  - 2.9.1 API additions 22
- 2.10 Deploying Meeting Server Using NFVIS 22
- 2.11 Version 4.0 on Meeting Server Small (Bare metal OS) 23
- 2.12 External export of user configuration and media statistics logs 23
  - 2.12.1 MMP additions 25
- 2.13 Configuring faster transitions for custom pane layouts 25
  - 2.13.1 API addition 25

2.14 Related user documentation 25

3 What's new in Cisco Meeting Server web app 27
3.1 Breakout rooms 27
3.2 Enhancements in Web app user interface 29
Meeting Preview Page 30
Controls 30
3.3 Suppress ambient noise 32
3.4 Enhanced background blur performance 33
3.5 Support for virtual video backgrounds 33
3.6 Automatic closed captions 34

4 Browser versions tested 36
Important note for users using iOS 13 or later and macOS 10.15 or later 36
Important note about screen sharing on Chrome on macOS 10.15 or later 37
Important note about accessibility settings in Safari browsers 37
Important note about group policy settings in Microsoft Edge 37

5 Product documentation 38

6 Upgrading and deploying Cisco Meeting Server software version 4.0 39
6.1 Upgrading to Release 4.0 39
6.2 Cisco Meeting Server Deployments 42
6.2.1 Points to note 43

7 Bug search tool, resolved and open issues 44
7.1 Resolved issues in Meeting Server 4.0 44
7.2 Open issues Meeting Server 4.0 46
7.3 Resolved issues in Meeting Server 4.0 web app 47
7.4 Open issues in Meeting Server 4.0 web app 48

Appendix A: Sample syslog formats 49

Appendix B: Cisco Meeting Server platform maintenance 54
Call capacities 54
Cisco Meeting Server web app call capacities 57
Cisco Meeting Server web app call capacities – external calling 57
Cisco Meeting Server web app capacities – mixed (internal + external) calling 58

Appendix B: Apps feature comparison 59

Accessibility Notice 64

Accessibility Support Features 65

Cisco Legal Information 66

Cisco Trademark 67

What's changed

Version	Change
Nov 11, 2026	New version for release 4.0.

.

1 Introduction

This document describes the changes in version 4.0 of the Cisco Meeting Server software and Cisco Meeting Server web app.

1.1 Cisco Meeting Server

The Cisco Meeting Server software 4.0 can be hosted on:

Meeting Server Platform	Variant	Meeting Server deployment
Newer Generations		
Cisco Meeting Server Small	M7	Bare metal OS
Cisco Meeting Server Small	M7	VM deployment (ESXi 8.X)
Cisco Meeting Server Medium	M8	Bare metal OS
Previous Generations		
Cisco Meeting Server 1000	M6, M5v2	VM deployment (ESXi 8.X)
Cisco Meeting Server 2000	M6, M5v2	CMS 2K OS
Spec based hardware		VM deployment (ESXi 8.0)

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 4.0 is required with Meeting Server 4.0.

- **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 MMP Command Reference document for full details, and ***Cisco Meeting Server*** **White Paper on Upgrading to Release 4.0** for mandatory upgrade procedures.

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 End of Software Maintenance

On release of Cisco Meeting Server software version 4.0, 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 3.12	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.12.x is May 2027.

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

1.4 Deprecation Notice

Discontinuation of the Uploader Component for Cisco Meeting Server: Cisco has ended its partnership with VBrick. As a result, the Uploader component will be discontinued in future versions of Cisco Meeting Server.

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 features and changes in 4.0:

Security Enhancements

- Enhanced logo file name validation for security
- TLS/DTLS 1.2 minimum requirements
- Secure storage (encrypted storage)
- Implementing No-Index/No-Follow for Meeting Server web app pages

AI Features

- Configuring background noise removal for web app participants
- Enabling automatic closed captions
- Enhanced virtual background capabilities

Media and User Experience

- Enhanced media quality and stability
- Enabling breakout rooms in Meeting Server

Deployment

- Deploying Meeting Server using NFVIS
- Version 4.0 on Meeting Server Small (Bare metal OS)

Observability

- External export of user configuration and media statistics logs

API Optimisation

- Configuring faster transitions for custom pane layouts

2.1 Enhanced logo file name validation

Starting with version 4.0, logo file name specifications have been updated. The Logo File names must consist exclusively of alphanumeric characters; spaces, punctuation, special characters, and path separators are not supported.

Note: Images from previous releases containing restricted characters will not render after upgrading to version 4.0. It is recommended to delete these files and re-upload them using the supported naming convention.

2.2 Updates to TLS and DTLS protocol requirements

Starting with version 4.0, support for TLS 1.0, TLS 1.1, and DTLS 1.0 has been deprecated. The minimum supported version for TLS and DTLS is now 1.2. Meeting Server provides end-to-end support for TLS 1.3, TLS 1.2, and DTLS 1.2 encryption for all the services. Additionally, TLS 1.3 has been validated with FIPS.

2.3 Security improvements - Secure storage (encrypted storage)

Version 4.0 adds further enhancements to the Meeting Server's security specifications by enabling Secure Storage by default. This setting is now permanent and is irreversible.

As part of this update:

- the **`secure_storage enable`** MMP command has been removed.
- Additionally, dual passphrase confirmation has been introduced during private key and backup file encryption setup to help prevent passphrase entry errors. When creating a passphrase for the first time, users will be prompted to enter the passphrase twice for verification and confirmation.

Note: Existing private key and backup file operations continue to function as before. Secure Storage is available on Bare metal OS (Meeting Server Medium and Meeting Server Small), Meeting Server VM (Spec based, Meeting Server 1000/Meeting Server Small)

CAUTION:

- Any upgrade from earlier versions whether secure storage is enabled or not, to the current version will result in loss of existing configuration and network settings. Therefore, it is critical for users to take a backup of their configuration to an external device before proceeding with the upgrade. This backup must be stored in external location and not on the Meeting Server itself to ensure it remains accessible and safe.
- Once upgraded to release 4.0, downgrade to any of the 3.x versions is not supported.

2.3.1 Steps to follow before upgrading to Version 4.0

This section summarizes the steps to follow before upgrading. For comprehensive instructions, refer to " *White Paper for Upgrade Scenarios and Steps to Upgrade to 4.0*" .

These requirements apply exclusively to Meeting Server 1000, Small/VM, and Bare Metal deployments(Small and Medium). Meeting Server 2000 remains unaffected.

Before starting the upgrade, complete the following actions:

- Meeting Server follows a sequential upgrade path. To upgrade from version 3.11 to 4.0, install each intermediate version in order: 3.11 → 3.12 → 3.13 → 4.0. For Meeting Server Medium with versions 3.11.5 or 3.13, the upgrade path would be 3.11.5 → 3.13 → 4.0.
- Create and export a configuration backup to an external system when upgrading from version 3.13 to 4.0. Additionally, maintain multiple copies of your configuration backups as a safety measure for reliable recovery options available when needed.
- Transfer all custom data (e.g., logos, branding files, audio prompts, SSO files, etc.) stored on the internal SFTP server to an external location.
- Run 'ipv4 a' to capture current network settings; manual reconfiguration via console access (Hypervisor, CIMC, or Serial) will be required post-upgrade.
- Confirm console access is available if network connectivity is lost.
- Download the current log bundle (logbundle.tar.gz) for archival purposes.

2.3.2 Steps to follow after upgrading to version 4.0

- Manually restore the IP network settings using console access.
- Restore the saved configuration backup and any required custom data from the external backup location.
- Generate a new secret key for MeetingApps and update the Webbridge configuration with this new key to restore the MeetingApps functionality.

The following table details the supported upgrade and downgrade scenarios:

Upgrade/downgrade scenarios	Status	Notes
Upgrade from 3.13 to 4.0 with Y as user input (Secure Storage enabled or not enabled in 3.13)	Supported	To prevent data loss, export your configuration, system backups, and any custom SFTP data to an external system before starting the upgrade. • Secure Storage OFF: Pre-upgrade backups transfer normally. After upgrading to 4.0, backups require a passphrase and must be manually encrypted before transfer. • Secure Storage ON: A passphrase is required when creating the backup and again during post-upgrade rollback. • Secure Storage transition from OFF to ON: Existing unencrypted backups cannot be transferred and must be manually encrypted first. Refer to "***White Paper for Upgrade Scenarios and Steps to Upgrade to 4.0***" for mandatory upgrade procedures.
Upgrade 3.13 to 4.0 – with N as user input	Upgrade aborted	Upgrade aborted as user has denied upgrade.
Downgrade from 4.0 to 3.x versions	Not supported	Downgrade not supported.

2.4 Implementing No-Index/No-Follow for Meeting Server Web App Pages

Version 4.0 prevents search engines (like Google, Bing) from indexing or following Meeting Server Web App pages. Although authentication restricts access to page content, search engines can still discover and index publicly reachable URLs. Implementing noindex and nofollow directives mitigates security risks by protecting sensitive meeting information and reducing the likelihood of unauthorized discovery.

This implementation works seamlessly across all supported browsers—including Chrome, Firefox, Safari and Edge.

Note:

- Search engines may retain cached versions of pages that were indexed prior to this implementation.
- This feature does not prevent the manual sharing or bookmarking of URLs by users.

2.5 Configuring background noise removal for web app participants

Meeting Server 4.0 introduces the Noise Removal feature for the web app, which filters ambient background noise before audio is transmitted to other participants, significantly improving meeting clarity. Participants can enable this feature either before joining the meeting from the lobby page or during an active meeting.

Administrators can control the availability of this feature using the new **`noiseRemovalAllowed`** API parameter. This setting determines whether web app participants can enable or disable background noise removal during the meeting. The parameters must be enabled in lobby profiles and call profiles to enable the feature on the join meeting page and in-meeting page respectively.

2.5.1 API addition

To add noise removal option in the join meeting page, configure:

- POST to the "**/lobbyProfiles**" node
- PUT to "**/lobbyProfiles/<lobby Profile id>**"
- GET on the "**/lobbyProfiles**" node

To add noise removal option in the in-meeting page, configure:

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

Parameter	Type/value	Description
`noiseRemovalAllowed`	**true** | false	If specified, determines whether noise removal is allowed for webapp participant in the lobby or call. If unset at all levels of the hierarchy, defaults to true. For non-signedin users, the parameter follows the hierarchy: **accessMethod > coSpaces > tenant > system/profiles**. For users who are trying to join a space that they are a member of, using the **Join** button, the parameter follows the hierarchy: **coSpaceUsers > accessMethod > coSpaces > tenant > system/profiles**.

2.6 Configuring automatic closed captions

From version 4.0, Meeting Server integrates Collab AI Pods, establishing a foundation for future AI-driven productivity tools. Starting with this release, participants can initiate real-time call transcription through the AI Assistant and manage their individual captioning preferences. Participants with the appropriate administrative permissions can also select the spoken language for real-time captions.

The AI Assistant feature includes the following modes:

- **Automatic**: Transcription begins automatically upon call initiation, requiring no user Intervention.
- **Manual**: Users can start or stop transcription at any time during an active call.
- **Disabled**: Closed Captions is disabled, and the existing manual captions behavior applies if it is enabled.

New audio prompts are added to announce when the meeting transcription starts/ stops.

Note:

- Meeting Server does not currently support translation; therefore, the Spoken Language and the Caption Language are same.
- The Meeting Server must be connected to at least one configured Collab AI POD node with valid API key(s) and should have a trusted CA bundle set for the transcription service. Trust between Collab AI POD and Meeting Server should be established using valid

---

certificates.

- This feature is supported only on the web app.
- To ensure system stability, avoid switching between AI Assistant modes during an active session.
- The AI Pod must maintain a Healthy status to ensure optimal service performance and system stability.
- If the AI Assistant mode is disabled or not configured, the system defaults to the existing Manual Captioning feature, provided the **captionContributionAllowed** API is enabled.

2.6.1 API additions

API endpoint addition

The new **`collaborationAiPods`** API endpoint has been added to support secure integration with on-premises AI servers. The parameters, **`server`**, **`apiKey`**, and **`serverSelectionPolicy`** allows configuring server addresses, authentication credentials, and load-balancing policies to ensure reliable connectivity. It is supported on the following methods:

/api/v1/collaborationAiPods

API methods:

- GET on **/collaborationAiPods**
- POST to **/collaborationAiPods**
- PUT on **/collaborationAiPods**
- DELETE **/collaborationAiPods**

Parameter	Type/value	Description
`server`	String	AI Server FQDN. For example, " server.example.com"
`apiKey`	String	API key for authentication with the server.

PUT on **/api/v1/collaborationAiPods/serverSelectionPolicy**

Parameter	Type/value	Description
serverSelectionPolicy	LoadBalanced | TopDown	Determines how requests are distributed across servers. • LoadBalanced spreads evenly; • TopDown uses a priority/fallback order. Updates the server selection policy used when choosing between configured Collaboration Ai pods.

API parameter additions:

The following API parameters have been added to enable the AI Assistant to provide real-time captions of spoken content.

- **aiAssistantControlAllowed**, **aiAssistantMode**, **captionLanguage**, and **aiAssistant**: Managed through callLegProfile, callProfiles, and calls. In addition to the above parameters, the existing **captionsAllowed** parameter enables the CC button and caption pane inside the meeting menu for the participants.

The **aiAssistantControlAllowed** parameter is introduced on /api/v1/callLegProfiles

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

Parameter	Type/value	Description
aiAssistanControlAllowed	true | false	Indicates if AI assistant button is shown in the web app screen and the user has permission to change the caption language and the ability to start or stop the AI Assistant. true – Indicates the participant can manage AI Assistant. false – Indicates the participant does not have the permission to manage AI Assistant. The default value is true.

The **aiAssistantMode** parameter is introduced on /api/v1/callProfiles

- GET on /callProfiles
- POST to /callProfiles/< callProfiles ID>

- PUT on /callProfiles /< callProfiles ID>

Parameter	Type/value	Description
aiAssistantMode	Automatic | Manual | Disabled	Controls AI Assistant behavior. **Automatic**: Transcription starts automatically when a call begins. No user action is needed. **Manual**: Transcription can be started/stopped in between the call. **Disabled**: AI Assistant is not available. If unset, it defaults to Disabled.

The **aiAssistantLanguages** object is added on /api/v1/callProfiles/<call_id>/aiAssistantLanguages

- PUT on /callProfiles /<call_id>/aiAssistantLanguages

Parameter	Type/value	Description
English|	true|false	Specify the languages supported by the AI Assistant.
French	true|false	Specify the languages supported by the AI Assistant.
German	true|false	Specify the languages supported by the AI Assistant.
Italian	true|false	Specify the languages supported by the AI Assistant.
Spanish	true|false	Specify the languages supported by the AI Assistant.
defaultLanguage	(English| French| German| Italian| Spanish|)	This will set the default language for the closed captions. If unset, it defaults to English.

The **captionLanguage** and **aiAssistant** parameters are introduced on /api/v1/calls

- GET on /calls
- POST to /calls/<call Id>
- PUT to calls/<call Id>

Parameter	Type/value	Description
captionLanguage	English | French | German | Italian | Spanish	Select language from the list to generate real-time transcriptions of active calls. Default language is English. When **aiAssistantMode**=**Automatic**, transcription starts automatically. Use this parameter only to change the language. When **aiAssistantMode**=**Manual**, a participant must first enable AI Assistant from the web app UI, then this endpoint can be used to change the language.
aiAssistant	**true** | false	**true** -When the **aiAssitantMode** is set to Manual, AI Assistant will be enabled by setting this to true. **false**- When the **aiAssitantMode** is set to Manual, AI Assistant will be disabled by setting this to false.

Note:

- When **aiAssistantMode**=**Automatic**, transcription starts automatically. Use this parameter only to change the language.
- When **aiAssistantMode**=**Manual**, a participant must first enable AI Assistant from the web app UI, then this endpoint can be used to change the language.

2.6.2 MMP additions

New MMP commands are introduced to facilitate the connection between Callbridge and Colloab AI Pods and creating virtual participants to enable automatic closed captioning on Callbridge.

sip_cmgr starts a virtual participant that supports transcription. It serves a role similar to the recorder or streamer service and starts automatically on all Callbridges. The component is enabled by default on port 5072 and cannot be disabled. However, only the listening port can be changed. After changing it, run **sip_cmgr restart** to restart the service and apply the new port. The service will then listen on the configured port.

Note:

- The proper functioning of automatic captions depends on both the transcription container and the sip_cmgr services being active and running.
- The commands must be enabled on callbridge for the feature to work. Restart the callbridge for the changes to be applied.
- If you have already configured Transcription Trust, you must reconfigure it after upgrading to version 4.0 Meeting Server, as configuration changes require these settings to be

reapplied using the command **`callbridge transcription trust <bundle>`**.

Command	Description
`callbridge transcription trust <bundle>`	Configures the transcription container to use a particular bundle of certificates to validate the identity of the AI Pods. The bundle can be either a certificate chain, or an allowed list of trusted certificates.
`callbridge transcription trust none`	Removes the certificate bundle for the transcription container from trust store.
`callbridge transcription restart`	Restarts the transcription container.
`callbridge transcription status`	Displays the current status of the transcription container.
`callbridge transcription logs`	Displays logs of the transcription container. For Meeting Server 2000, transcription logs can be monitored using the syslog follow command.
`callbridge sip_cmgr restart`	Restarts the sip_cmgr service.
`callbridge sip_cmgr port <port>`	Configures a port on which sip_cmgr listens. Default port is 5072.
`callbridge sip_cmgr status`	Displays current status of the sip_cmgr service.

For more details on Automatic Closed Captions, refer to Cisco Meeting Server Admin QRGs-AI assisted features-Automatic Closed Caption 4.0.

2.7 Enhanced virtual background capabilities

Version 4.0 adds significant improvements to the virtual background capabilities for participants using the web app.

- **Enhancements in blur/virtual background** - Background blur and virtual backgrounds, previously available only during a call, can now be applied directly from the lobby before joining the meeting. Additionally, the Administrators can control the availability of this feature by configuring the API accordingly.
- **Applying custom video background** - Meeting Server Administrators can now provide custom video backgrounds for participants using the web app.

In addition to these new capabilities, the Meeting Server has been optimized to reduce the latency in applying custom background images, ensuring a faster and more responsive experience when participants switch between backgrounds.

2.7.1 Enhancements in blur/virtual background

Web app participants can now apply and preview virtual backgrounds before joining a meeting. This feature is now available directly from the Join meeting screen, allowing users to configure their background settings before entering the call.

Administrators can control the availability of this feature in the lobby, by configuring the API parameter **`backgroundBlurAllowed`** under lobby profiles.

2.7.2 API addition

The parameter is supported on the following methods:

POST to the **" lobbyProfiles"** node

PUT to **" /lobbyProfiles/<lobby Profile id>"**

GET on the **" /lobbyProfiles"** node

Parameter	Type/value	Description
`backgroundBlurAllowed`	true | **false**	If specified, determines whether background blur is allowed for webapp participant using this lobby profile. If unset at all levels of the hierarchy, defaults to false. For non-signedin users, the parameter follows the hierarchy: **accessMethod > coSpaces > tenant > system/profiles**. For users who are trying to join a space that they are a member of, using the **Join** button, the parameter follows the hierarchy: **coSpaceUsers > accessMethod > coSpaces > tenant > system/profiles**.

2.7.3 Adding custom video backgrounds

Meeting Server Administrators can now provide custom video backgrounds for participants using the web app. These backgrounds are managed alongside existing image-based background.

The video files must be included in the same zip archive used for other branding files and the utils.json file must be updated with the number of images and videos accordingly.

Video background configuration requirements:

- Each video background can have a maximum file size of 4 MB. The combined size of all background images and branding assets must not exceed 30 MB prior to being compressed into a ZIP file.
- All video files must follow the naming convention: vb_videos_<number>. mp4 (e.g., vb_videos_1.mp4, vb_videos_2.mp4). Files must be numbered sequentially starting from 1.
- Update the vb_count parameter in utils.json file to reflect the total number of available background assets.

  For example:

  If the number of images is 6 and number of video files is 2, the total count will be 8. The count in the utils.json file must be updated as follows:

  The count of the total files to be displayed in web app must be specified in the following format:

  {

  " vb_count" :8

  }

Note: The background files will be picked up after the web bridge/ call bridge is restarted, that may affect any ongoing meetings. Therefore, it is recommended to not upload the images, while a meeting is in progress.

2.8 Enhanced media quality and stability

Version 4.0 introduces improvements to media quality and stability for a better meeting and conferencing experience. These changes focus on improving media resilience visibility, extended diagnostic logging, and modernizing the meeting interface.

2.8.1 Resilience Indicators

On Web Admin → Status → Calls, the media-stream detail line can display FEC, RTX, or both.

FEC indicates that forward error correction is active for the stream. FEC is available for Cisco SIP endpoints and ensures multiple packets to reserve quality.

RTX indicates that retransmission is enabled for the stream. RTX support for web app to improve quality over packet loss network.

2.8.2 Media Quality Analysis

New fields have been added to **rxVideo** and **txVideo** in media statistics logs. See Section 2.12 for configuring media-statistics export and its reporting interval. These fields are dynamic and will only appear in the configuration and media statistics logs if their value is greater than zero and can be exported to external servers.

Note that Meeting Server now prefers in-band DTMF handling over RFC2833.

2.9 Enabling Breakout Rooms in Meeting Server

Version 4.0 introduces support for breakout rooms in Cisco Meeting Server Web app meetings, enabling web app participants to engage in smaller group discussions during an active call and return to the main call at any time.

Breakout rooms facilitate smaller group discussions within a meeting. Administrators can designate a participant as the host and grant them permission to create and manage breakout rooms during the meeting. Up to 10 breakout sessions can be created in a meeting. As these permissions apply to individual participants, they are configured at the participant level instead of the call level.

2.9.1 API additions

A new API parameter, **`canEnableBreakoutRoom`**, is introduced on the following methods:

POST and PUT on **callLegProfiles/<callLegProfileId>**

POST and PUT on **callLegs/<callLegId>**

Parameter	Type/value	Description
`canEnableBreakoutRoom`	true | **false**	Indicates if the participant has the ability to create and manage breakout rooms in a call. **True** - The participant has the ability to create and manage Breakout rooms during the call. **False** - The participant does not have the ability to create and manage Breakout rooms during the call. If unset, it defaults to false.

For more details on Breakout Rooms, refer to Cisco Meeting Server 4.0 Admin QRG Breakout Rooms.

2.10 Deploying Meeting Server Using NFVIS

Starting with version 4.0, Cisco Network Function Virtualization Infrastructure Software (NFVIS) provides the virtualization platform for hosting and managing Cisco Meeting Server virtual instances. It delivers a streamlined and reliable foundation for the meeting environment.

Components	Version
NFVIS Version	26.2.1 (GA Version)
Server Model	Server Model BE6K/7K
Meeting Server Version	Meeting Server version 4.0

For the detailed instructions about installing NFVIS and starting the management portal, refer to the Cisco Network Function Virtualization Infrastructure Software Getting Started Guide, Release 26.x and Later - Install Cisco Enterprise NFVIS Using CIMC [Cisco Enterprise NFV Infrastructure Software] - Cisco

Note: Use the following URL to access the NFVIS environment.

Components	Version
NFVIS Mgmt	Portal URL: https://<NFVIS-mgmtip>
Credentials	Username: admin , Password: < configured-password>

See Installation guide for Meeting Server 1000/ Small and virtualized deployments for version 4.0, for details on deploying Meeting Server using NFVIS.

2.11 Version 4.0 on Meeting Server Small (Bare metal OS)

Meeting Server 4.0 can be hosted on the Meeting Server Small platform, which is built on the Cisco UCS C220 rack server running a Bare Metal OS.

2.12 External export of user configuration and media statistics logs

Meeting Server Administrators can now export comprehensive call events containing participant details and media statistics data for a particular call, to external entities via syslogs. This enhancement improves visibility into calls and participants, enables monitoring of media quality, and provides administrators with greater control over data export processes.

Detailed logging includes call initiation events, participant leg configurations, and periodic media statistics (e.g., jitter, packet loss, bit rate, codec) at configurable intervals.

Key features include:

- Exporting logs in Cisco Meeting Server is a configurable feature. Administrators can enable or disable the export functionality according to their requirements.
- Administrators can configure the export mechanism for Meeting Server logs primarily using syslog to transmit logs to external systems in JSON format.

- User configuration is logged once per call, while media statistics are sent periodically at configurable intervals of 30, 60, and 120. The default interval is 30 seconds.
- Each participant can be traced using callLegId, CallId and GroupId in user config stats and user config media stats to enable detailed tracking and analysis of call events in external dashboards.
- Additionally new fields are have been added to rxVideo and txVideo in the media statistics logs. These fields are dynamic and will only appear in the configuration and media statistics logs if their value is greater than zero. See section Enhanced media quality and stability for

  rxVideo

Parameter	Description
mediaPackets	Total media packets since call start.
fecPackets	Total Forward Error Correction (FEC) packets.
rtxPackets	Total RFC 4588 NACK/RTX packets.
recoveredPackets	Total packets lost but recovered via FEC or RTX.
droppedPackets	Total packets dropped (e.g., late arrival).

  txVideo

Parameter	Description
mediaPackets	Total media packets since call start.
fecPackets	Total Forward Error Correction (FEC) packets.
rtxPackets	Total RFC 4588 NACK/RTX packets.
repeatNackPackets	Total repeated NACK requests received.
failNackPackets	Total failed NACK attempts.
rolloverCounter	Current 32-bit RTP sequence number rollover counter.

- New field, **globalCallId**, is added to uniquely track participant statistics across call bridges in clustered deployments. This identifier remains consistent for each meeting within the same coSpace, enabling correlation of distributed call legs across the cluster.

Note: The remote server must be configured using the **syslog server add <ip> <port>** command.

2.12.1 MMP additions

Command	Value	Description
`syslog extended_logging`	Enable/disable	Enables/disables extended syslog. **Note:** Restart call bridge for the changes to take effect.
`syslog extended_logging_ mediaStats_interval <interval in sec>`	Integer	The frequency in which the Meeting Server generates logs for media statistics. The possible values are 30, 60 and 120, with 30 being the default value. **Note:** Restart call bridge for the changes to take effect.

See Appendix A: Sample syslog formats for sample User Configstats and Media Configstats on web app and SIP calls.

2.13 Configuring faster transitions for custom pane layouts

Meeting Server 4.0 reduces latency when applying custom pane placement layouts via Meeting Management, resulting in faster and more responsive transitions. This optimization is achieved by applying the **layoutTemplate** parameter at the call level, which updates all participants associated with the call simultaneously.

Configuration requirements

To enable this performance improvement, ensure the following API parameters are set:

`layout`: Must be set to Automatic.

`layoutTemplate`: ID of the selected template.

2.13.1 API addition

The **layoutTemplate** parameter is added on the following API method to set properties for all participants associated with the specified call.

PUT to **`calls/<call_id>/participants/*`** node.

Parameter	Type/value	Description
`layoutTemplate`	ID	Associates the layout template for all the participants in the call.

2.14 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 feature and changes:

- Breakout rooms
- Enhancements in web app user interface
- Suppress ambient noise
- Enhanced background blur performance
- Support for virtual video backgrounds
- Automatic closed captions

3.1 Breakout rooms

Version 4.0 introduces Breakout Rooms feature which allows meeting hosts to create smaller, focused sub-sessions during an active call, facilitating more effective brainstorming, workshops, and training. Once discussions conclude, participants can be seamlessly returned to the main meeting.

- To access Breakout Rooms, click **More controls** (3-dot menu beside **End meeting**) > **Enable breakout rooms**

Host

A host is a meeting participant who has been granted specific " Breakout Room" permissions via the Cisco Meeting Server. They are the primary facilitators responsible for managing the breakout room experience.

From the Breakout Rooms dashboard, host can create up to 10 rooms, assign participants, and set a session timer. The host can start and stop sessions, join individual rooms to monitor discussions, and respond to help requests from participants.

Note:

- While multiple participants may have permission to manage breakout rooms, only one host can actively run a session at a time. Other authorized users may prepare and save their own room configurations at any time. However, once a session is started by a host, other authorized users cannot start their own configurations. They will still have access to the management menu to view their draft, but they cannot override the active session.
- Only signed-in users with the required permission can see and enable Breakout rooms. Guest users cannot enable or manage breakout rooms, but they can be assigned to and participate in breakout sessions.

- Unlike signed-in participants, guest participants do not have a unique identifier that remains consistent when moving between the main meeting and breakout rooms. This may cause inconsistencies in how guest participants appear in the breakout room interface.

Participants

Participants are attendees who join breakout sessions to engage in focused, smaller group discussions.

In a web app meeting, participants receive clear notifications when sessions begin and can request help from the host at any time. The participants can view and interact with other participants assigned to the same breakout room.

3.1.0.1 Points to Note

Availability and requirements

- Only participants with required permissions can enable the feature.
- This feature is available on web app only. SIP and audio-only endpoints are not supported.
- Breakout rooms cannot be scheduled in advance; they must be created during an active meeting.

Session management

- The breakout room host cannot assign themselves to any of the breakout sessions.
- The Host is notified, whenever a new participant joins the main meeting room, after all sessions are started.
- Sessions can be ended manually by the host or automatically upon timer expiry. The timer must be set to a minimum of 5 minutes. If a specific timer is not configured and the host does not manually end the session, the system applies a default duration of 45 minutes. A 30-second warning is provided to all participants before sessions closes.
- After a participant selects `Ask for help`, the option is automatically available again after 10 seconds, regardless of the host's response.
- In the event a host disconnects, the system can automatically assign a new host or breakout sessions continue until the last participant leaves the room, or the configured session timer expires.
- Participants who join the meeting after breakout sessions have already started will be identified in the main meeting participants list.
- Audio and video settings are preserved when switching between the main meeting and a breakout room.

- If a participant uses 'Return to main meeting' from a breakout room, they can rejoin the same breakout room while the session is active. If a participant leaves or disconnects from the meeting and then joins again, they cannot rejoin their previous breakout room until the host assigns them to a breakout session again.

Configuration and stability

- A breakout room cannot start if it contains no participants. Only rooms with assigned participants will initiate when the " Start breakout sessions" action is triggered.
- The main meeting remains active even if no participants are present, provided there are participants in breakout rooms. If no participants remain in either the main meeting or any breakout rooms, all breakout sessions are terminated first, followed by the automatic end of the main call.
- Breakout room configuration is user specific. If an active host or authorized participant disconnects before starting the sessions, their created configuration will be lost. Once a breakout session has started, the configuration cannot be reset or updated.
- Before starting the breakout sessions, the host can use the " Reset" option to delete all current sessions and participant assignments.
- Following the closure of all breakout sessions and the return of participants to the main meeting, a 30-second cooldown period applies before new breakout rooms can be initiated.
- Content such as chat, notes, or file shares cannot be transferred between the main meeting and breakout rooms.
- The current release does not support multi-host management, co-hosting, auto-join, auto-assign, or broadcast messaging.

For more details on Breakout Rooms, refer to Cisco Meeting Server 4.0 Admin QRG Breakout Rooms.

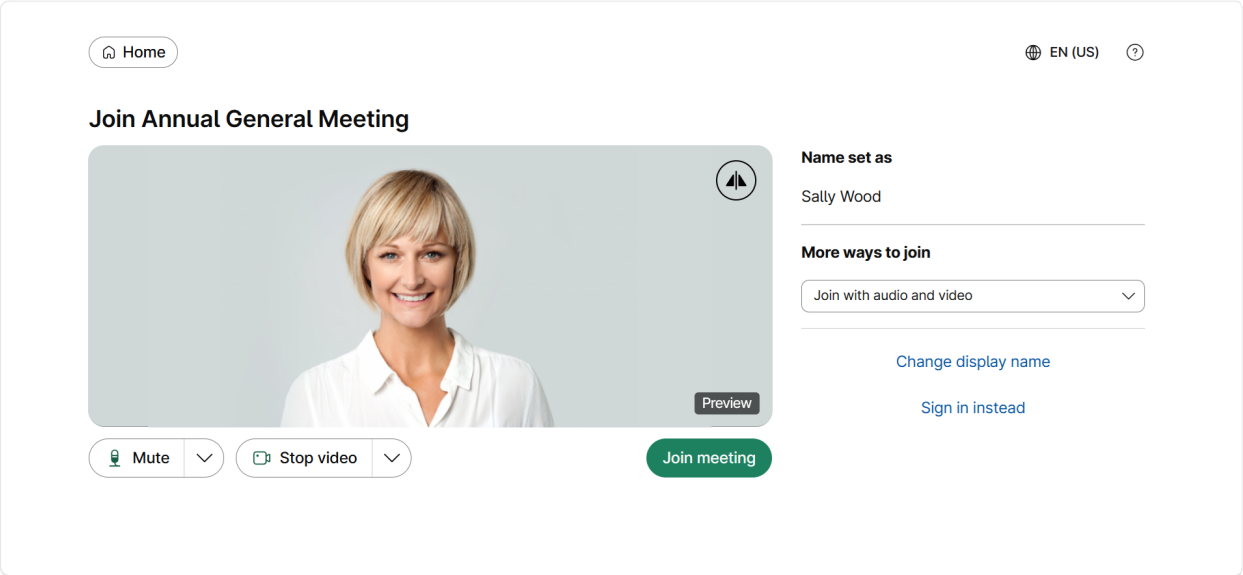
3.2 Enhancements in Web app user interface

- Improved visuals and usability on user home page
- Enhanced schedule meeting screens and scheduled meetings view
- Updated space details layout
- Accessibility improvements across the app
- Refined meeting details popover
- Refreshed login page for a modern look

- Video Layouts: Improved aesthetics featuring rounded corners on video panes.
- Active Speaker: Active speakers are now highlighted in blue for better visibility.

Meeting Preview Page

The preview page (lobby/join meeting page) now features updated visuals and enhanced usability, offering a more modern and intuitive experience.



- **Modernized Layout**: The interface has been simplified with a centered, high-visibility design, providing a cleaner look before you join.
- **Refined Control Placement**: Audio and video controls are now integrated directly into the buttons, making it faster to adjust your settings.
- **Improved Navigation**: “Change display name”, “More ways to join”, and “Sign in” options have been reorganized, ensuring a consistent and clutter-free experience as you prepare for your meeting.

Controls

Microphone button | Audio options

The  icon indicates that audio is enabled. Click it to mute the audio. When muted, the button changes to the  icon. Click it again to re-enable the audio.

Click the drop-down button beside the microphone button to access audio options:

- Audio connection
  - Don't connect to audio - Join the meeting without connecting to audio.
  - Computer audio - Use device's microphone and speakers (or connected audio devices) for meeting audio.
- Microphone: Select the microphone from the list of available microphones connected to device.
- Speaker: Select the speaker or audio output device from the list of available speakers or headphones connected to device.
- Smart Audio - microphone
  - Noise removal - Reduces background sounds and ambient noise.
  - No optimisation - Disables audio processing and captures audio as-is.

Camera button | Video options

The  icon indicates that video is on. Click it to turn off video. When video is off, the button changes to  icon. Click it again to turn video back on.

Click the drop-down button beside the camera button to access video options:

- Camera: Select the camera you want to use.
  - No Camera - Join or continue the meeting without sharing video.
  - Integrated Camera or another camera connected - Select the camera you want to use.
- Virtual Background: Blur or replace your background while keeping yourself in focus.
  - None - Use your real background.
  - Blur - Keeps you in focus while blurring your surroundings to reduce distractions.
  - Background images/videos - Replace your real background with a selected image/video while keeping you in focus.
- Camera resolution: Select **Enable HD** to use high-definition video. Clear **Enable HD** to reduce CPU usage and improve battery life. On mobiles and tablets, HD is disabled by default. To enable it, tap 3-dot menu on self-view > **Enable HD**.

Mirror video

On preview page, click the  icon to disable mirrored view. The icon will change to ; click it again to revert to the mirrored view.

Note: This release introduces a refreshed web app UI, developed using the latest Momentum components. While most previous issues have been resolved, some UI components may not yet fully adapt to all screen sizes. Consequently, users may encounter occasional visual inconsistencies (such as spacing) or minor functionality discrepancies in rare scenarios. These items are being tracked and will be addressed in future releases.

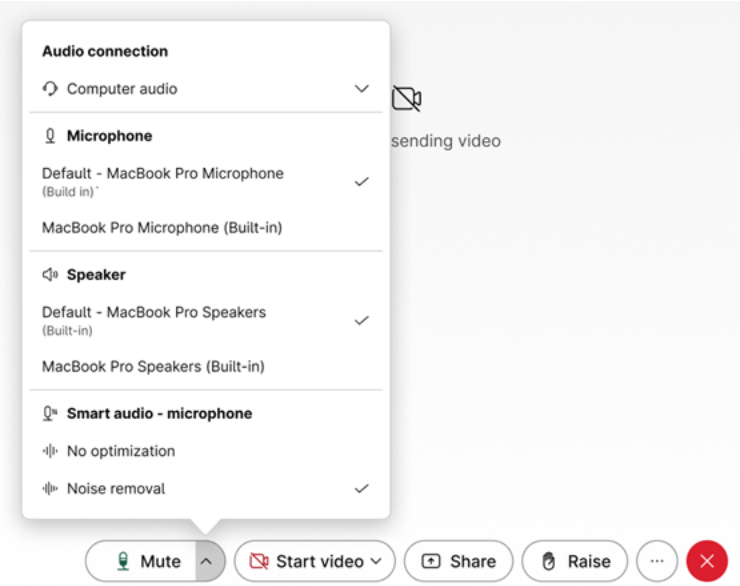
3.3 Suppress ambient noise

Meeting Server 4.0 introduces **Noise Removal** feature that filters ambient background noise before audio is transmitted to other participants, significantly improving meeting clarity.

This feature can be enabled via the **Smart audio-microphone** settings on the **Join call** page or the drop-down menu next to the **Mute** button during a meeting.

- Join call page > Settings > Smart audio-microphone
- In meeting page > drop-down menu next to the **Mute** button > Smart audio-microphone

Once enabled, the preference is automatically saved and applied to all subsequent meetings.



No optimization - The ambient background noise will not be removed before the audio is transmitted to other participants.

Noise removal - The background noise will be removed before the audio is transmitted to other participants.

Note: This feature is supported on web app only.

3.4 Enhanced background blur performance

Web app now utilizes an updated library for background blur processing. This update modifies how background blur and saturation adjustments are rendered. The background blur feature in the previous versions recommended GPU-based systems to ensure optimal performance. This version provides improved support for both CPU and GPU-based environments.

Note:

- This update is supported on Google Chrome, Mozilla Firefox, and Microsoft Edge browsers.
- The updated library supports standard background blur application and saturation level adjustments.
- Performance may vary depending on the specific CPU model and operating system configuration.
- Users of Microsoft Edge may experience performance issues with video backgrounds if " **Enhanced Security Mode**" is enabled. This browser setting restricts certain background processes, which can cause video backgrounds to run slowly and increase CPU usage. To ensure optimal performance, it is recommended that the " **Enhance your security on the web**" setting be configured to **Basic** or **disabled** within the Microsoft Edge privacy settings (edge://settings/privacy). This behavior is specific to Microsoft Edge and does not affect other browsers such as Chrome or Firefox.

3.5 Support for virtual video backgrounds

In version 4.0 of web app, the virtual background capabilities have been enhanced to offer more dynamic customization options. Meeting Server administrators can now upload video files to be used as virtual video backgrounds, building upon the existing support for image backgrounds. This enhancement gives administrators greater control over the visual experience in a meeting.

Further, participants can now apply and preview virtual backgrounds before joining a meeting. This feature is available directly from the Join meeting screen, allowing users to configure their background settings before entering the call.

Note:

- Custom backgrounds will appear in web app, if the administrator has uploaded the images and videos to the Meeting Server.
- Web app participants cannot upload their own custom images or video backgrounds to the web app.

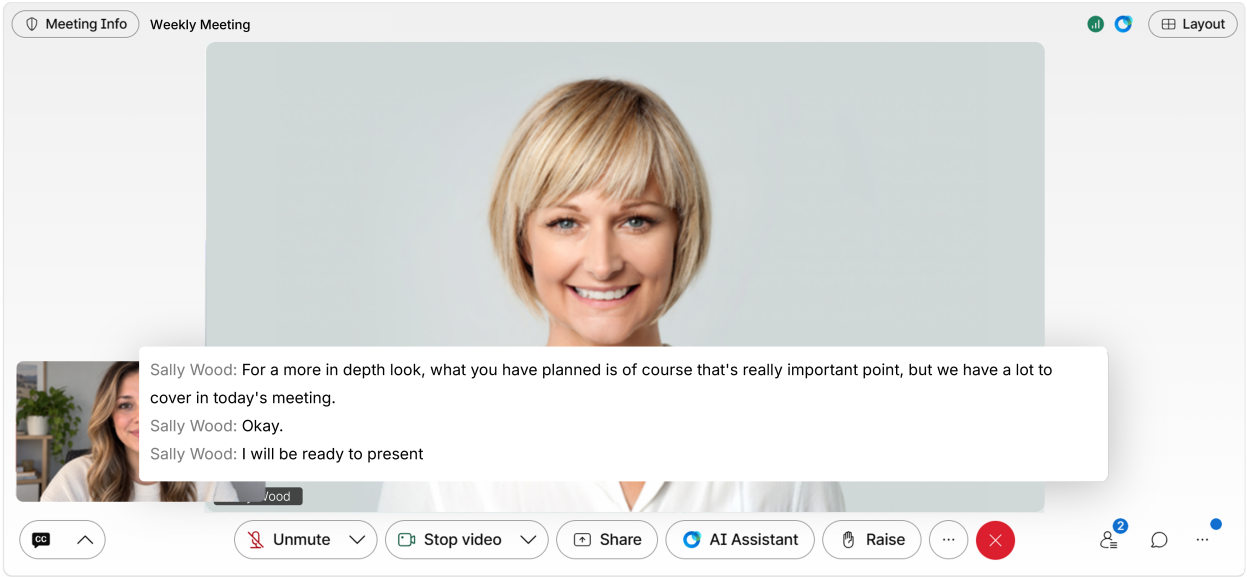
3.6 Automatic closed captions

Version 4.0 introduces automatic, real-time closed captioning powered by Collaboration AI PODs. It utilizes an AI Assistant to transcribe spoken content into captions. By enabling the AI Assistant, participants can view live captions directly on their screen.

Note: This feature is supported on web app only. Availability of this feature is subject to organization's configuration and assigned permissions.

Usage

- Locate the **CC** button in the bottom-left corner of the meeting window; and **AI Assistant** button beside **Share** button.
- Click the **CC** button to toggle the caption overlay on or off.
- Use drop-down on **CC** button or **AI Assistant** button to select preferred spoken language. Use drop-down on **CC** button to change caption language.
- The AI Assistant status indicator shows the transcription status in the meeting header; hover for details.
- View caption history: On bottom-right of the meeting screen **> More panels** (3-dot button) > **Captions**.



Key features:

- The AI Assistant button is enabled for web app participants who have the required permissions.

- AI Assistant takes precedence over legacy manual captioning. When AI Assistant is active, the system suppresses manual captioning to ensure a consistent experience; both features cannot run simultaneously.
- Switching between Manual and Automatic modes during an active call is not supported.
- The AI Assistant session persists for the duration of the meeting, even if the participant who initiated it leaves. The session remains active until an authorized participant disables it or the meeting concludes.
- Currently, there are five supported spoken languages, English, French, German, Italian, and Spanish. English is default language.
- Participants joining after the transcription has started cannot view previously generated captions.
- All meeting participants will receive an audio and visual notification when the AI Assistant starts or stops transcribing. Web app provides toast notifications for successful language updates or error messages if a connection failure occurs.
- The caption overlay is designed with a fixed width and displays up to four lines of text.
- Legacy manual captioning option will be available, if enabled for the call and AI Assistant is configured as Disabled. Participant with required permissions can type captions: Click **More panels** on bottom-right > **Captions**.

Note:

- Captioning is currently limited to transcription only; real-time translation is not supported.
- Save caption history is not available for the captions generated via AI Assistant. It is available for legacy manual captions only.

---

4 Browser versions tested

The table below 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)	156.0.8078.80
Google Chrome (macOS)	154.0.8037.93
Mozilla Firefox (Windows)	159.0.1 (64-bit)
Chromium-based Microsoft Edge (Windows)	156.0.4314.58
Apple Safari for macOS	27.2
Apple Safari for iOS	27.0.1

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.

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.

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.

5 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/meeting-server/products-user-guide-list.html

6 Upgrading and deploying Cisco Meeting Server software version 4.0

CAUTION:

- Any upgrade from earlier versions whether secure storage is enabled or not, to the current version will result in loss of existing configuration and network settings. Therefore, it is critical for users to take a backup of their configuration to an external device before proceeding with the upgrade. This backup must be stored in external location and not on the Meeting Server itself to ensure it remains accessible and safe. Refer to " **White Paper for Upgrade Scenarios and Steps to Upgrade to 4.0**" for mandatory upgrade procedures.
- Once upgraded to release 4.0, downgrade to any of the 3.x versions is not supported on any of the platforms.

This section assumes that you are upgrading from Cisco Meeting Server software version 3.13. If you are upgrading from an earlier version, then you must first upgrade to 3.13 following the instructions in the 3.13 release notes, before following any instructions in this Cisco Meeting Server 4.0 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 3.13.

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

6.1 Upgrading to Release 4.0

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. 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. See the MMP Command Reference document for complete details on backup procedures.

Note: Meeting Server backup does not include the MeetingApps secret key. Therefore, after the backup restoration is completed, the MeetingApps secret key must be regenerated and applied manually to all WebBridge nodes.

Note:

- 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.
- 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: This release installs the prerequisites for UEFI Secure Boot, an industry-standard security feature that allows platform firmware to load only trusted, signed boot software. The medium upgrade image now lays down a UEFI boot chain consisting of shim and GRUB, with the kernel command line embedded in the GRUB binary.

During the upgrade you will see the message: 'Installing Secure Boot readiness EFI chain.' This is an expected part of the upgrade process. Secure Boot is not enforced in this release. The GRUB binary is not yet signed, so Secure Boot must remain disabled in the server's UEFI/BIOS configuration. Enabling Secure Boot at this stage will prevent the system from booting. Support for signed boot components and full Secure Boot enforcement will be introduced in a future release.

Meeting Server 4.0 supports the following specifications on ESXi, Nutanix and NFVIS deployments:

Deployment	Specifications
ESXi	ESXi 8.0 update 3k
Nutanix Cluster	AHV - 10.3.1.2 AOS - 7.3.1.2
NFVIS	26.2.1

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_4_0_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:fe1f81a0e272f254eee32f36a9a7cf0a8098d253ffcac7b2ce23ce8c91aa16f8

   Cisco_Meeting_Server_4_0_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:f72caa445bc9e67fd590ae7e6adf7aa0b2fd466700ee8bfb77bd91edb8105727

   Cisco_Meeting_Server_4_0.ova

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

   hash (SHA-512) for Cisco_Meeting_Server_4_0.ova:
   a5cbc719c72935afb77d85b8baf8cfa61ddc811f0e306418374c2a1bf5b46cdceb3652d79415a4e0847c095133cbfe2f0a273ab749cf6491e78a758c7e905972

   Cisco_Meeting_Server_4_0_appliance_medium-upgrade.zip

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

   Hash (SHA-256) for upgrade.img file:
   2405f838597d34b4035d0f2f99beea73442625f91bf58368538c43629c995fc8

   Cisco_Meeting_Server_4_0_appliance_small-upgrade.zip

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

   Hash (SHA-256) for upgrade.img file:
   2405f838597d34b4035d0f2f99beea73442625f91bf58368538c43629c995fc8

2. To validate the OVA file, the checksum for the 4.0 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 <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.

6.2 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.

6.2.1 Points to note

6.2.1.1 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.

6.2.1.2 Cisco Meeting Server Small/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.

7 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 4.0.
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.

7.1 Resolved issues in Meeting Server 4.0

Issues seen in previous versions that are fixed in 4.0.

Cisco identifier	Summary
CSCwt95025	The web app participant list displayed inconsistent mute/unmute status for calls distributed across Call Bridge nodes in clustered deployments.
CSCww60571	Meeting Server incorrectly logged “no client instance to copy TURN credentials from” as an ERROR during outgoing SIP call creation, although signaling and media were unaffected.
CSCww60535	Meeting Server CUCM XML-RPC service lacked request-size and worker limits, potentially causing temporary service unavailability.
CSCww86900	A memory leak in configd on M8 hardware exhausted system memory, causing media service termination and disruption in active calls.

Cisco identifier	Summary
CSCwu93730	Updated the CMS 3.13 display to accurately reflect FIPS 140-3 compliance instead of FIPS 140-2.
CSCwt91722	System logs may be flooded with repeated "**tcgetattr: Input/output error**" messages due to attempts to start a serial console on an unavailable virtual environment.
CSCwv44761	Secondary nodes in a Meeting Server cluster may fail to receive or process logo configurations during call transfers using the SIP Replaces mechanism, causing the rendering process to abort due to empty file references.
CSCwt91318	When FIPS is enabled, the Nginx process crashes intermittently, causing instability in the system's web services. This issue disrupts normal operations and requires investigation to identify the root cause and implement a resolution. The crashes occur unpredictably during FIPS-enabled operation, impacting service availability.
CSCwt91229	While this operation is allowed in the Webadmin interface, the web app erroneously dis plays an error stating that the passcode must be between 8 and 63 digits long. When a passcode is present and its length is less than the minimum passcode length of 8, the API returns an HTTP 400 error with the message: " passcode" : " The passcode must contain at least 8 digits." This inconsistency causes users to be unable to remove passcodes via the web app.
CSCwm72253	Meeting Server Webadmin uses an outdated jQuery JavaScript library which might have known vulnerabilities.
CSCwv68858	While joining a meeting or leaving a space in web app, system triggers false " Could not get Rest Node Connection" error logs for setPresenceInfo and resetPresenceInfo operations.
CSCwv91122	Sending an unsupported POST API request to Meeting Server with a malformed Authorization header caused the Meeting Server client_backend process to crash and generate a core dump. This results in the loss of active Webbridge3 connections for affected users.
CSCww6059	Users with the crypto SFTP role can use directory traversal to write .png files outside the designated directory.
CSCww60527	Invalid conference.destroy requests can still delete a CoSpace, which is achieved by misusing cached Meeting Server client authority from a previous session and bypassing current authentication checks.
CSCwu14054	During peak concurrency, SSO authentication requests fail to complete within configured timeout thresholds, preventing successful user authentication.
CSCwt88045	Meeting Server crashes abruptly when using the API Explorer to modify layout templates when API tracing is enabled.
CSCwv42215	LDAP users configured via MMP are unable to access webadmin on Meeting Server 2000.

Cisco identifier	Summary
CSCwv50938	The **renameParticipantAllowed** permission in the Meeting Server controls the visibility of the participant rename option in the web app UI. However, users can bypass this restriction using client-side JavaScript to rename participants even when the permission is disabled or hidden through CallLegProfile.
CSCwv64370	The LDAP service in Meeting Server 2000 setups intermittently displays a Not Running status, even though it is enabled and the LDAP server is accessible.
CSCwv91122	Sending an unsupported POST API request to Meeting Server with a malformed Authorization header caused the Meeting Server client_backend process to crash and generate a core dump. This results in the loss of active Webbridge3 connections for affected users.

7.2 Open issues Meeting Server 4.0

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
CSCwx69845	If a single node in the cluster reaches its maximum call capacity, triggering load balancing across other nodes, users may experience functional inconsistencies within breakout rooms.
CSCwx69472	SD and audio call capacity does not scale to the expected call numbers on Meeting Server Small BM/VM.
CSCwx65768	The Scheduler HTTPS interface does not support TLS 1.3; it supports only TLS 1.2.
CSCwx65780	A trailing slash (/) in the webBridgeAddresses field of the API configuration can cause the meeting URL to be generated incorrectly. As a result, the webUrlQuery API will return an invalid URL with double slash, preventing Jabber users from cross-linking with Meeting Server.
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 **`leaveTonePar-ticipantThreshold`** parameters accepts values more than the set maximum value of 100.
CSCwh41791	Failed to access webbridge intermittantly, on Meeting Server 2000.

Cisco identifier	Summary
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.

7.3 Resolved issues in Meeting Server 4.0 web app

The table below lists issues seen in previous versions that are fixed in 4.0.

Cisco Identifier	Summary
CSCws75265	Web app exposed web server information through the Server: nginx response header in WebRTC join links.
CSCwx65080	In Chromium browsers on Windows 11, the web app continued playing meeting audio after users selected **Don't connect to audio**.
CSCww74922	Web app /VERSION page exposed detailed build information when accessed through the web application URL.
CSCwx66900	Web app displayed unexpected GUID entries in the participant list after breakout sessions were ended and restarted.
CSCwt76200	In a web app space, **Cancel** button was misaligned when editing meeting join information in the Japanese-language interface.
CSCwp32445	Web app users on Safari 18.5 and later on MacBook experienced intermittent loss of participant and shared-content audio, along with persistent video lag.
CSCwt96456	The one-click Single Sign-On (SSO) functionality fails to authenticate users when the `allowUnauthenticatedGuests` setting is set to false in the web bridge profile.

7.4 Open issues in Meeting Server 4.0 web app

Cisco Identifier	Summary
CSCwx69859	" Display Name Changed" notification is triggered each time a participant transitions between the main meeting and a breakout room.
CSCwx66889	Web app screen sharing with audio stopped unexpectedly when an external microphone was plugged in or unplugged in Chrome or Edge on Windows.
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.
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: Sample syslog formats

Sample syslog formats

Webapp call:

USERCONFIGSTATS

{
" callLegId" : " 5dfd7ea7-bd15-449a-b6bc-dc1888522b64" ,
" callId" : " 15c25d0e-fb46-42f2-9fdb-73117c436678" ,
" groupId" : " 5dfd7ea7-bd15-449a-b6bc-dc1888522b64" ,
" globalCallId" : " a1b2c3d4-e5f6-7890-abcd-ef1234567890" ,
" layout" : " telepresence" ,
" cameraControlAvailable" : false,
" encryption" : {
" encrypted" : true,
" unencrypted" : false,
" cipherSuite" : " AES_CM_128_HMAC_SHA1_80"
}
}

USERMEDIASTATS

{
" callLegId" : " dab10111-a1cf-4bbc-9bd3-4d52ea63d238" ,
" callId" : " c1148986-445f-4ffb-9489-e1a007357ded" ,
" groupId" : " dab10111-a1cf-4bbc-9bd3-4d52ea63d238" ,
" globalCallId" : " a1b2c3d4-e5f6-7890-abcd-ef1234567890" ,
" layout" : " telepresence" ,
" muteAudioRx" : true,
" muteVideoRx" : true,
" muteAudioTx" : false,
" muteVideoTx" : false,

" mediaStats" : {
" rxAudio" : {
" codec" : " opus" ,
" packetLossPercentage" : 0.0,
" jitterMs" : 1,
" bitRate" : 21970,
" gainApplied" : -6.0
},
" txAudio" : {
" codec" : " opus" ,
" packetLossPercentage" : 0.0,
" jitterMs" : 13,
" bitRate" : 64000,
" roundTripTimeMs" : 53
},
" rxMainVideo" : {
" codec" : " h264" ,
" width" : 0,
" height" : 0,
" frameRate" : 0.0,
" bitRate" : 3509,
" packetLossPercentage" : 0.0,
" jitterMs" : 10
},
" txMainVideo" : {
" codec" : " h264" ,
" width" : 958,
" height" : 538,
" frameRate" : 29.899999618530273,
" bitRate" : 1115652,
" packetLossPercentage" : 0.0,
" jitterMs" : 9,

" roundTripTimeMs" : 57
}
}
}

SIP call:

USERCONFIGSTATS

{
" callLegId" : " 85e81a31-fb6a-4608-b641-11a461dc753c" ,
" callId" : " 15c25d0e-fb46-42f2-9fdb-73117c436678" ,
" groupId" : " 85e81a31-fb6a-4608-b641-11a461dc753c" ,
" globalCallId" : " a1b2c3d4-e5f6-7890-abcd-ef1234567890" ,
" layout" : " telepresence" ,
" cameraControlAvailable" : false,
" encryption" : {
" encrypted" : false,
" unencrypted" : true
}
}

USERMEDIASTATS:

{
" callLegId" : " b0d07485-2199-4562-9c94-7e986bff0dbd" ,
" callId" : " c1148986-445f-4ffb-9489-e1a007357ded" ,
" groupId" : " b0d07485-2199-4562-9c94-7e986bff0dbd" ,
" sipCallId" : " 20e29062-c200-4c64-bc3f-ab4dd4f992a1" ,
" globalCallId" : " a1b2c3d4-e5f6-7890-abcd-ef1234567890" ,
" layout" : " telepresence" ,
" muteAudioRx" : true,
" muteVideoRx" : false,
" muteAudioTx" : false,
" muteVideoTx" : false,

" activeControl" : {
" encrypted" : false,
" remoteSubscription" : {
" capabilities" : true,
" conferenceInfo" : true,
" legacyConferenceInfo" : false,
" layouts" : true,
" legacyLayouts" : false,
" speakerInfo" : true,
" legacySpeakerInfo" : false,
" selfInfo" : true
},
" localSubscription" : {
" capabilities" : true,
" conferenceInfo" : false,
" legacyConferenceInfo" : false,
" layouts" : false,
" legacyLayouts" : false,
" speakerInfo" : false,
" legacySpeakerInfo" : false,
" selfInfo" : false
}
},
" mediaStats" : {
" rxAudio" : {
" codec" : " opus" ,
" packetLossPercentage" : 0.0,
" jitterMs" : 1,
" bitRate" : 16367,
" gainApplied" : -6.0
},
" txAudio" : {

" codec" : " opus" ,
" packetLossPercentage" : 0.0,
" jitterMs" : 5,
" bitRate" : 64000,
" roundTripTimeMs" : 6
},
" rxMainVideo" : {
" codec" : " h264" ,
" width" : 1920,
" height" : 1080,
" frameRate" : 29.899999618530273,
" bitRate" : 1937470,
" packetLossPercentage" : 0.0,
" jitterMs" : 7
},
" txMainVideo" : {
" codec" : " h264" ,
" width" : 1920,
" height" : 1080,
" frameRate" : 4.900000095367432,
" bitRate" : 359,
" packetLossPercentage" : 0.0,
" jitterMs" : 5,
" roundTripTimeMs" : 17
}
}
}

Appendix B: Cisco 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.

The Cisco Meeting Server software 4.0 can be hosted on:

Meeting Server Platform	Variant	Meeting Server deployment
Newer Generations		
Cisco Meeting Server Small	M7	Bare metal OS
Cisco Meeting Server Small	M7	VM deployment (ESXi 8.X)
Cisco Meeting Server Medium	M8	Bare metal OS
Previous Generations		
Cisco Meeting Server 1000	M6, M5v2	VM deployment (ESXi 8.X)
Cisco Meeting Server 2000	M6, M5v2	CMS 2K OS
Spec based hardware		VM deployment (ESXi 8.0)

Call capacities

The following table provides 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 (Bare metal OS)	Cisco Meeting Server Medium M8	Cisco Meeting Server Small M7 (VM deployment)	Cisco Meeting Server 1000 M6	Cisco Meeting Server 2000 M6
Full HD calls 1080p60 video 720p30 content	60	150	60	40	324
Full HD calls 1080p30 video 1080p30/4K7 content	60	150	60	40	324

Type of calls	Cisco Meeting Server Small M7 (Bare metal OS)	Cisco Meeting Server Medium M8	Cisco Meeting Server Small M7 (VM deployment)	Cisco Meeting Server 1000 M6	Cisco Meeting Server 2000 M6
Full HD calls 1080p30 video 720p30 content	120	225	120	80	648
HD calls 720p30 video 720p5 content	240	450	240	160	1296
SD calls 480p30 video 720p5 content	480	850	480	320	1875
Audio calls (G.711)	3000	3000	3000	3000	3200

Note: Virtual deployments on Meeting Server Small M7 variants support a maximum of 94 vCPU and 128 GB RAM.

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 Medium M8(per node)	Cisco Meeting Server Small M7(Bare metal OS)	Cisco Meeting Server Small 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	225 450 850 3000	120 240 480 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	225 450 850 3000	120 240 480 3000	120 240 480 3000	648 1296 1875 1875
Meeting Servers in a Call Bridge Group	Call type supported				
	Load limit	450,000	240,000	240,000	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.
- 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.
- Meeting Server Small M7 variants support a maximum of 94 vCPU and 128 GB RAM.
- Meeting Server M8 platform supports a maximum load limit of 450,000.

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 , X15.5.21. 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 (X15.5.21)	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 4.0	Web app 3.13	Web app 3.12	Web app 3.11	Web app 3.10
General					
Cisco Meeting Server version	4.0	3.13	3.12	3.11	3.10
Managing access for members	Yes	Yes	Yes	Yes	Yes
User-level permissions (e.g. can create space)	Yes	Yes	Yes	Yes	Yes
Support for localization	Yes	Yes	Yes	Yes	Yes
Branding	Yes	Yes	Yes	Yes	Yes
Online help	Yes	Yes	Yes	Yes	Yes
Encryption	Yes	Yes	Yes	Yes	Yes
Single sign on	Yes	Yes	Yes	Yes	Yes
One-click SSO	Yes	Yes	No	No	No
Support for custom pages in online help	Yes	Yes	Yes	Yes	No
Refreshed user interface (color, font, and icons)	Yes	Yes	Yes	No	No
UI Enhancements: Preview page, One-click SSO, Meeting controls	Yes	No	No	No	No
Join using video address (URI)	Yes	Yes	Yes	Yes	Yes
Notifications					
Audio notification when participant joins/leaves	Yes	Yes	Yes	Yes	Yes
Connection resiliency (Auto reconnect in bad network)	Yes	Yes	Yes	Yes	Yes
Web app session timeout	Yes	Yes	Yes	No	No
Schedule a meeting					

Feature	Web app 4.0	Web app 3.13	Web app 3.12	Web app 3.11	Web app 3.10
View list of scheduled meeting	Yes	Yes	Yes	Yes	Yes
Schedule a meeting	Yes	Yes	Yes	Yes	Yes
Modify a scheduled meeting	Yes	Yes	Yes	Yes	Yes
Delete a scheduled meeting	Yes	Yes	Yes	Yes	Yes
Space Management					
Space member roles	Yes	Yes	Yes	Yes	Yes
All permissions except 'Leave space' are disabled by default for new coSpace members	Yes	Yes	No	No	No
Meeting invite links for members-only space	Yes	Yes	Yes	No	No
Restrict access of non-members to space	Yes	Yes	Yes	Yes	Yes
Create / edit space	Yes	Yes	Yes	Yes	Yes
Activate newly provisioned spaces	Yes	Yes	Yes	Yes	Yes
Add / edit / delete space members	Yes	Yes	Yes	Yes	Yes
Directory look up for Add Members feature	Yes	Yes	Yes	Yes	Yes
View information for space	Yes	Yes	Yes	Yes	Yes
Send invitation	Yes	Yes	Yes	Yes	Yes
Audio and video					
Audio	OPUS	OPUS	OPUS	OPUS	OPUS
Video	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8
Mic/camera configuration controls	Yes	Yes	Yes	Yes	Yes
Speaker configuration controls	Yes	Yes	Yes	Yes	Yes
Blur your background	Yes	Yes	Yes	Yes	Yes

Feature	Web app 4.0	Web app 3.13	Web app 3.12	Web app 3.11	Web app 3.10
Virtual background	Yes	Yes	Yes	Yes	Yes
Virtual background: Videos	Yes	No	No	No	No
Virtual background on preview page	Yes	No	No	No	No
Far end camera control	Yes	Yes	Yes	Yes	Yes
Auto prioritization of audio and video	Yes	Yes	Yes	Yes	Yes
Noise removal	Yes	No	No	No	No
Screen share					
Content magnification	Yes	Yes	Yes	Yes	Yes
Reset content zoom	Yes	Yes	Yes	Yes	Yes
View screen share	Yes	Yes	Yes	Yes	Yes
Desktop sharing	Yes	Yes	Yes	Yes	Yes
Application sharing	Yes	Yes	Yes	Yes	Yes
View screen share in a new window	Yes	Yes	Yes	Yes	Yes
Re-size the video pane	Yes	Yes	Yes	Yes	Yes
Share content audio	Yes	Yes	Yes	Yes	Yes
Optimize for Text (Share screen in 1080p)	Yes	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	Yes, in meeting only
Chat (Private)	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only
Export chat history	Yes	Yes	Yes	No	No
In-call					
On-screen messages	Yes	Yes	Yes	Yes	Yes
Full-screen view	Yes	Yes	Yes	Yes	Yes
Layout control	Yes	Yes	Yes	Yes	Yes

Feature	Web app 4.0	Web app 3.13	Web app 3.12	Web app 3.11	Web app 3.10
Name labels	Yes	Yes	Yes	Yes	Yes
Recording	Yes	Yes	Yes	Yes	Yes
Streaming	Yes	Yes	Yes	Yes	Yes
Active speaker label (Beta support)	Yes	Yes	Yes	Yes	Yes
Self-view	Yes	Yes	Yes	Yes	Yes
Pin self-view	Yes	Yes	Yes	Yes	Yes
Mirror self-view	Yes	Yes	Yes	Yes	Yes
Move self-view	Yes	Yes	Yes	Yes	Yes
HD/SD selection	Yes	Yes	Yes	Yes	Yes
Pin presentation preview	Yes	Yes	Yes	Yes	Yes
Move presentation preview	Yes	Yes	Yes	Yes	Yes
Meeting notes	Yes	Yes	Yes	Yes	Yes
Closed captioning	Yes	Yes	Yes	Yes	Yes
Share files	Yes	Yes	Yes	Yes	Yes
Network health indicator and media statistics	Yes	Yes	Yes	Yes	Yes
Content share metrics	Yes	Yes	Yes	Yes	Yes
Logo support	Yes	Yes	Yes	Yes	Yes
Surveys	Yes	Yes	Yes	Yes	Yes
Breakout rooms	Yes	No	No	No	No
Automatic closed captions	Yes	No	No	No	No
Participants					
Rename participants	Yes	Yes	Yes	No	No
Increased character limit for participant names	Yes	Yes	Yes	Yes	No
User identification in Participants list	Yes	Yes	Yes	Yes	No

Feature	Web app 4.0	Web app 3.13	Web app 3.12	Web app 3.11	Web app 3.10
Configurable user indicators in Participants list	Yes	Yes	Yes	No	No
Move participant	Yes	Yes	Yes	Yes	Yes
Add participant	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)
Remove participants	Yes	Yes	Yes	Yes	Yes
Admit participants to a locked meeting	Yes	Yes	Yes	Yes	Yes
Change a participant's role	Yes	Yes	Yes	Yes	Yes
Make participant important	Yes	Yes	Yes	Yes	Yes
Mute/Unmute other participants' audio and video individually	Yes	Yes	Yes	Yes	Yes
Mute/Unmute all participants' audio and video	Yes	Yes	Yes	Yes	Yes
Send diagnostics during a meeting	Yes	Yes	Yes	Yes	Yes
Send invite	Yes	Yes	Yes	Yes	Yes
View call info	Yes	Yes	Yes	Yes	Yes
Mic / Camera controls during call	Yes	Yes	Yes	Yes	Yes
Raise hand	Yes	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	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.

© 2026 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

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