Cisco Meeting Server and web app

Release 3.13

Release Notes

07 September, 2026

Contents

What's changed 4

1 Introduction 5
- 1.1 Cisco Meeting Server 5
- 1.2 Cisco Meeting Server web app 5
  - 1.2.1 Using the web app 5
- 1.3 Smart Licensing 6
- 1.4 End of Software Maintenance 7
- 1.5 Deprecation Notice 7

2 What's new in Cisco Meeting Server 8
- 2.1 Configuring One Click Single Sign On (Beta feature) 8
- 2.2 Configuring short term credentials for Meeting Server deployments with Expressway as Turn server 9
  - 2.2.1 API additions 10
- 2.3 TLS 1.3 support validation with IM and Presence 11
- 2.4 Media downspeeding 11
  - 2.4.1 MMP additions 11
- 2.5 TLS certificate policy update and Cisco Meeting Server 3.13 compatibility 12
- 2.6 Enhanced load monitoring in Cisco Meeting Server 12
- 2.7 Passcode requirements and validation for coSpaces 14
  - 2.7.1 API Modifications 16
- 2.8 New platform support: Nutanix 16
- 2.9 Summary of API additions and changes 16
- 2.10 Summary of MMP additions and changes 18
- 2.11 Related user documentation 18

3 What's new in Cisco Meeting Server web app 20
- 3.1 One-click Single Sign-On (SSO) 20
- 3.2 Modifications to default permissions for new coSpace members 20

4 Browser versions tested 22

Important note for users using iOS 13 or later and macOS 10.15 or later 22

Important note about screen sharing on Chrome on macOS 10.15 or later 23

Important note about accessibility settings in Safari browsers 23

Important note about audio and video issues observed in Safari browsers 23

Important note about group policy settings in Microsoft Edge 23

5 Product documentation 24

6 Upgrading, downgrading and deploying Cisco Meeting Server software version 3.13 25
6.1 Upgrading to Release 3.13 25
6.2 Downgrading 27
6.3 Cisco Meeting Server Deployments 28
6.3.1 Points to note 29

7 Bug search tool, resolved and open issues 30
7.1 Resolved issues in Cisco Meeting Server 30
7.2 Open issues in Cisco Meeting Server 31
7.3 Known limitations 32
7.4 Resolved issues in Cisco Meeting Server web app 32
7.5 Open issues in Cisco Meeting Server web app 33

Appendix A: Meeting Server platform maintenance 34
Cisco Meeting Server Small and other virtualized platforms 34
Cisco Meeting Server Medium 34
A.1 Cisco Meeting Server 2000 34
Call capacities 34
Cisco Meeting Server web app call capacities 37
Cisco Meeting Server web app call capacities – external calling 37
Cisco Meeting Server web app capacities – mixed (internal + external) calling 38

Appendix B: Apps feature comparison 39

Accessibility Notice 44

Accessibility Support Features 45

Cisco Legal Information 46

Cisco Trademark 47

What's changed

Version	Change
Sep 3, 2026	Maintenance release for 3.13.1 See Resolved issues.
May 4, 2026	New version for release 3.13.

.

1 Introduction

This document describes the changes in version 3.13 of the Cisco Meeting Server software and Cisco Meeting Server web app.

1.1 Cisco Meeting Server

The Cisco Meeting Server software can be hosted on:

- Cisco Meeting Server Small, installed as a VM deployment.
- Cisco Meeting Server Medium, UCS C245 M8 Rack Server with AMD Genoa (4thGen) processors and Cisco Meeting Server software pre-installed.
- Cisco Meeting Server 1000, installed as a VM deployment.
- Cisco Meeting Server 2000, a UCS 5108 chassis with 8 B200 blades and the Meeting Server software pre-installed as the sole application.
- Or on a specification-based VM server.

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

Note: Cisco Meeting Management handles the product registration and interaction with your Smart Account for Smart Licensing support. Meeting Management 3.13 is required with Meeting Server 3.13.

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

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

1.2 Cisco Meeting Server web app

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

1.2.1 Using the web app

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

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

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

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

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

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

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

1.3 Smart Licensing

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

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

1.4 End of Software Maintenance

On release of Cisco Meeting Server software version 3.13, 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 3.11	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.11.x is Oct 2026.

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

1.5 Deprecation Notice

- Cisco has initiated the process of deprecating support for Skype for Business and TelePresence Interoperability Protocol in the Meeting Server. Support for these features will be removed in a future release. We recommend preparing for the transition to supported alternatives to avoid any disruption in the service.
- Discontinuation of Cloud Connected Service for Cisco Meeting Management: Cisco has initiated the process of discontinuing the Cloud Connected Service for Cisco Meeting Management. Support for this service will be withdrawn from 3.13.

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 3.13:

- Configuring One Click Single Sign On
- Configuring short term credentials for Meeting Server deployments with Expressway as Turn server
- TLS 1.3 support validation with IM and Presence
- Media downspeeding
- TLS Certificate policy update and Cisco Meeting Server 3.13 compatibility
- Enhanced load monitoring in Cisco Meeting Server
- Passcode requirements and validation for coSpaces

New platform support

- New platform support: Nutanix

2.1 Configuring One Click Single Sign On (Beta feature)

Version 3.13 enhances the Single Sign-On (SSO) experience in the Cisco Meeting Server web app by enabling automatic redirection. When a default domain is configured, users are no longer required to manually enter their username during the login process.

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

To enable this feature, set the new **`isDefaultIdp`** parameter to true within your config.json file. Once enabled, the Meeting Server identifies the first domain listed in the **`supportedDomains`** array as the default domain. Other configured domains remain accessible via **Alternate SSO**.

Points to Note:

- **Default Behavior**: If the **`isDefaultIdp`** parameter is not added in the config.json file, the sign-in experience remains unchanged; participants must continue to select " **Sign in**" and provide their credentials in **username@domain** format.

- **UI Indicator**: The " **SSO Sign in**" label will only appear when a **`default IdP`** is configured, enabling one-click SSO.
- **Managing Multiple Domains**: To change the default domain, administrators must reorder the **`supportedDomains`** list so that the preferred domain appears first.
- **Configuration Conflicts**: Only one identity provider should be set as the default (**isDefaultIdp: true**). If multiple identity providers are configured with this parameter set to true, the system will default to the alphabetically first SSO configuration file.

Example: config.json file

This is an example config.json file:

```
{
" authenticationIdMapping" : " <uid>" ,
" ssoServiceProviderAddress" : " https://<domain>:<port>" ,
" supportedDomains" : [" <domain1>" ," <domain2>" ],
" isDefaultIdp" : true
}
```

Refer to Deployment Guides for more information on configuring Single Sign On.

2.2 Configuring short term credentials for Meeting Server deployments with Expressway as Turn server

This feature allows Meeting Server to support short-term credentials when integrating with Expressway as a TURN server. It provides secure access for external clients joining meetings via Meeting Server by using credentials that are valid for a short duration. By leveraging short-term credentials, the system minimizes the risk of credential theft or misuse, ensuring that only authorized clients can access media traversal services temporarily and securely.

The credentials generated will be valid for 24 hours. These credentials are generated on a per-call basis by the Meeting Server and stored in Expressway-C for every web app call join request. After the call disconnects, the credentials are deleted. If the credentials expire during an active media session, the media session will be reconnected to maintain the call continuity.

Note: This feature has been validated on Cisco Expressway version X15.4.

Prerequisites:

- Set the **`useShortTermCredentials`** parameter to **true** and the **`type`** parameter to **expressway** in the TURN server configuration.

- The Call Bridge needs to trust the CA that signed the Expressway-C certificate and it can be achieved by either signing the Call Bridge certificate and Expressway- C certificate with the same CA, or build a CA bundle and apply it to Call Bridge. This is needed to avoid " HTTPS 60 Error" during POST request for Short-Term TURN Credentials.

  Note: Ensure that all FQDNs or IP address for the Meeting Server, Expressway-C, and Expressway-E are included in the CSR under the Subject Alternative Name (SAN) field to avoid HTTPS 60: Error

- When configuring multiple TURN servers via the Meeting Server API in an Expressway TURN deployment, ensure that all TURN servers use the same credential mode either long-term or short-term. This will help to prevent security conflicts such as the exposure of plain passwords.
- The **domain** name configured in the Meeting Server under **`credentialServerAddress`** and **`username_prefix`** must be same as configured in the Expressway-C configurations under **domain**.
- Ensure that the **`credentialServerUsername`** (The username of the Expressway – C server) configured on **/api/v1/turnservers** on Meeting Server has the required API access permissions set to true on Expressway-C (which is set to false by default in Expressway x15.X) this is to avoid 401 authroization error between Meeting Server and Expressway-C

Note: In an Expressway TURN deployment with short-term credential mode, failover for a configured credential server in a clustered Expressway-C server is currently not supported on Meeting Server.

2.2.1 API additions

The following new API parameters are introduced to implement this support in the Meeting Server.

- **Creating**: POST method to the " **`/turnServers`**" node
- **Modifying**: PUT to " **`/turnServers/`**"
- **Retrieving**: GET on " **`/turnServers`**" node

Parameter	Type/value	Description
credentialServerAddress	String	The address that Meeting Server must use to connect to Expressway-C for the TURN server. The URL should include the protocol https://, followed by the **fully qualified domain name** (FQDN) or IP address and port of your Expressway-C server.
credentialServerUsername	String	The username of the Expressway – C server.
credentialServerPassword	String	The password of the Expressway – C server.
username_prefix	String	The username prefix, formatted as **JC:<domainname of credential server>**, should be used as a prefix along with the short-term username generated by Meeting Server when making allocations on this TURN server. **Example** : **JC:test.example.com**

Refer to Deployment Planning and Preparation Guide for more information on Expressway deployments.

2.3 TLS 1.3 support validation with IM and Presence

As part of the ongoing effort to support TLS 1.3 across all components of Meeting Server, Meeting Server 3.13 has been validated for interoperability scenarios with Cisco Unified Communications Manager IM and Presence.

2.4 Media downspeeding

Meeting Server introduces MMP commands to manage media downspeeding in Meeting Server conferences under varying network conditions.

Administrators can enable/disable media downspeeding using the **callbridge media_downspeeding <enable/disable>** MMP commands. If unset, media downspeeding is enabled by default.

2.4.1 MMP additions

Note: This command must be used only under the guidance of the Cisco Support team.

Command	Description
`callbridge media_downspeeding disable`	Disables downspeeding. If unset, media downspeeding is enabled by default. **Note:** Restart call bridge for the changes to be applied.
`callbridge media_downspeeding enable`	Enables downspeeding. **Note:** Restart call bridge for the changes to be applied.

2.5 TLS certificate policy update and Cisco Meeting Server 3.13 compatibility

Meeting Server version 3.13 has been validated to support the updated TLS Certificate Policy, where Public Certificate Authorities (CAs) will no longer issue certificates containing the Client Authentication (clientAuth) Extended Key Usage (EKU). Instead, certificates will be issued with only the Server Authentication (serverAuth) EKU.

Meeting Server will no longer enforce client EKU validation on certificates. All services and components within the Meeting Server will continue to work with the existing certificates without requiring any changes to the certificates in current deployments.

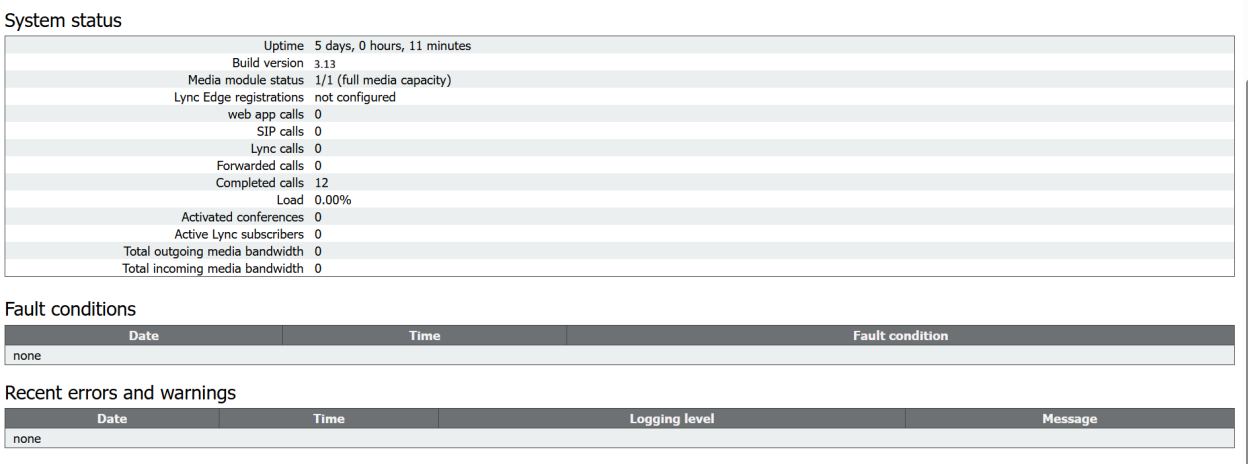
If certificates with the client authentication EKU are required, such as for database connections, it is recommended to generate these through an internal or private Certificate Authority (CA).

2.6 Enhanced load monitoring in Cisco Meeting Server

Meeting Server introduces a new **`load`** attribute in the web admin interface that periodically logs data and displays the real-time load status as a percentage. This feature enables proactive management of server resources within a cluster environment.

Load Percentage Calculation:

The load percentage is calculated based on the server's configured **`loadLimit`** and is displayed in the System status under the General tab of the Meeting Server web admin interface. Administrators can refresh the Webadmin UI page to view the latest load percentage.



System status

Uptime	5 days, 0 hours, 11 minutes
Build version	3.13
Media module status	1/1 (full media capacity)
Lync Edge registrations	not configured
web app calls	0
SIP calls	0
Lync calls	0
Forwarded calls	0
Completed calls	12
Load	0.00%
Activated conferences	0
Active Lync subscribers	0
Total outgoing media bandwidth	0
Total incoming media bandwidth	0

Fault conditions

Date	Time	Fault condition
none		

Recent errors and warnings

Date	Time	Logging level	Message
none			

If the `loadLimit` API parameter is not configured by the administrator, the **System Status** tab for Load displays " **not configured**" .

Parameters used in calculation:

- **mediaProcessingLoad**: The current media processing load on the server.
- **loadLimit**: The maximum load configured for the server.
- **Thresholds values**: the existing conference threshold and the new conference threshold using the values derived from:
  - **existing conference threshold** = existingConferenceLoadLimitBasisPoints/10000×loadLimit
  - **new conference threshold** = newConferenceLoadLimitBasisPoints/10000×loadLimit

For detailed information on load balancing and thresholds, refer to the ***" Load Balancing Calls Across Cisco Meeting Servers" white paper***.

Eventlogs and Syslogs:

Meeting Server captures the threshold values as Info, Warnings, and Errors every five minutes, in the eventlogs and syslogs.

Severity	Condition	Action
INFO	If Load percentage < New conference threshold	Information will be captured in Event Log and Syslog. LOAD_MONITOR: {" currentLoad" : X," loadLimit" : Y," loadPercentage" : Z%," message" : " NA" }

Severity	Condition	Action
WARNING	• If Load percentage > New conference threshold • If Load percentage > Existing conference threshold	Warning will be captured in Event Log, Syslog, and Recent Errors & Warnings. LOAD_MONITOR: {" currentLoad" : X," loadLimit" : Y," loadPercentage" : Z%," message" :" Incoming calls to new conferences will be rejected on callbridge <Callbridge hostname> " }
ERROR	If Load percentage > 100%	Error will be captured in Event Log, Syslog, and Recent Errors & Warnings. LOAD_MONITOR: {" currentLoad" : X," loadLimit" : Y," loadPercentage" : Z," message" :" New conferences and participants will be rejected on callbridge <Callbridge hostname> " }

This enhanced load monitoring capability helps administrators maintain optimal server performance and avoid overload by providing clear, real-time visibility into server load and threshold events.

2.7 Passcode requirements and validation for coSpaces

The Passcode rule for coSpaces is updated to enforce a minimum passcode length of 8 digits and the passcode must contain only digits. Previously, there was no minimum passcode length requirement, and passcodes could be alphanumeric strings.

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

If the minimum passcode length in the **dial-in security profile** was set to less than 8 digits or allowed alphanumeric characters in a previous version, it is recommended after upgrading to version 3.12.1 to update the minimum passcode length to a value between 8 and 63 digits and ensure the passcode consists only of numeric characters.

CAUTION: When upgrading to Meeting Server 3.13, all meeting access PINs must have at least 8 digits. If Cisco TelePresence Management Suite scheduled meetings use PINs shorter than 8 digits, they will fail to launch on Meeting Server after the upgrade.

Points to note

- The updated passcode rule applies to **coSpaces** and **dialInSecurityProfiles**, only when a passcode is configured or modified.
- Existing **coSpaces** and configurations are unaffected unless their passcodes are changed.

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

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

The passcode rule is enforced on the following API methods:

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

2.7.1 API Modifications

API method	Parameter	Type/value	Description/Notes
POST/PUT on /dialInSecurityProfiles	minPasscodeLength	Number	The minimum allowed passcode length: 0 or between 8 to 63 digits in length (inclusive).
POST/PUT on /coSpaces/accessMethods	passcode	Number	The security code for the access method. The minimum allowed passcode length: 0 or between 8 to 63 digits in length (inclusive).
POST/PUT on /coSpaces	passcode	Number	The security code for the coSpace. The minimum allowed passcode length: 0 or between 8 to 63 digits in length (inclusive).

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

2.8 New platform support: Nutanix

Starting with version 3.13, Meeting Server supports deployment on Nutanix clusters. This configuration is supported on 220 M7+ HCI nodes, and all Meeting Server 3.13 components have been fully validated for this environment.

- Required AHV Version: 10.3.1.2
- Required AOS Version: 7.3.1.2

Note: Meeting Server support on Nutanix is limited to fresh installations. Direct migration of Meeting Server virtual machines from ESXi to Nutanix is not supported; however, existing Meeting Server Virtual Machines in-line to 3.13 version on ESXi can be moved to Nutanix deployments using the backup and restore procedure.

2.9 Summary of API additions and changes

API functionality for Meeting Server 3.13 includes the following API additions.

- **`Load`** API attribute is added in the web admin interface that periodically logs data and displays the real-time load status as a percentage.

- The following API parameters are added to support short-term credentials when integrating with Expressway as a TURN server.
    - Creating: POST method to the "`/turnServers`" node
    - Modifying: PUT to "`/turnServers/`"

Parameter	Type/value	Description
`credentialServerAddress`	String	The address that Meeting Server must use to connect to Expressway-C for the TURN server. The URL should include the protocol https://, followed by the **fully qualified domain name** (FQDN) or IP address and port of your Expressway-C server, and then the fixed API path /api/v1/turnServers/.
`credentialServerUsername`	String	The username of the Expressway – C server.
`credentialServerPassword`	String	The password of the Expressway – C server.
`username_prefix`	String	The username prefix, formatted as **`JC:<domainname of credential server>`**, should be used as a prefix along with the short-term username generated by Meeting Server when making allocations on this TURN server.

API functionality for Meeting Server 3.13 includes the following API modifications.

- The following API parameters are modified to enforce minimum passcode length for coSpaces from 0 or between 8 to 63 digits in length (inclusive).

  API Modifications

API method	Parameter	Type/value	Description/Notes
POST/PUT on /dialInSecurityProfiles	minPasscodeLength	Number	The minimum allowed passcode length: 0 or between 8 to 63 digits in length (inclusive).
POST/PUT on /coSpaces/accessMethods	passcode	Number	The security code for the access method. The minimum allowed passcode length: 0 or between 8 to 63 digits in length (inclusive).

API method	Parameter	Type/value	Description/Notes
POST/PUT on /coSpaces	passcode	Number	The security code for the coSpace. The minimum allowed passcode length: 0 or between 8 to 63 digits in length (inclusive).

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

2.10 Summary of MMP additions and changes

- Meeting Server 3.13 has been validated for TLS 1.3 support in interoperability scenarios with Cisco Unified Communications Manager IM and Presence.
- The following MMP commands are added to enable/disable media downspeeding.

  Note: This command must be used only under the guidance of the Cisco Support team.

Command	Description
`callbridge media_downspeeding disable`	Disables downspeeding. If unset, media downspeeding is enabled by default. **Note:** Restart call bridge for the changes to be applied.
`callbridge media_downspeeding enable`	Enables downspeeding. **Note:** Restart call bridge for the changes to be applied.

2.11 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:

- One-click Single Sign-On (SSO)
- Modifications to default permissions for new coSpace members

3.1 One-click Single Sign-On (SSO)

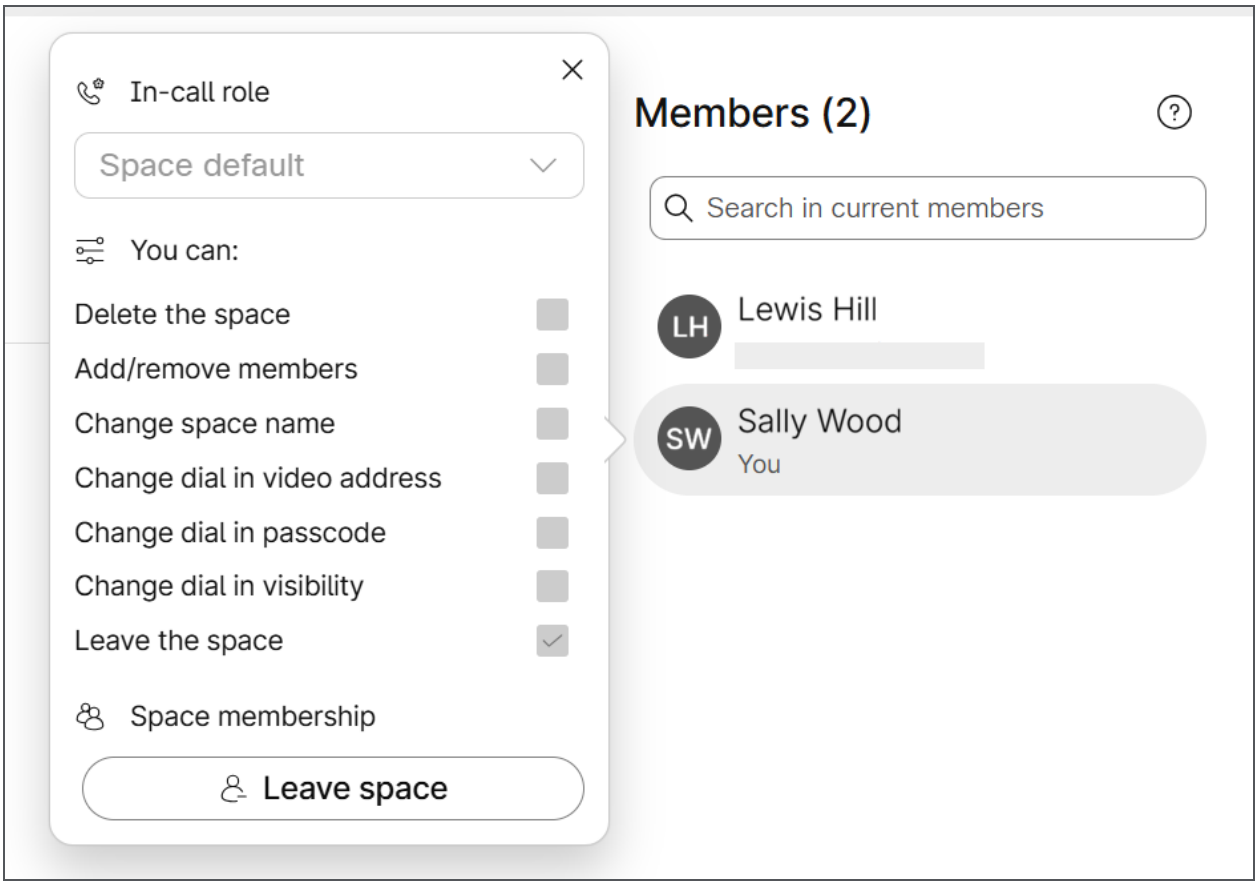
From version 3.13, web app introduces a more efficient SSO authentication flow. By configuring a default domain, administrators can enable one-click SSO. This allows participants to access the Web App home page via the '**SSO Sign in**' button without having to manually re-enter their credentials.

Note:

- If no default SSO domain is set, the sign-in experience remains unchanged. Participants should select **Sign in** and then enter their username to sign in.
- If multiple SSO domains are configured, and one domain is set as the default, users get a **SSO sign in** button for that domain and Use **alternate SSO** option to sign in with another domain.

3.2 Modifications to default permissions for new coSpace members

In previous versions of web app, when a member was added to a coSpace, all permissions (such as Delete the space, Add/remove members, Change space name, Change dial in video address, Change dial in passcode, Change dial in visibility, and Leave the space) were enabled by default and/or copied from the owner. From 3.13, only the **Leave the space** permission is enabled by default for newly added members; all other permissions are disabled, allowing coSpace owners to grant additional permissions as needed.



Note: This change applies to all new member additions in coSpaces. Existing members are not affected unless their permissions are modified by coSpace owner.

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)	146.0.7680.177
Google Chrome (macOS)	146.0.7680.81
Mozilla Firefox (Windows)	149.0
Chromium-based Microsoft Edge (Windows)	146.0.3856.84
Apple Safari for macOS	26.4
Apple Safari for iOS	26.4.1

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 audio and video issues observed in Safari browsers

CSCwp32445

In Safari versions 26.3 and 26.4.1 on iOS devices, users experience intermittent audio issues during meetings. Unlike previous occurrences limited to screen sharing sessions with content audio, this issue now also affects meetings without content sharing. Users initially hear participant audio but then lose both participant and shared content audio.

This issue was previously observed in Safari 18.5 on MacBook systems only during screen sharing sessions with content audio. The current behavior extends to iOS Safari and occurs regardless of content sharing.

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

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, downgrading and deploying Cisco Meeting Server software version 3.13

IMPORTANT:

- This release includes updates to the platform components. Performing a new deployment will provide a refined installation experience aligned with these updates.

This section assumes that you are upgrading from Cisco Meeting Server software version 3.12. If you are upgrading from an earlier version, then you must first upgrade to 3.12 following the instructions in the 3.12 release notes, before following any instructions in this Cisco Meeting Server 3.13 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 3.12.

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 3.13

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

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

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

Upgrading the firmware is a two-stage process: first, upload the upgraded firmware image; then issue the upgrade command. This restarts the server: the restart process interrupts all

active calls running on the server; therefore, this stage should be done at a suitable time so as not to impact users – or users should be warned in advance.

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

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

   Cisco_Meeting_Server_3_13_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:c7e297467ffd2dbf99a5fa49dea5be2f82b8c62a095eb98bb4a7d4e9cef9da9e

   Cisco_Meeting_Server_3_13_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:ad140d1f691b8e32b704f5f3114350382ca907cab373ab973581df01a0dbb4ff

   Cisco_Meeting_Server_3_13.ova

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

   hash (SHA-512) for Cisco_Meeting_Server_3_13.ova:
   b57fbde6c0074c75327805fa9e393e28ec27fa4d8adfb2c3a6ec80de056809694416ad85e29798c2e1a36b81025b67a32eb93b0e5d0080f91fcd66f38b87d386

   Cisco_Meeting_Server_3_13_appliance-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:
   0da961b3bb777bcdc688a08d2427a5fc4c65100945bd1f788e1d809fe5022a19

2. To validate the OVA file, the checksum for the 3.13 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 Downgrading

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

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

Note: If you are downgrading from version 3.13 with secure storage enabled, the process will be aborted. To proceed, perform a **`<factory_reset full>`** to clear secure storage settings, then downgrade to the desired version.

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

   The Server/ virtualized server will restart automatically – allow 10-12 minutes for the process to complete and for the Web Admin to be available after downgrading the server.
3. Log in to the Web Admin and go to Status > General and verify the new version is showing under System status.
4. Use the MMP command **`factory_reset app`** on the server and wait for it to reboot from the factory reset.
5. Restore the configuration backup for the older version, using the MMP command **`backup rollback <name>`** command.

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

   The Meeting Server will reboot to apply the backup file.

   For a clustered deployment, repeat steps 1-5 for each node in the cluster.
6. Finally, check that:
   - the Web Admin interface on each Call Bridge can display the list of coSpaces.
   - dial plans are intact,
   - no fault conditions are reported on the Web Admin and log files.
   - you can connect using SIP and Cisco Meeting Apps (as well as Web Bridge if that is supported).

   The downgrade of your Meeting Server deployment is now complete.

6.3 Cisco Meeting Server Deployments

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

- Single Combined Meeting Server – all Meeting Server components (Call Bridge, Web Bridge 3, Database, Recorder, Uploader, Streamer and TURN server) are available, the Call Bridge and Database are automatically enabled but the other components can be

individually enabled depending upon the requirements of the deployment. All enabled components reside on a single host server.

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

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

6.3.1 Points to note

6.3.1.1 Cisco Meeting Server 2000

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

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

6.3.1.2 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 3.13.
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 Cisco Meeting Server

Issues seen in previous versions that are fixed in 3.13.

Cisco identifier	Summary
CSCwt01653	The first participant pane is not displayed correctly when the custom layout 'onePlusFour' is applied through Pane Placement using Meeting Management. The first participant's image does not fill the full screen, leaving gaps at the top and bottom, which affects the meeting display and prevents participants from appearing as expected.
CSCws27917	The logo for the standard screen layout does not appear on SIP devices when the user connects and disconnects multiple times. This issue occurs specifically with SIP end points during repeated connection attempts.

Cisco identifier	Summary
CSCws62493	VIP users connected via CUCM Cluster B experience one-way audio 15 minutes into Meeting Server meetings due to a media renegotiation failure during session refresh. This issue causes an encryption mismatch that interrupts audio from the Meeting Server to the endpoint, requiring a manual Hold/Resume to resolve.
CSCwt91229	While this operation is allowed in the Webadmin interface, the web app erroneously displays 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.
CSCwt37736	The media process crashes consistently about one second after a WebRTC (WB3/Chrome) participant joins a conference. The crash occurs in the AV1 video decode path during the initial stream start and decoder synchronization phase, causing the media module to terminate while call control remains active until the call is dropped due to media inactivity. This issue is reproducible during the join sequence and does not depend on call duration. The crash affects only the media blade process and does not cause a full Meeting Server control-plane failure.
CSCwt91364	Meeting Server provisioning via Meeting Management fails due to the default settings in the dial-in security profile.

7.2 Open issues in Cisco Meeting Server

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

Cisco identifier	Summary
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.
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.

Cisco identifier	Summary
CSCwh41791	Failed to access webbridge intermittantly, on Meeting Server 2000.
CSCwd89530	If the packet capture is not stopped gracefully using Ctrl+C and the terminal is closed abruptly, further packet captures are not possible until CMS reboot.
CSCwb77929	In a deployment with multiple Web Bridge, web app participants can see the Meeting notes only if they are connected to the same webbridge where the notes was saved and published initially.
CSCwa83782	A conference is booked on TMS as Automatic connect type and one of the participants is joining the conference through an unmanaged device. When the conference starts, the participant is called by CMS/TMS, but Meeting Serverdisconnects the call after some time.
CSCvz01886	When a participant's role does not have permissions to share video and presentation, then the role is changed and they have permissions to share video and presentation, the presentation is not visible to other participants when they share content.
CSCvt74033	When content is being shared and an event happens to trigger a Webex Room Panorama to drop from sending two video streams to one, the video frame rate being received by a remote endpoint from the Room Panorama can drop noticeably.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.

7.3 Known limitations

- CSCwt85559 - Meeting Server version 3.13 is not supported with Cisco Expressway 15.5.

  Workaround - Version 3.11 is the recommended release for compatibility with Expressway 15.5.

7.4 Resolved issues in Cisco Meeting Server web app

The table below lists issues seen in previous versions that are fixed in 3.13.

Cisco Identifier	Summary
CSCwt93423	Clicking the **Join** button of a cospace redirects to the 'Join Information' page instead of the 'Join Meeting' page.
CSCwt93421	On iPad Safari (Desktop Site mode), users are repeatedly prompted to allow pop-ups on page refresh.
CSCwr88103	In Microsoft Edge, a blank pop-up appears on web app page refresh after allowing pop-ups; multiple refreshes generate multiple persistent blank pop-ups.
CSCwt93417	On the 'Email or copy invite' pop-up, the **Copy** button fails to copy email invite content.

Cisco Identifier	Summary
CSCwq10397	'Meeting created' popup appears when scheduling a yearly recurring meeting with an invalid date, though meeting is not created and does not show under upcoming meetings.
CSCwp96170	On the 'Email or copy invite' screen, some language names in the 'Language' drop-down are not displayed correctly.
CSCwi05238	Web app briefly shows an error message 'Sign in failed' when participant is logging in.

7.5 Open issues in Cisco Meeting Server web app

Cisco Identifier	Summary
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: Meeting Server platform maintenance

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

Cisco Meeting Server Small and other virtualized platforms

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

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

Cisco Meeting Server Medium

The Cisco Meeting Server Medium platform is built on the Cisco UCS technology using a preconfigured Cisco UCS C245 M8 Rack Server with AMD Genoa (4thGen) processors.

A.1 Cisco Meeting Server 2000

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

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

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 1000 M6	Cisco Meeting Server Small M7	Cisco Meeting Server 2000 M6	Cisco Meeting Server Medium M8
Full HD calls 1080p60 video 720p30 content	40	60	324	150
Full HD calls 1080p30 video 1080p30/4K7 content	40	60	324	150
Full HD calls 1080p30 video 720p30 content	80	120	648	225
HD calls 720p30 video 720p5 content	160	240	1296	450
SD calls 480p30 video 720p5 content	320	480	1875	850
Audio calls (G.711)	3000	3000	3200	3000

Note: 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 Small M7 (per node)	Cisco Meeting Server 2000 M6(per node)	Cisco Meeting Server Medium M8(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	120 240 480 3000	648 1296 1875 3200	225 450 850 3000
	HD participants per conference per server			
	web app call capacities (internal calling & external calling on CMS web edge): Full HD HD SD Audio calls	120 240 480 3000	648 1296 1875 1875	225 450 850 3000
Meeting Servers in a Call Bridge Group	Call type supported			
	Load limit	240,000	1,296,000	450,000

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 X15.4, earlier Expressway versions are not supported by Web Bridge 3.

Table 5: Cisco Meeting Server web app call capacities – using Expressway for external calling

Setup	Call Type	CE1200 Platform	Large OVA Expressway	Medium OVA Expressway
Per Cisco Expressway (X14.3 or later)	Full HD	150	150	50
	Other	200	200	50

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

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

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

Both standalone and clustered deployments can support combined internal and external call usage. When supporting a mix of internal and external participants the total web app capacity will follow Table 4 for Internal Calls and if using Cisco Meeting Server web edge solution for external calling. However, if using Expressway at the edge, the number of participants within the total that can connect from external is still bound by the limits in Table 5.

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

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

Appendix B: Apps feature comparison

Table 6:Feature comparison for Cisco Meeting Server web app

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

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

Feature	Web app 3.13	Web app 3.12	Web app 3.11	Web app 3.10
Auto prioritization of audio and video	Yes	Yes	Yes	Yes
Screen share				
Content magnification	Yes	Yes	Yes	Yes
Reset content zoom	Yes	Yes	Yes	Yes
View screen share	Yes	Yes	Yes	Yes
Desktop sharing	Yes	Yes	Yes	Yes
Application sharing	Yes	Yes	Yes	Yes
View screen share in a new window	Yes	Yes	Yes	Yes
Re-size the video pane	Yes	Yes	Yes	Yes
Share content audio	Yes	Yes	Yes	Yes
Optimize for Text (Share screen in 1080p)	Yes	Yes	Yes	Yes
Chat				
Chat (Broadcast to all participants in the meeting)	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only
Chat (Private)	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only
Export chat history	Yes	Yes	No	No
In-call				
On-screen messages	Yes	Yes	Yes	Yes
Full-screen view	Yes	Yes	Yes	Yes
Layout control	Yes	Yes	Yes	Yes
Name labels	Yes	Yes	Yes	Yes
Recording	Yes	Yes	Yes	Yes
Streaming	Yes	Yes	Yes	Yes
Active speaker label (Beta support)	Yes	Yes	Yes	Yes
Self-view	Yes	Yes	Yes	Yes
Pin self-view	Yes	Yes	Yes	Yes

Feature	Web app 3.13	Web app 3.12	Web app 3.11	Web app 3.10
Mirror self-view	Yes	Yes	Yes	Yes
Move self-view	Yes	Yes	Yes	Yes
HD/SD selection	Yes	Yes	Yes	Yes
Pin presentation preview	Yes	Yes	Yes	Yes
Move presentation preview	Yes	Yes	Yes	Yes
Meeting notes	Yes	Yes	Yes	Yes
Closed captioning	Yes	Yes	Yes	Yes
Share files	Yes	Yes	Yes	Yes
Network health indicator and media statistics	Yes	Yes	Yes	Yes
Content share metrics	Yes	Yes	Yes	Yes
Logo support	Yes	Yes	Yes	Yes
Surveys	Yes	Yes	Yes	Yes
Participants				
Rename participants	Yes	Yes	No	No
Increased character limit for participant names	Yes	Yes	Yes	No
User identification in Participants list	Yes	Yes	Yes	No
Configurable user indicators in Participants list	Yes	Yes	No	No
Move participant	Yes	Yes	Yes	Yes
Add participant	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)
Remove participants	Yes	Yes	Yes	Yes
Admit participants to a locked meeting	Yes	Yes	Yes	Yes
Change a participant's role	Yes	Yes	Yes	Yes
Make participant important	Yes	Yes	Yes	Yes

Feature	Web app 3.13	Web app 3.12	Web app 3.11	Web app 3.10
Mute/Unmute other participants' audio and video individually	Yes	Yes	Yes	Yes
Mute/Unmute all participants' audio and video	Yes	Yes	Yes	Yes
Send diagnostics during a meeting	Yes	Yes	Yes	Yes
Send invite	Yes	Yes	Yes	Yes
View call info	Yes	Yes	Yes	Yes
Mic / Camera controls during call	Yes	Yes	Yes	Yes
Raise hand	Yes	Yes	Yes	Yes
Move call				
Use this device for screen share and call management only (while another device is used for audio and video)	Yes	Yes	Yes	Yes

Accessibility Notice

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

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

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

You can find more information about accessibility here:

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

Accessibility Support Features

Keyboard navigation

You can use your keyboard to navigate through web app.

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

Screen reader support

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

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

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

Cisco Legal Information

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

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

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

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

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

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

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

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

© 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)