Cisco Meeting Server and web app

Release 3.8.2

Release Notes

09 August, 2024

Contents

What's changed

Version	Change
August 9, 2024	Maintenance release 3.8.2 See [Resolved Issues.](#)
November 9, 2023	Maintenance release 3.8.1 See [Resolved Issues](#), [Enhancements in 3.8.1](#).
September 7, 2023	First release for version 3.8

1   Introduction

This document describes the new features, improvements and changes in version 3.9 of the Cisco Meeting Server software and Cisco Meeting Server web app.

1.1   Cisco Meeting Server

The Cisco Meeting Server software can be hosted on:

- Cisco Meeting Server 2000, a UCS 5108 chassis with 8 B200 blades and the Meeting Server software pre-installed as the sole application.

- Cisco Meeting Server 1000, a Cisco UCS server pre-configured with VMware and the Cisco Meeting Server installed as a VM deployment.

- Or on a specification-based VM server.

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

Note: Cisco Meeting Management handles the product registration and interaction with your Smart Account for Smart Licensing support. Meeting Management 3.9 is required with Meeting Server 3.9.

■ **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.

1.3   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 3.9, 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 3.7	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.7.x is August, 2024.
Cisco Meeting Server version 3.6.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.6.x is Jan 05, 2024.

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

2   Cisco Meeting Server

This section of the document lists the new features and changes implemented in Meeting Server version 3.8.

2.1 Enhancements in 3.81

- User search optimization in web app

2.2 What's new in Cisco Meeting Server

Following are the new features and changes introduced in this release:

- Web app session timeout
- Enabling Surveys in Meeting Server
- Updating Jabber Presence
- Adding tags to coSpaces
- Configuring screen resolution for content shared in web app
- Assigning a name to callProfiles
- Support to send chat messages to a particular participant in a web app meeting
- Screen sharing improvements

2.2.1 User search optimization in web app

Version 3.8.1 introduces improvements in the Meeting Server to reduce the time taken to search, retrieve and add participants to spaces or while scheduling web app meetings. Previously, the search took longer when the active directory has more than 100,000 users and the search names contain language-specific characters. With the improvements made in this release, the search time has been reduced significantly.

Note: It is required to resync the LDAP using web admin for this improvement to take effect.

2.2.2 Web app session timeout

The default timeout value for web app sessions is 24 hours. From version 3.8, administrators can configure this value in the Meeting Server. A new MMP command `callbridge wc3jwt expiry <expiry time in hours>` is added to set the session timeout, in hours. The command accepts values ranging from 1 to 24.

2.2.2.1 MMP additions

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

2.2.3 Enabling surveys in Meeting Server

Version 3.8 introduces the Surveys feature, which allows web app meeting hosts to make the meeting more interactive by inviting participants to share their opinion.

This feature is enabled at call level and participant level. Enabling it at the call level determines if the meeting can have surveys or not and enabling it at the participant level determines if the participant can create/launch/delete/view results of surveys or not.

2.2.3.1 API additions

A new API parameter `surveyAllowed` is introduced to enable/disable the Survey feature at call level. The parameter is supported on the following API methods:

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

Request parameters	Type/ Value	Description/ Notes
`surveyAllowed`	`true`|`false`	True – Indicates that surveys are allowed in the meeting and participants can take survey.
		False – Indicates that surveys are not allowed in the meeting.
		The usual rules for the hierarchy of calls and call profiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to false.

Additionally, a new API parameter `surveyOpsAllowed` is introduced to enable/disable the Survey feature at the participant level. The parameter is supported on the following API methods:

- POST to **/calls/<call id>/callLegs**

- PUT to **/callLegs/<callLegId>**

- GET on **/callLegs/<callLegID>**

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

- POST to **/callLegProfiles**

- GET on **/callLegProfiles/<call leg profile id>**

- PUT to **/callLegProfiles/<call leg profile id>**

Request parameters	Type/ Value	Description/ Notes
surveyOpsAllowed	true|**false**	True – Indicates that the participant can create/launch/delete/view results of surveys.
		False – Indicates that the participant cannot create/launch/delete/view results of surveys.
		The usual rules for the hierarchy of calls and call profiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to false.

This feature is implemented through the MeetingApps service. Refer to [Cisco Meeting Server Single split deployment guide](#) for details on deploying the MeetingApps service and [Cisco Meeting Server MMP guide](#) for configuring MeetingApps.

2.2.4   Updating Jabber presence

2.2.4.1   Enhancements in Jabber user status messages

Version 3.8 introduces modifications to the presence status messages of Jabber users. In the previous release of version 3.7, when a Jabber user signs into web app and joins a meeting, Meeting Server updates the Jabber status to 'In a meeting, In a call'. From version 3.8, this status message has been modified to read 'On a call'.

Further improvements have been made in the Meeting Server to show appropriate availability status when the Jabber user joins a Meeting Server web app meeting.

As in the previous release, Meeting Server reverts to the previous status after the user ends the meeting. Meeting Server does not update the Jabber status in the following cases:

- If the Jabber user is in another meeting/call while joining the web app meeting, Meeting Server does not update the Jabber status.

- If the Jabber user has set their status to DND – Do not disturb or manually set to away, before joining the web app meeting, Meeting Server does not update the Jabber status.

- If the user updates the Jabber status manually anytime during the web app meeting, Meeting Server does not override the manually updated user status.

- Meeting Server will not update the presence for content share.

Note: The Meeting Server connects with the IMP server using TCP port 8083. If there is a firewall between IMP servers and Meeting Server call bridge, it is recommended to open this port to allow communication.

2.2.4.2   Enabling secure communication between Meeting Server and Cisco Unified Communications Manager/IMP Server

Version 3.8 enables secure communication between Meeting Server and Cisco Unified Communications Manager/IMP servers. This is achieved by installing and verifying the CA certificate bundle between the entities.

New MMP commands have been introduced to install and verify the certificates for Cisco Unified Communications Manager and IMPS in Meeting Server. The CUPS certificate for IMP Server and Tomcat certificate for Cisco Unified Communications Manager must be uploaded and verified in the Meeting Server.

To install the certificates for Cisco Unified Communications Manager and IMPS:

1. Using your SFTP client, log into Meeting Server and copy the certificate authority bundle file to your Meeting Server.

2. SSH into MMP of the Meeting server.

3. Assign the certificate for CUCM and IMPS using the following commands:

    a. For Cisco Unified Communications Manager:

        `callbridge ucm certs <cert-bundle>`

    b. For IMPS:
        `callbridge imps certs <cert-bundle>`

Note: Use the MMP commands `callbridge ucm certs none` or `callbridge imps certs none` to remove the Cisco Unified Communications Manager or IMPS certificate from the Meeting Server respectively.

To verify the TLS certificate for IMPS:

You can enable/disable the TLS verification for Cisco Unified Communications Manager and IMP Server using the following commands:

1. To enable/disable the TLS verification between Meeting Server and Cisco Unified Communications Manager use:
    `callbridge ucm verify <enable/disable>`

2. To enable/disable the TLS verification between Meeting server and IMPS use:
    `callbridge imps verify <enable/disable>`

3. Restart the call bridge to apply these changes using the command.
    `callbridgerestart`

4. You may check the CUCM services using the MMP command
    `callbridge imps <hostname/IP> <presence_user> presence_service status`

Similarly, the callbridge certificate bundle for Meeting Server must be uploaded to the CUPS trust store for IMP server and Tomcat trust store for Cisco Unified Communications Manager.

2.2.4.3 MMP additions

Command / Examples	Description
`callbridge ucm certs <cert-bundle>`	Adds the CA trusted certificate for Cisco Unified Communications Manager.
`callbridge ucm verify <enable/disable>`	Enables/disables TLS verification between Meeting Server and Cisco Unified Communications Manager.
`callbridge ucm certs none`	Removes the certificate added for TLS verification between Meeting Server and Cisco Unified Communications Manager.
`callbridge imps certs <cert-bundle>`	Adds the CA trusted certificate for IMP server.
`callbridge imps verify <enable/disable>`	Enables/disables TLS verification between Meeting Server and IMP server.
`callbridge imps certs none`	Removes the certificate added for TLS verification between Meeting Server and IMP server.

2.2.5 Adding tags to coSpaces

From version 3.8, Meeting Management video operators can be given access to only those meetings and spaces that they are associated with. Administrators can enable this feature by adding a tag to each coSpace in the Meeting Server API which will be used by Meeting Management to retrieve the respective meeting spaces. These tags when assigned to the video operators in Meeting Management, will determine the spaces or the meetings they will have access to.

A new API parameter has been introduced on the `coSpaces` API, to support this feature. Administrators can set a name of choice for the tags while creating or modifying the `coSpaces` API. Each coSpace can have one tag only. However, the same tag name can be added to multiple coSpaces.

Note: Tags added or modified for a coSpace during an ongoing meeting in Meeting Management, will reflect only from the subsequent meeting/session.

2.2.5.1   API additions

A new API parameter `spaceTag` is added to the `coSpaces` API. The parameter is supported on the following methods:

POST to `/coSpaces`

PUT to `/coSpaces/<coSpace ID>`

GET on `/coSpaces`

GET on `/coSpace/<coSpace ID>`

Request parameters	Type/ Value	Description/ Notes
`spaceTag`	String	Name of the tag given to the particular `coSpace`. Tag for each space is unique, case–insensitive and may contain up to ten characters.

2.2.6   Configuring screen resolution for content shared in web app

Version 3.8 provides the option to set the maximum resolution of the presenter's screen, while sharing content in web app meeting. However, in varying network conditions, the screen resolution adapts based on available bandwidth but will not exceed the maximum limit specified. For example, if the limit is set to 720p, the sender's screen share resolution can go lower but not exceed 720p.

Screen resolution can be set as 720p, 1080p or unrestricted. By selecting unrestricted web app relies on browser to set the resolution for content share.

This feature is implemented using the new `contentResolution` parameter in the `webBridgeProfiles` API.

2.2.6.1   API additions

A new API parameter `contentResolution` is added to the `webbridgeProfile` API. This parameter is supported on POST, PUT and GET methods on `/webBridgeProfiles/`.

Request parameters	Type/ Value	Description/ Notes
`contentResolution`	720p|1080p|unrestricted	The maximum resolution of the presenter's screen while sharing content in web app.

2.2.7   Assigning a name to callProfiles API

From version 3.8, system administrators can search and retrieve `callProfiles` by its name. This makes it easier to search for the required `callProfiles` using the name as against the `callProfile ID`, which is an autogenerated long string.

The `callProfiles` API has been enhanced to include the `name` parameter for each `callProfiles` created. A name of choice can be assigned using the new parameter while creating or modifying the `callProfiles`. This parameter can have a maximum length of 200 characters. A new filter option is added in the `callProfiles` API in the Meeting Server web interface to search the `callProfile` using the name attribute.

2.2.7.1   API additions

A new `name` API parameter is introduced on the `callProfiles` API. This parameter is supported on the following methods:

POST to `/callProfiles/`

PUT to `/callProfiles/<call profile id>/`

GET on `/callProfiles/<call profile id>/`

GET on `/callProfiles/`

Request parameters	Type/ Value	Description/ Notes
name	String	Name of the `callProfiles`.

2.2.8   Support to send chat messages to a particular participant in a web app meeting

Version 3.8 introduces support to send chat messages to a particular participant during a web app meeting. Previously, web app participants could send messages that were broadcast to everyone in the meeting. With this release, web app participants can choose to send messages to everyone or to a particular participant in the meeting.

The existing API parameters `chatAllowed` and `chatContributionAllowed` are used to support this feature on web app. This feature is supported on web app only.

2.2.8.1   API additions

The `chatAllowed` request parameter is used to enable/disable chat at a call level. The parameter is supported on the following API operations:

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

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

Request parameters	Type/ Value	Description/ Notes
chatAllowed	**true**|false	If the value is specified, it determines whether or not chat is allowed on this call/s using this call profile.

Additionally, the administrator can control at a finer level of granularity which participants in a given call are allowed to send chat messages using the **chatContributionAllowed** parameter. The parameter is supported on the following API operations:

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

Request parameters	Type/ Value	Description/ Notes
chatContributionAllowed	**true**|false	If the value is specified, it determines whether or not this call leg/this participant/call legs using this **callLegProfile** are allowed to send messages on the chat.

2.2.9 Screen sharing Improvements

Improvements have been made in the Meeting Server to enhance the screensharing/ presentation quality in a web app meeting. Enhancements have been made to take care of keep alive packets from Chrome while presentation is shared and reduce any packet loss because of the same. Further, the MaxQp value of the H.264 encoder has been modified for better image and video quality.

2.3 Summary of API additions and changes

API functionality for Meeting Server 3.8 includes the following new API parameters.

New API parameter is added to search callProfile API by name

- **name** is introduced on:

  - POST to **/callProfiles/**

  - PUT to **/callProfiles/<call profile id>/**

  - GET on **/callProfiles/**

  - GET on **/callProfiles/<call profile id>/**

New API parameter is added to set the maximum resolution on the presenter's screen in web app meeting

- **contentResolution** parameter is introduced on:

  - POST, PUT and GET methods on **/webBridgeProfiles/**

New API parameter is added to add tags to coSpaces

- **spaceTag** parameter is introduced on:

  - POST to **/coSpaces**

  - PUT to **/coSpaces/<coSpace ID>**

  - GET on **/coSpaces**

  - GET on **/coSpace/<coSpace ID>**

New API parameter is added to enable the Surveys feature in web app:

- **surveyAllowed** is introduced on:

  - POST to **/calls/**

  - PUT to **/calls/call id/**

  - GET on **/calls/call id/**

  - POST to **/callProfiles**

  - PUT to **/callProfiles/<call profile id>**

  - GET on **/callProfiles/<call profile id>**

- **surveyOpsAllowed** is introduced on:

  - POST to **/calls/<call Id>/callLegs**

  - GET on **/callLegs/<callLeg ID>**

  - PUT to **/callLegs/<callLeg ID>**

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

  - POST to **/callLegProfiles**

- GET on **/callLegProfiles/<call leg profile id>**
- PUT to **/callLegProfiles/<call leg profile id>**

API parameter enhanced to enable sending chat messages to a particular participant

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

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

2.4 Summary of MMP additions and changes

Version 3.8 supports the MMP additions described in this section.

Enabling secure communication between Meeting Server and Cisco Unified Communications Manager/IMP Server

The commands for TLS verification between Meeting Server and Cisco Unified Communications Manager/IMP server are listed below:

Command / Examples	Description
callbridge ucm certs <cert-bundle>	Adds the CA trusted certificate for Cisco Unified Communications Manager.
callbridge ucm verify <enable/disable>	Enables/disables TLS verification between Meeting Server and Cisco Unified Communications Manager.

Command / Examples	Description
`callbridge ucm certs none`	Removes the certificate added for TLS verification between Meeting Server and Cisco Unified Communications Manager.
`callbridge imps certs <cert-bundle>`	Adds the CA trusted certificate for IMP server.
`callbridge imps verify <enable/disable>`	Enables/disables TLS verification between Meeting Server and IMP server.
`callbridge imps certs none`	Removes the certificate added for TLS verification between Meeting Server and IMP server.

Configuring web app session timeout

Administrators can set the web app session timeout, in hours using the command below:

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

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   Upgrading, downgrading and deploying Cisco Meeting Server software version 3.8.2

This section assumes that you are upgrading from Cisco Meeting Server software version 3.7. If you are upgrading from an earlier version, then you must first upgrade to 3.7 following the instructions in the 3.7 release notes, before following any instructions in this Cisco Meeting Server 3.8.2 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 3.7.

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

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

3.1   Upgrading to Release 3.8.2

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, before upgrading your Meeting Servers, uncluster all the nodes using the `database cluster remove` command. Users must uncluster the nodes, upgrade Meeting Server and cluster the nodes back using the 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 <u>software download</u> pages of the Cisco website:

    Cisco_Meeting_Server_3_8_2_CMS2000.zip

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

    Hash (SHA-256) for upgrade.img

    file:fe59b28d20f081dcba502a9a0147b9418669d42b8870e8c1e1bf91109ddb45b8

    Cisco_Meeting_Server_3_8_2_vm-upgrade.zip

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

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

    8cc4b0328e1ffd86aabaaf6f55a7da2740e5b33e989543bec8cb97462572ce2a

    Cisco_Meeting_Server_3_8_2_vSphere-7_0.ova

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

    For vSphere7.0 and higher, hash (SHA-512) for Cisco_Meeting_Server_3_8_2_vSphere-7_0.ova:
    0bb0cd75887459c2d10bf886b9142c05c78e04a59db142450c723ba3d601966a4eda202ac4bc774e0afa2
    7b7e4160357a5464366eff99d74e0ff94aadbc5517f

2. To validate the OVA file, the checksum for the 3.8.2 release is shown in a pop up box that appears when you hover over the description for the download. In addition, you can check the integrity of the download using the SHA-512 hash value listed above.

    Note: VMware has discontinued support for ESXi 6.x versions and Meeting Server will no longer be tested in any of the 6.x versions. This release supports ESXi 7.0.x only. Support for ESXi 8.0 will be added in the upcoming releases.

    ---

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.

Note: If the active directory has more than 100K users and the participant names contain language-specific characters, resync the LDAP using web admin to reduce the time taken to search and add participant names to spaces or while scheduling web app meetings.

3.2 Downgrading

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

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

2. To apply the downgrade, use the SSH connection to the MMP and start the downgrade by executing the `upgrade <filename>` command.

    The Server/ virtualized server will restart automatically — allow 10-12 minutes for the process to complete and for the Web Admin to be available after downgrading the server.

3. Log in to the Web Admin and go to **Status > General** and verify the new version is showing under **System status**.

4. Use the MMP command `factory_reset app` on the server and wait for it to reboot from the factory reset.

5. Restore the configuration backup for the older version, using the MMP command `backup rollback <name>` command.

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

The Meeting Server will reboot to apply the backup file.

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

6. 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.

3.3 Cisco Meeting Server Deployments

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

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

- single split Meeting Server — in this model the TURN server, 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.

3.3.1 Points to note

3.3.1.1 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.

3.3.1.2 Cisco Meeting Server 1000 and specification-based VM server

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

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

4   Cisco Meeting Server web app

This section of the document describes the new features and changes in this release of the Cisco Meeting Server web app.

4.1   What's new in Cisco Meeting Server web app

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

- Optimize content share in a meeting

- Create surveys in a meeting

- Improved virtual background performance

- In-meeting private chat

- Support for Czech language

- UI modification

- Accessibility improvements

4.1.1   Optimize content share in a meeting

Version 3.8 gives web app users have the flexibility to optimize the screen resolution while sharing content in a web app meeting. To implement this feature, a new option **Optimize for Text** is added in the self-view settings menu under ⬓ **Sharing** section.

When a participant checks this option while sharing their screen, web app will override any screen share resolution set by the administrator in Meeting Server and the screen is shared in 1080p resolution. If left unchecked, the content will be shared as per the resolution set by the administrator. Until changed, a participant's preference for **Optimize for Text** is saved and used in subsequent meetings.

Note: The participant must restart the screen share after selecting **Optimize for Text** for the screen resolution to take effect. Web app also notifies the participant with an onscreen message to restart the screen share.
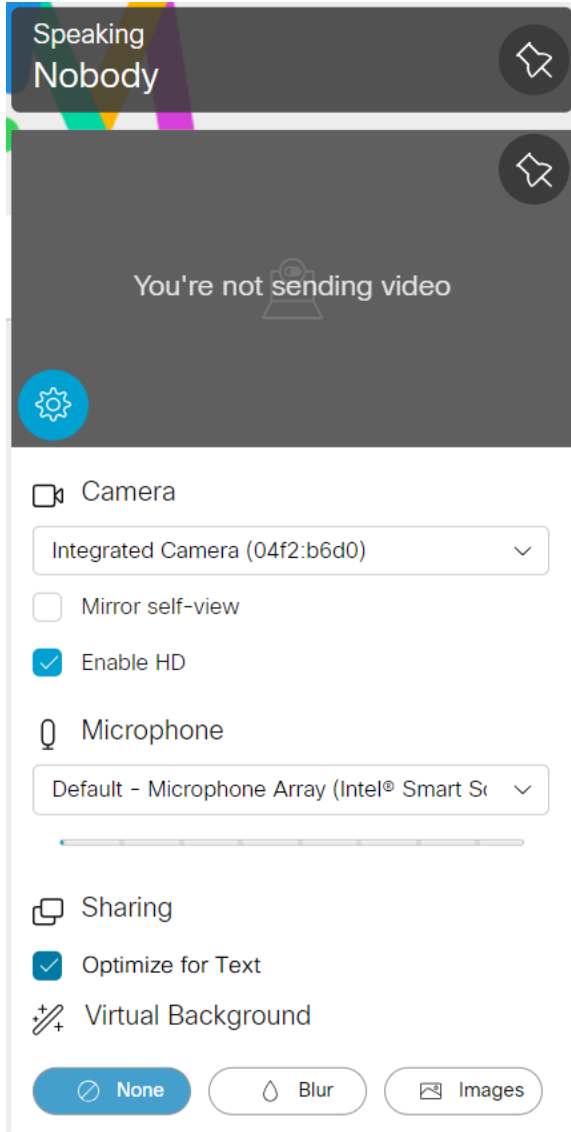
Note: The screen resolution is set only on the sender's screen while sharing screen.

4.1.2 Create surveys in a meeting

From version 3.8, web app allows participants with appropriate permissions to create surveys in a meeting. A new 🔲 **Surveys** icon is added on the side panel as an in-meeting menu option to create and participate in the surveys during the meeting.

Note: 🔲 **Surveys** icon is visible to the participants, only if the feature is enabled for the meeting, in the Meeting Server.

Surveys can be created and launched by the meeting organizer. A web app meeting can have only one active survey at a time. Each survey can have a maximum of 5 questions. Each

question must have a minimum of 2 choices and a maximum of 4 choices with the participant selecting one of them. Multiple answer entries or free form text answers are not allowed.

A red dot on the **Surveys** icon ᐧᐧᐧ indicates that a new survey is active. Web app also notifies the participants in the meeting, when a survey is launched by the meeting organizer.

To create a survey, select ᐧᐧᐧ **Surveys** on the side pane:

- Select **Survey Dashboard** > **Create survey**, to create a survey. Enter the survey title, question(s), and options, then select **Save**.

  Note: Double quotation mark **"** is not allowed in the survey's title/question/options. Participant cannot save or create new surveys if **"** is used.

- Select ⊙ **Launch**, to activate the saved survey.
  Participants can see the survey, only when it is launched by the meeting organizer.
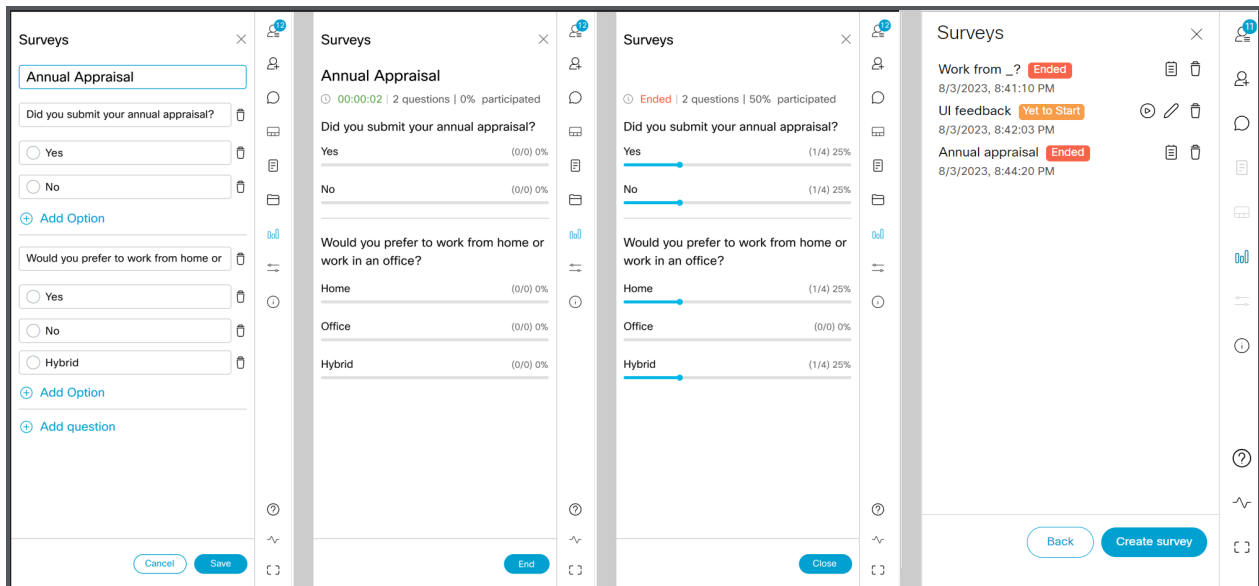
Meeting organizer(s):

Meeting organizer(s) with appropriate permissions can create surveys and view the survey results.

- A web app meeting can have multiple organizers. Organizers other than the one who created the survey, can also participate in the survey.

- Only the organizer who creates a survey can save/edit/delete/launch/end their survey. Upon launching the survey, the other organizers can only end the ongoing survey and view results.

- Organizers can create multiple surveys and save them for later use in the meeting.

- When a meeting organizer creates and launches a survey and then gets disconnected from the meeting, the organizer can rejoin the meeting and still perform all the actions on their ongoing/saved surveys.

The following actions can be performed in the ᴑᴑ⃗ **Surveys** window by the meeting organizer(s):

Icon	Description	Who can use?
▷	Launch survey – Launch a saved survey.	Meeting organizer who creates the survey.
▢	End survey – End an ongoing survey.	Any one of the meeting organizers.
🗒	View results – View survey results.	All organizers can view results after survey ends. **Note:** The survey responses are anonymous. Organizers cannot identify the participant's name or the options they have chosen in the survey.
✎	Edit – Edit the questions and options of the survey.	Meeting organizer who creates the survey. **Note:** Survey can be edited only before launching the survey.
🗑	Delete – Delete questions, options, or a survey.	Meeting organizer who creates the survey.

Participants:

Participants can choose to participate or not to participate in the survey. To participate in a survey, select ᴑᴑ⃗ **Surveys** > **Take Survey** and select the required response from the options provided for a question. Select **Submit your response** to submit.

- Participants can only choose from the provided options for a question. Entering free text and selecting multiple options are not supported.
- Participants cannot see what options they have chosen or edit their choices after submitting the survey.
- Participants can take part in the survey anytime until it ends, even if they join/rejoin the meeting after the survey is launched.
- In case of multiple organizers in a meeting, the organizer who creates the survey cannot participate in the survey. However, the other organizers can participate in the survey.
- Apart from signed-in users, guests too can participate in the surveys.

Surveys ✕

Annual Appraisal

Did you submit your annual appraisal?

○ Yes

○ No

Would you prefer to work from home or work in an office?

○ Home

○ Office

○ Hybrid

Submit your response

The ⌷o⌷ Surveys icon is visible to the web app participants, if the `surveyAllowed` API is set to true in Meeting Server. The participants who have `surveyOpsAllowed` API set to true, can create a survey in the meeting and view results. For more information, refer to Cisco Meeting Server API Guide.

4.1.2.1 Important note for Surveys and File Share features

Web app in-meeting features like Surveys and File Share might not work as intended if the certificates are not validated or if the service is not reachable. In such scenarios, web app shows a warning message. The link given in the warning message allows the web app user to validate the certificates.

Note: The certificates need to be validated only when the participant uses new web app features for the first time on a browser.

> ⚠️ **For File Share & Survey**
>
> An issue with connectivity might exist. Please click the [link](#) to accept the certificate, then retry. Please contact your administrator if there are any persistent problems.
>
> [**Retry**]   [**Dismiss**]
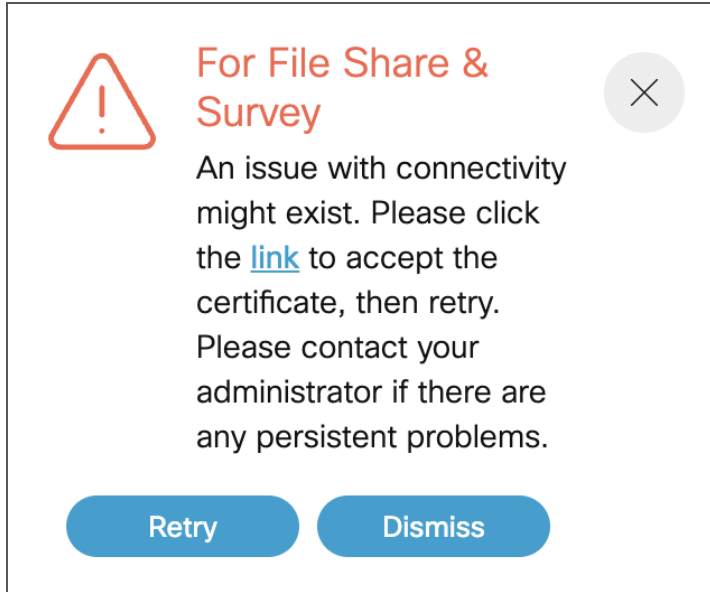
If the above error is displayed during a web app meeting,

1. Click the link given in the pop-up.

2. A new tab will open and displays `{" ping" : " pong!" }` if there is connectivity.

3. Open the web app tab and select **Retry** in the pop-up to get the services back.

Please contact the Meeting Server administrator if the issue persists.

4.1.3 Improved virtual background performance

The virtual background feature enables web app participants to change or blur their background during a meeting. Version 3.8 further improves virtual background/blur performance with the help of a latest upgraded video AI library, which results in faster virtual background/blur application and lesser pixelation on participant's video.

This feature is supported on Google Chrome, Mozilla Firefox, and Microsoft Edge browsers on Windows and macOS devices.

Note:

- Virtual background works best with systems having Graphics Processing Unit (GPU).

- The upgraded library is implemented for web app only. SIP participants can apply images that are locally available in the endpoints.

4.1.4 In-meeting private chat

The chat feature allows web app participants to send messages to other participants in the same meeting. In earlier versions of web app, chat messages were broadcast to all participants in the meeting and not private. From version 3.8, web app participants can choose to send a

chat message to everyone or to a particular participant in the meeting, using **To:** drop-down option in the chat window.
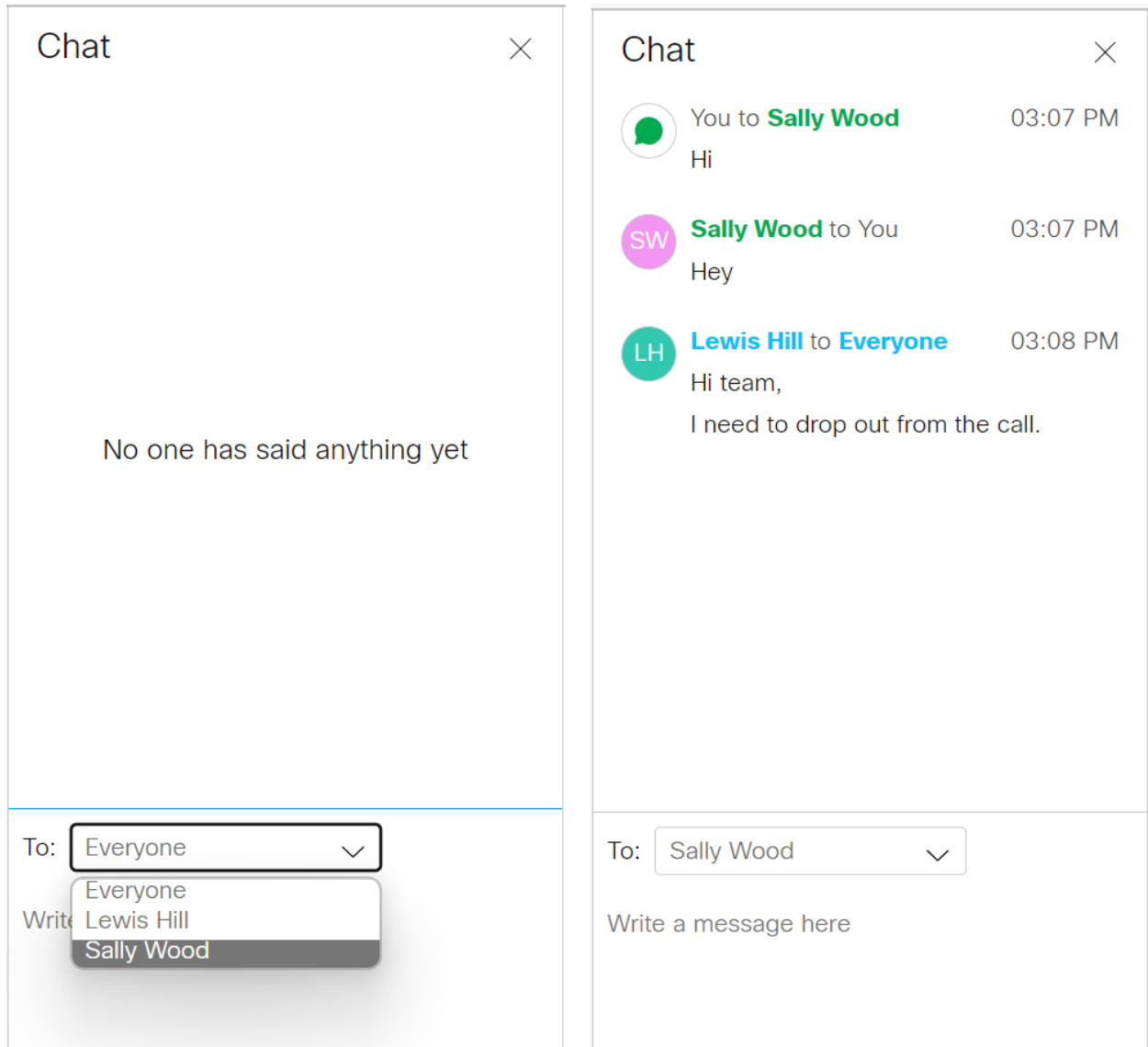
Other participants in the meeting cannot see the private chats which happen between the sender and receiver. Chat messages are only available during the meeting, and not before or later. The chat messages disappear when the participant leaves and rejoins the meeting or refreshes the browser. Administrators can control which calls can have the chat feature enabled and which participants are allowed to send chat messages.

Note: Since this feature is supported only on web app, only web app participants will be listed in the **To:** drop-down list in the chat window.

If the `chatAllowed` API is set to true in `CallProfiles` in Meeting Server, all the web app participants in the meeting can see drop-down option in the chat window. For more information, refer to Meeting Server API Guide.

4.1.5   Support for Czech language

In previous versions, web app was supported in 22 languages. From version 3.8, web app also supports Czech language. Users can now select **Čeština** from the list of languages on the web app.

4.1.6   UI modification

From version 3.8, the video toggle icon that was previously located under the **Settings** option, has been moved beside the mic toggle icon for easy access.
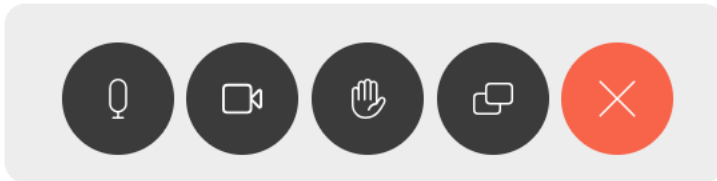
4.1.7   Accessibility improvements

In version 3.8, web app supports the following accessibility improvements:

- Users can now use up or down arrow keys in the keyboard to navigate through any lists like spaces, participants, and in-meeting menu panels.

- Screen reader now announces all the titles, notifications, warnings, and status messages appearing on the screen.

4.2   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.

4.3 Browser versions tested

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

We always recommend using the latest version of browsers.

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

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

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

Browsers	Versions
Google Chrome (Windows, macOS, and Android)	116.0.5845.140
Mozilla Firefox (Windows)	116.0.3
Chromium-based Microsoft Edge (Windows)	116.0.1938.62
Apple Safari for macOS	16.6 (18615.3.12.11.2)
Apple Safari for iOS	16.6

Browsers	Versions
Yandex (Windows)	23.7.3.823

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.

4.3.1   Important note about accessibility settings in Safari browsers

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

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

4.3.2   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.

4.4 Product documentation

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

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

5   Bug search tool, resolved and open issues

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

1. Using a web browser, go to the Bug Search Tool.

2. Sign in with a cisco.com registered username and password.

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

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

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

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

    or,

    in the **Product** field select **Series/Model** and start typing `Cisco Meeting Server`, then in the **Releases** field select **Fixed in these Releases** and type the releases to search for example `3.8`.

2. From the list of bugs that appears, filter the list using the *Modified Date*, *Status*, *Severity*, *Rating* drop down lists.

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

5.1   Resolved issues in Cisco Meeting Server

Issues seen in previous versions that are fixed in 3.8.2.

Cisco identifier	Summary
CSCwk62286	Cisco has evaluated the impact of vulnerability, identified by CVE-2024-6387 in OpenSSH. The product is affected by the vulnerability and hence the OpenSSH version has been upgraded to ciscossh-1.13.48.
CSCwj82289	Meeting Server 2000 crashes while searching for cospace members in webapp and resulting in segmentation fault.

Issues seen in previous versions that are fixed in 3.8.

Cisco identifier	Summary
CSCwd25525	CMS2K TLS syslog trust not working consistently
CSCwd06315	When a WebRTC user shares chrome tab with static content in a distributed call set up with SIP end points, SIP participants can intermittently see gray screen for few seconds and then restored.

5.2   Resolved issues in Cisco Meeting Server web app

The table below lists issues seen in previous versions that are fixed in 3.8.1.

Cisco Identifier	Summary
CSCwh77260	Even if the File Sharing and Surveys features are disabled in the Meeting Server, an error message is displayed during the web app meeting.

The table below lists issues seen in previous versions that are fixed in 3.8

Cisco Identifier	Summary
CSCwf87693	Unable to search or add users to Spaces in Meeting Server 2000 with 240,000 users. **Note:** The user search may take longer when participant's email address is directly pasted in search while scheduling a meeting in web app.
CSCwf43552	In a meeting, when a SIP participant takes over the screen share while a web app participant is still presenting, then theweb app participant cannot see the SIP participant's screen share.
CSCwf02530	Attendee search results will stop working, when **Backspace** button is used on keyboard to delete an incorrect entry while adding attendees using scheduler.

Cisco Identifier	Summary
CSCwe26144	When scheduling a meeting through the web app scheduler, if the participant's role is selected as 'Role 1' (default), the participant cannot join the meeting using **Join** button.
CSCwd56907	Participant gets disconnected from web app meeting when participant selects **Open Email** in **Call information** on Google Chrome and Microsoft Edge browsers.

5.3 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
CSCwf69666	Due to incorrect status sent from IMPS node, Meeting Server updates incorrect presence status intermittently, for users on secondary IMPS node.
CSCwh41791	Failed to access webbridge intermittantly, on CMS 2k
CSCwd89530	If the packet capture is not stopped gracefully using ctrl+C and the terminal is closed abruptly, further packet captures are not possible until CMS reboot.
CSCwb77929	In a deployment with multiple Web Bridge, web app participants can see the Meeting notes only if they are connected to the same webbridge where the notes was saved and published initially.
CSCwa83782	A conference is booked on TMS as Automatic connect type and one of the participants is joining the conference through an unmanaged device. When the conference starts, the participant is called by CMS/TMS, but Meeting Serverdisconnects the call after some time.
CSCvz01886	When a participant's role does not have permissions to share video and presentation, then the role is changed and they have permissions to share video and presentation, the presentation is not visible to other participants when they share content.
CSCvt74033	When content is being shared and an event happens to trigger a Webex Room Panorama to drop from sending two video streams to one, the video frame rate being received by a remote endpoint from the Room Panorama can drop noticeably.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.

5.3.1 Known limitations

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

5.4 Open issues in Cisco Meeting Server web app

Cisco Identifier	Summary
CSCwh48463	When participant enters **"** (double quotation mark) in the survey's title/question/options and selects **Save**, the survey is not created, and then onwards, the participant cannot create any further surveys.
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 still 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 1000 and other virtualized platforms

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

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

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 M5v2	Cisco Meeting Server 1000 M6	Cisco Meeting Server 2000 M5v2	Cisco Meeting Server 2000 M6
Full HD calls 1080p60 video 720p30 content	30	40	218	324
Full HD calls 1080p30 video 1080p30/4K7 content	30	40	218	324

Type of calls	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 1000 M6	Cisco Meeting Server 2000 M5v2	Cisco Meeting Server 2000 M6
Full HD calls 1080p30 video 720p30 content	60	80	437	648
HD calls 720p30 video 720p5 content	120	160	875	1296
SD calls 480p30 video 720p5 content	240	320	1250	1875
Audio calls (G.711)	2200	3000	3000	3200

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

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

Cisco Meeting Server platform		Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 1000 M6	Cisco Meeting Server 2000 M5v2	Cisco Meeting Server 2000 M6
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	60 120 240 2200	80 160 320 3000	437 875 1250 3000	648 1296 1875 3200
	HD participants per conference per server	120		450	
	web app call capa-cities (internal call-ing & external calling on CMS web edge):				
	Full HD HD SD Audio calls	60 120 240 500	80 160 320 500	437 875 1250 1250	648 1296 1875 1875
Meeting Servers in a Call Bridge Group	Call type supported				
	Load limit	120,000		875,000	

Note 1: Maximum of 24 Call Bridge nodes per cluster; cluster designs of 8 or more nodes need to be approved by Cisco, contact Cisco Support for more information.

Note 2: Clustered Cisco Meeting Server 2000's without Call Bridge Groups configured, support integer multiples of maximum calls, for example integer multiples of 700 HD calls.

Note 3: Up to 21,000 HD concurrent calls per cluster (24 nodes x 875 HD calls) applies to SIP or web app calls.

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

Note 5: Table 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.

Note 6: The call setup rate supported for the cluster is up to 40 calls per second for SIP calls and 20 calls per second for Cisco Meeting Server web app calls.

Cisco Meeting Server web app call capacities

This section details call capacities for deployments using Web Bridge 3 and web app for external and mixed calling. (For internal calling capacities, see Table 4.)

Cisco Meeting Server web app call capacities – external calling

Expressway (Large OVA or CE1200) is the recommended solution for deployments with medium web app scale requirements (i.e. 800 calls or less). Expressway (Medium OVA) is the recommended solution for deployments with small web app scale requirements (i.e. 200 calls or less). However, for deployments that need larger web app scale, from version 3.1 we recommend Cisco Meeting Server web edge as the required solution.

For more information on using Cisco Meeting Server web edge solution, see Cisco Meeting Server Deployment Guides.

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

When using Expressway to proxy web app calls, the Expressway will impose maximum calls restrictions to your calls as shown in the table below.

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

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

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

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

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

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

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

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

Appendix B: Apps feature comparison

Table 6:Feature comparison for Cisco Meeting Server web app

Feature	Web app 3.8	Web app 3.7	Web app 3.6	Web app 3.5	Web app 3.4	Web app 3.3	Web app 3.2	Web app 3.1	Web app 3.0
General									
Cisco Meeting Server version	3.8	3.7	3.6	3.5	3.4	3.3	3.2	3.1	3.0
Managing access for members	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
User-level permissions (e.g. can create space)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Support for localization	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Branding	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Online help	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encryption	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Single sign on	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Arabic language support	Yes	Yes	Yes	No	No	No	No	No	No
Czech language support	Yes	No	No	No	No	No	No	No	No
Join using video address (URI)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Schedule a meeting									
View list of scheduled meeting	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Schedule a meeting	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No

Feature	Web app 3.8	Web app 3.7	Web app 3.6	Web app 3.5	Web app 3.4	Web app 3.3	Web app 3.2	Web app 3.1	Web app 3.0
Modify a scheduled meeting	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Delete a scheduled meeting	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Space Management									
Space member roles	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Create / edit space	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Activate newly pro- visioned spaces	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Add / edit / delete space members	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Directory look up for Add Members feature	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View inform- ation for space	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Send invit- ation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audio and video									
Audio	OPUS	OPUS	OPUS	OPUS	OPUS	OPUS	OPUS	OPUS	OPUS
Video	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8
Mic/camera configuration controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Blur your background	Yes	Yes	Yes	Yes	Yes	No	No	No	No

Feature	Web app 3.8	Web app 3.7	Web app 3.6	Web app 3.5	Web app 3.4	Web app 3.3	Web app 3.2	Web app 3.1	Web app 3.0
Virtual background	Yes	Yes	Yes	No	No	No	No	No	No
Far end camera control	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Auto prioritization of audio and video	Yes	Yes	No	No	No	No	No	No	No
Screen share									
Content magnification	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Reset content zoom	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
View screen share	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Desktop sharing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Application sharing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View screen share in a new window	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Re-size the video pane	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Share content audio	Yes	Yes	Yes	Yes	No	No	No	No	No
Optimize for Text (Share screen in 1080p)	Yes	No	No	No	No	No	No	No	No
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	Yes, in meeting only	Yes, in meeting only	No	No

Feature	Web app 3.8	Web app 3.7	Web app 3.6	Web app 3.5	Web app 3.4	Web app 3.3	Web app 3.2	Web app 3.1	Web app 3.0
Chat (Private)	Yes, in meeting only	No	No	No	No	No	No	No	No
In-call									
On-screen messages	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Full-screen view	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layout control	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Name labels	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Recording	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Streaming	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Active speaker label (Beta support)	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Self-view	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pin self-view	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mirror self-view	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Move self-view	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HD/SD selection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pin presentation preview	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Move presentation preview	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Meeting notes	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Closed captioning	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Share files	Yes	Yes	Yes	Yes	No	No	No	No	No

Feature	Web app 3.8	Web app 3.7	Web app 3.6	Web app 3.5	Web app 3.4	Web app 3.3	Web app 3.2	Web app 3.1	Web app 3.0
Network health indicator and media statistics	Yes	Yes	Yes	No	No	No	No	No	No
Content share metrics	Yes	Yes	No	No	No	No	No	No	No
Logo support	Yes	Yes	No	No	No	No	No	No	No
Surveys	Yes	No	No	No	No	No	No	No	No
Participants									
Move participant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Add participant	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP onl y)	Yes (SIP only)	Yes (SIP only)
Remove participants	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Admit participants to a locked meeting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Change a participant's role	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Make participant important	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mute/Unmute other participants' audio and video individually	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mute/Unmute all participants' audio and video	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Feature	Web app 3.8	Web app 3.7	Web app 3.6	Web app 3.5	Web app 3.4	Web app 3.3	Web app 3.2	Web app 3.1	Web app 3.0
Send diagnostics during a meeting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Send invite	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
View call info	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Mic / Camera controls during call	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Raise hand	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
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	Yes	Yes	Yes	Yes

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

Accessibility Notice

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

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

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

You can find more information about accessibility here:

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

Accessibility Support Features

Keyboard navigation

You can use your keyboard to navigate through web app.

- Use **Tab** to navigate between areas in web app. You'll know an area is in focus when it's surrounded by an outline.
  Use **Shift + Tab** to move to the previously focused area.

- Use the **Spacebar** or **Enter** key to select items.

- Use arrow keys to scroll through lists or drop-down menus.

- Use **Esc** to close or dismiss opened screens/menus.

Screen reader support

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

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

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

Cisco Legal Information

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

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

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

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

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

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

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

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

Cisco Trademark

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)