Cisco Meeting Server

Cisco Meeting Server Release 3.5

Release Notes

13 March, 2024

Contents

What's changed

Version	Change
January 12, 2023	Updated Smart Licensing section.
May 3, 2022	Updated Upgrade section.
April 20, 2022	First release for version 3.5.

1 Introduction

This document describes the new features, improvements and changes in version 3.5 of the Cisco Meeting Server software.

The Cisco Meeting Server software can be hosted on:

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

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

Note: Cisco Meeting Management handles the product registration and interaction with your Smart Account for Smart Licensing support. Meeting Management 3.5 is required with Meeting Server 3.5.

- **Upgrade**: The recommended work flow is to first upgrade Meeting Management, complete Smart Licensing, and then upgrade Meeting Server.
- **Smart Licensing**: From the 3.4 release onwards, Smart licensing is mandatory for Meeting Server. The support for traditional licensing has been deprecated 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 .

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

Note about Microsoft RTVideo: Microsoft RTVideo and consequently Lync 2010 on Windows and Lync 2011 on Mac OS, will not be supported going forward. However, support for Skype for Business and Office 365 will continue.

1.1 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 .

Note: Cisco Smart Licensing Cloud Certificates were updated on January 15, 2023. Customers using Direct Mode for licensing between Meeting Management and Smart Licensing Portal must upgrade to version 3.6 and later to continue to use direct mode. If upgrade to version 3.6 is not possible, customers can opt for SLR/PLR mode or on-premise satellite mode. The certificate update will not impact deployments that are using SLR/PLR or on-premise satellite with Meeting Management (3.5 or below).
If Meeting Management is not upgraded in time, Meeting Server will continue to work, but the license enforcement will be initiated. Meeting Management will be on a 90 day grace period, after which non-compliance notifications will be flashed on the participant's screen and audio prompts.

1.2 End of Software Maintenance

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

Cisco Meeting Server software version	End of Software Maintenance notice period
Cisco Meeting Server version 3.2.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.2.x is April 17, 2022.
Cisco Meeting Server version 3.3.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.3.x is August 22, 2022.

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

2 New features and changes in version 3.5

Version 3.5 of the Meeting Server software introduces the following new features and changes:

2.1 Automatic join for blast dial participants

In previous release, a new audio prompt was introduced to guide the participants with DTMF key options to accept or reject the call. From version 3.5, Meeting Management allows the blast dial participants to join the meeting immediately without having to input the DTMF keys. For meetings where participants must join immediately or if the participants cannot respond using the DTMF keys, the Meeting Management administrators can disable the audio prompt. The Meeting Management administrator can turn the audio prompt on or off both at the global level and at the participant level.

If the audio prompt is disabled at the global level, the audio prompt is disabled for all the participants in the blast dial list. Enabling or disabling the audio prompt at global level overrides the setting at the participant level. Administrator can then change the setting for individual participant if needed.

If the audio prompt is disabled, only the prompts **Hello, you are invited to enter the Cisco meeting** and **You are entering to the meeting now** are played. The audio prompt **Press 1 to enter the meeting or * to hang up** will not be played and the participant need not enter any DTMF key. They enter the meeting when they accept the call.

Note: Meeting Management stops redialing when call **Decline** or **End call** is received from remote end. In some cases, if due to network latency, these messages are not propagated to Meeting Server (For example: during PSTN calls), Meeting Management will continue to redial the participant until it reaches the maximum number of retries configured by the administrator. In such scenarios, it is recommended to enable the audio prompt so that the participant can enter the * DTMF key when prompted, to decline the call.

Refer to *CMM Release Notes* for more details.

2.1.1 API additions

A new API parameter **`audioPrompt`** is introduced in 3.5 to turn the audio prompt on or off for a call leg or a participant. It is supported on the following methods:

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

Note: The **`audioPrompt`** parameter cannot be configured on the Webadmin interface. You can use third party tools to configure the parameter.

Parameter	Type/Value	Description
`audioPrompt`	On/Off	• On – Blast dial audio prompt will be played, and user has to enter DTMF key to join the conference. • Off – Blast dial audio prompt will not be played, and user doesn't have to enter any DTMF key to join the conference. This parameter is only supported on POST methods.

Further, GET on **`/api/v1/coSpaces/<coSpace ID>/metadata`** now returns two new fields, **`audioPrompt`** and **`audioPromptGlobal`**.

Parameter	Type/Value	Description
`audioPrompt`	On|Off	This parameter is set at the participant level. • On – Blast dial audio prompt will be played, and user has to enter DTMF key to join the conference. • Off – Blast dial audio prompt will not be played, and user doesn't have to enter any DTMF key to join the conference.

Parameter	Type/Value	Description
audioPromptGlobal	On|Off	This parameter is set at the global level on Meeting Management. • On – The audio prompt is enabled for all the participants in the blast dial list. • Off – The audio prompt is disabled for all the participants in the blast dial list. Enabling or disabling the audio prompt at global level overrides the setting at the participant level.

2.2 Sharing content audio

In a web app meeting when a presenter shares a video, other participants in the meeting could only view the video but could not hear the audio. From version 3.5, web app participant can share both audio and video when they share the screen in the meeting.

The participants can share content audio only on the latest Chromium-based browsers like Chrome, Edge, and Yandex.

On a Windows system, while sharing the entire screen you can select **Share System audio** to share the content audio along with the video. While share only the browser tab, you can select **Share tab audio** to share the audio of the video played on the browser tab. This option is selected by default. Uncheck the option if you do not want to share the browser tab audio.

On a Macintosh system, the participants can only share the browser tab audio. While sharing the browser tab, select the **Share tab audio** to share the audio of the video played on the browser tab. The participants cannot share the audio when they are sharing the entire screen. System audio share is blocked by the Operating System.

When the participant shares the screen,  icon is shown on presentation preview and  icon is displayed besides the presenter's name on participants list.

Note: If the audio output of the system is muted, the participants in the meeting will not be able to hear the audio of the shared content.

The audio of the presentation can be muted when a participant in the meeting mutes the presenter's microphone. The table lists the scenarios with their audio and video behavior during a screen share.

Presenter	Other participants in the meeting	Can participants hear?	
		Presenter's mic	Audio of the shared content
Unmuted	Joined with audio and video	Yes	Yes
Locally muted / No microphone	Joined with audio and video	No	Yes
Muted by other participant in the meeting	Joined with audio and video	No	No
Joined with presentation only	Joined with audio and video	No	Yes
Joined with presentation only and muted by other participant in the meeting	Joined with audio and video	No	No

Note: When a web app participant remotely mutes the presenter, both presenter's mic and presentation audio are muted. If participant unmutes the presenter, only presentation audio is unmuted. Presenter must unmute manually to share their microphone's audio.

2.3 Taking snapshots of participants in a meeting

In a managed meeting, a video operator can now take snapshots of the participant's video and/or snapshot of the meeting video i.e., video of all the participants that is displayed on the participant's screen.

The snapshots aid in monitoring the overall meeting experience or for any diagnostic purpose such as to check the layout being displayed at the participant end or to check the participant video quality.

Note: Due to security and privacy considerations, snapshot of content being shared in the meeting are not captured.

Snapshot is a licensed feature and is supported on Smart based Specific License Reservation (SLR) and online licensing mode. It is activated only when a separate license is purchased. The license is a cluster wide license thus supporting the snapshot feature on any call bridge in that cluster. The status of the snapshot license along with its expiry can be retrieved using the existing API object `/clusterLicensing`.

Note: In version 3.5, the snapshot feature is not implemented on the Permanent License Reservation (PLR) mode.

This feature is also supported in Meeting Management 3.5. Refer to *CMM Release Notes* for more information.

2.3.1 API additions

A new API, **`callLegs/<call leg id>/snapshot`** is introduced on GET method to take the snapshots. This option is available at participant level. It supports the following two optional parameters:

Parameter	Type/Value	Description
`Direction (optional)`	String	It accepts RX or TX • RX/incoming - Participant to CMS • TX/outgoing - CMS to participant If not specified, it defaults to RX/incoming.
`maxWidth (optional)`	Numeric	The maximum resolution of snapshot supported is 720 pixel. This API accepts maxwidth value. Therefore, to achieve a maximum resolution of 720P for the snapshot, this parameter has to be set to 1280. Although it accepts other values too, Meeting Server responds the snapshot with maximum resolution of 720 pixel. **Note:** The maximum resolution of the snapshot image is 720p (1280*720 pixel) If maxwidth value is not specified, Meeting Server responds to the snapshot with default resolution of 96p.

Note: The Snapshot API cannot be accessed using the Meeting Server web admin interface or API explorer.

Additionally, the API object **`/clusterLicensing`** is modified to include a new field **`snapshot`** to retrieve license information for this feature. A GET method performed on **`/clusterLicensing`** gives the following information for the snapshot feature:

Response elements	Type/Value	Description/Notes
`features`		If licensing is enabled then the <features> element includes the elements below.

<table>
<tr><th>Response elements</th><th>Type/Value</th><th>Description/Notes</th></tr>
<tr><td></td><td colspan="2">
<table>
<tr><th>Name</th><th>Type/Value</th><th>Description</th></tr>
<tr><td>snapshot</td><td colspan="2">
<table>
<tr><th>Name</th><th>Type/Value</th><th>Description</th></tr>
<tr><td>status</td><td>noLicense| activated| expired</td><td>noLicense - no license is available for this feature.
activated - the feature is licensed and within its expiry date.
expired - the license for this feature is past its expiry date.</td></tr>
<tr><td>expiry</td><td>String</td><td>Date of expiry</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

2.4 Cisco Meeting Server Scheduler

2.4.1 Support for Scheduler on Cisco Meeting Server 2000

In version 3.4, Scheduler component was released as a fully supported feature on Meeting Server 1000 and Virtualized deployments. Version 3.5 introduces the support for Scheduler on Meeting Server 2000. It is now supported on Meeting Server 1000, Meeting Server 2000 and Meeting Server on Virtualized deployments. It is included in the base multiparty licensing (PMP Plus and SMP Plus) and does not require a separate feature license.

The MMP commands and API nodes added for Scheduler on Meeting Server 1000 and virtualized deployments are now supported on Meeting Server 2000 deployments. Refer to *Meeting Server 3.5 API Reference Guide* and *Meeting Server 3.5 MMP Command Line Reference Guide* for more details.

For information on deploying Scheduler, see *Meeting Server 3.5 Deployment Guide*.

For information about configuration of the email server and types of email configuration, see *Meeting Server 3.5 Installation Guide*.

2.4.2 Send appropriate Scheduler error messages

In previous releases, Scheduler sent a generic error message " Failed to create scheduled meeting." or "Meeting creation failed. Check form fields and try again." for all the error scenarios. From version 3.5, Scheduler has been modified to recognize the scenario and send appropriate error messages. For example, if a user attempts to create a meeting in already scheduled time in the same cospace, Scheduler would recognize the scenario and send " This meeting overlaps with an existing meeting" error message to the client.

2.4.3 Scheduler email queue enhancement

In version 3.5, Scheduler application has been enhanced to handle the failed email retries within a definite time interval. The Scheduler email queue cleaner has been introduced to clean up queued emails after specific expiry time.

2.5 Audit logs for web app user actions

In version 3.5, Meeting Server logs include the audit logs for the user actions. These actions include logging in or out, join or leave a meeting, create a space, muting or unmuting the microphone, turning on or off video, drop another participant from the meeting and so on.

2.6 Limiting concurrent web sessions

Version 3.5 introduces the option to configure the maximum number of concurrent web session requests on a Web Bridge. The existing **`/webBridgeProfiles`** API that contains various Web Bridge configuration options is enhanced to accept new parameter to set the maximum number of concurrent sessions allowed per user.

2.6.1 API additions

A new API parameter **`sessionLimit`** is introduced to configure the maximum number of web session requests per user. It is supported on the following methods:

- POST to **`/webBridgeProfiles`**
- PUT on individual profiles with **`/webBridgeProfiles/<web bridge profile id>`**
- GET on**`/webBridgeProfiles/<web bridge profile id>`**

Parameter	Type/Value	Description
`sessionLimit`	Numeric	Maximum number of web sessions allowed per user, ranging from 0 to 5. If not specified, it defaults to zero indicating that there is no session control.

2.7 Rendering bi-directional languages in participant label names

Version 3.5 introduces the support for rendering participant label names in bidirectional languages such as Arabic and Hebrew. In a meeting with participants joining from web app or SIP end points, the participant label names appearing under the participant video pane are now rendered and displayed correctly.

2.8 Sharing files in a meeting (Beta support)

From version 3.5, web app participants will be able to share files in the meeting. This feature is enabled at the call level. With this feature:

- If file sharing is allowed for the meeting, only a signed-in web app user can download the files.
- Only a signed-in web app user with appropriate permissions can share files in a meeting.
- The shared file is available for download only during the meeting. Participants joining after a meeting has started can only view or download the files that are shared after they joined the meeting.
- File sharing supports a maximum of 5 files with a size limit of 10MB at a time.
- Participants can share all types of files except for the following file extensions:

  .exe, .bat, .bin, .com, .cmd, .inf, .ipa, .osx, .pif, .run, .wsh, .pkg, .dmg, .apk, .sh, .html, .asp, .js, .vbs, .wsf, .php, .scpt

---

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.

Note:

- File share feature is not supported for web app participants joining as guest or participants joining through SIP endpoints, Lync, or Skype.
- Once a file is shared, it cannot be deleted by the participants in the meeting.

Refer to *Cisco Meeting Server web app Important Information* document for details on using File sharing feature in a meeting.

A new service called MeetingApps has been implemented to support file sharing. The MeetingApps must be configured on a stand alone Meeting Server node without any other services. Depending on whether the participants are joining from an external or an internal network, MeetingApps can be configured on DMZ network or on internal network accordingly.

We recommend you to configure MeetingApps on a stand alone Meeting Server in a split-server deployment.

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 file sharing in meetings with web app participants joining from internal and external network, MeetingApps must be deployed on DMZ network. The MeetingApps must be

assigned a publicly accessible IP address and the firewall ports must opened on DMZ for public access.

If file sharing is restricted only for participants joining a web app meeting internally, the MeetingApps can be deployed anywhere in the data center.

The MeetingApps can be configured on a Meeting Server 1000 or on VM deployments of Meeting Server using the MMP command **`meetingapps`**.

Note: MeetingApps services cannot be configured on a Meeting Server 2000. However, you can use Meeting server 2000 as a Call Bridge or Web Bridge along with MeetingApps on Meeting Server 1000 or Meeting Server on VM deployments.

File store capacity on MeetingApps is approximately 20 GB at a given point of time. Participants in the meeting will not be able to share the files if the file store capacity is exhausted within a period of 12 hours from the time the first file was shared. The files are deleted by an internal task that runs every 12 hours.

Web Bridges in your environment must be configured to talk to MeetingApps in order to upload or download the files shared in the meeting. The MeetingApps host name, port number and the secret key generated must be provided to configure the web bridge using the MMP command **`webbridge3 meetingapps add`**

For information on configuring MeetingApps refer to Cisco Meeting Server 3.5 Single Split Server Deployment Guide.

2.8.1 API additions

A new API parameter **`fileReceiveAllowed`** has been introduced to enable or disable the file share at the call level. It is supported on the following methods:

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

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

Additionally, the new parameter **fileUploadAllowed** is added to allow a participant to share files in a meeting. It is supported on the following methods:

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

Parameter	Type/Value	Description
fileUploadAllowed	String	• true – Indicates that the participant can share files in the call. • false – Indicates that the participant cannot share files in the call. The usual rules for the hierarchy of calls and call profiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to false.

2.8.2 MMP Additions

The MeetingApps and Web Bridge configuration details are provided using the new MMP commands listed below:

Command / Examples	Description
meetingapps	Displays the configured parameters of MeetingApps.

Command / Examples	Description
meetingapps https listen <interface> <port>	Configures the interface and port for the MeetingApps to listen on.
meetingapps https listen none	Removes the interface and port configuration for the MeetingApps.
meetingapps gen-secret	Generates the key that will be used to authenticate the Web Bridge and MeetingApps connection.
meetingapps https certs <key-file> <crt-fullchain-file>	Configures the HTTPS certificates for the MeetingApps. It is recommended to use publicly trusted HTTPS certificate signed by a valid certification authority (CA).
meetingapps https certs none	Removes HTTPS certificate configuration.
meetingapps (enable|disable)	Enables or disables the MeetingApps.
meetingapps restart	Restarts the MeetingApps services.
meetingapps status	Displays the status of MeetingApps. For example, Running, Starting.
webbridge3 meetingapps add <hostname> <port> <secretkey>	Configures the MeetingApps hostname, port number, and the secret key generated using the **meetingapps gensecret** command.
webbridge3 meetingapps add none	Clears the MeetingApps configured on the Web Bridge.

2.9 Blur your background (Beta Support)

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

Note:

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

- For Windows systems: Memory - 16 GB and CPU - 1.60 GHz
- For Mac systems: Memory - 16 GB and CPU - 2.30 GHz

2.9.1 API Additions

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

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

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

For more information on APIs, see *Meeting Server 3.5 API Reference Guide*.

Note:

- Cisco does not guarantee that a beta feature will become a fully supported feature in the future. Beta features are subject to change based on feedback, and functionality may change or be removed in the future.
- Background blur feature was introduced in 3.4, and no changes in functionality since last release.

2.10 Security enhancements

Version 3.5 introduces the following security enhancements:

2.10.1 Validating server identity on the database cluster

In a database cluster deployment, Meeting Server validates the nodes by checking the certificate chain up to the root certificate. However, identity of the Meeting Server that was added to the cluster was not validated.

Version 3.5 introduces the option to validate the server identity (hostname/IP address) along with the other validations, thus providing improved security and confidentiality. A new MMP command **`database cluster verifymode <full/ca>`** is added to set the preference for the validations accordingly.

If the verify mode is set to **`full`**, Meeting Server along with other validations, verifies if the server identity matches with the name stored in the server certificates. While if the verify mode is set to **`ca`**, Meeting Server validates the node from the certificate chain up to the root certificate without validating the server identity.

Note: The verify mode must be set to the same value(full/ca) on all the nodes in a cluster.

This is an optional command. If the command is not used, Meeting Server will validate only the Certificate Authority.

Note: The verify mode can be modified only on unclustered database. If you have already set up a database cluster, you must run the **`database cluster remove`** command on every node in the cluster and then set the preference for the verify mode.

For a successful validation of server identity:

1. The server's name must match an exact FQDN on its corresponding server certificate.
2. If your deployment does not have a DNS record, a DNS RR record must be created to resolve the hostname locally.
3. While adding the replica database nodes to the cluster:
    a. If the replica database nodes are added using the hostname, then the hostname must be added in the CN or SAN list of the Meeting Server database server certificate.
    b. If the replica database nodes are added using the IP address, then the IP address must be added in the SAN list of the Meeting Server database server certificate.
    c. All the replica databases in a cluster must be added using the same joining method: hostname or the IP address.
4. If the IP address is used in the server certificate, then, while generating the SAN for the certificate, the IP address must be added as DNS name in SAN along with the IP address field.

    For example:

`pki csr dbserver CN:server.db.example.com subjectAltName:10.1.1.1`

The above command will generate the following SAN entries in the certificate signing request:

`IP Address: 10.1.1.1, DNS:10.1.1.1, DNS:server.db.example.com`

5. The hostname of all the nodes in the cluster must match the IP address in the server certificate.

Note: From version 3.5, before upgrading your meeting servers, uncluster all the nodes using the **`database cluster remove`** command. Users must uncluster the nodes, upgrade the Meeting Server software and cluster the nodes back using the MMP commands. See Scalable and Resilient guide for steps on clustering databases.

2.10.1.1 MMP additions

Command / Examples	Description
`database cluster verifymode <full/ca>`	Configures the database validation mode. **`full`** - Meeting Server along with other validations, verifies if the server identity matches with the name stored in the server certificates. **`ca`** - Meeting Server validates the nodes from the certificate chain upto the root certificate without validating the server identity. If not specified, the verify mode defaults to **`ca`**.

2.10.2 Validating branding server certificates

From version 3.5, If branding server hosted over HTTPS, Meeting Server and branding server certificates must be signed by valid or same CA. If the branding server certificates are signed by valid CA, Meeting Server may fail to communicate with the branding server.

2.11 Summary of API additions and changes

API functionality for Meeting Server 3.5 includes the following new and modified API parameters.

New API parameter to allow the blast dial participants to join the meeting immediately without having to input the DTMF keys

- **`audioPrompt`** is introduced on
  - POST to **`/calls/<call id>/participants`**
  - POST to **`/calls/<call id>/callLegs`**

- GET on **/api/v1/coSpaces/<coSpace ID>/metadata** now returns two new fields, **audioPrompt** and **audioPromptGlobal**.

New API parameter to configure the maximum number of web session requests per user and per browser

- **sessionLimit** is introduced on
  - POST to **/webBridgeProfiles**
  - PUT on individual profiles with **/webBridgeProfiles/<web bridge profile id>**
  - GET on**/webBridgeProfiles/<web bridge profile id>**

New API parameters to support file sharing feature

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

Modification to API objects and parameters

- GET on **/api/v1/coSpaces/<coSpace ID>/metadata** now returns two new fields, **audioPrompt** and **audioPromptGlobal**

New API objects

A new API, GET on **callLegs/<call leg id>/snapshot** is introduced to take the snapshots of the participant's video and/ or snapshot of the meeting video.

A new API parameter **sessionLimit** is introduced to configure the maximum number of web session requests per user per browser. It is supported on the following methods:

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

Parameter	Type/Value	Description
sessionLimit	Numeric	Maximum number of web sessions allowed per user, ranging from 0 to 5. If not specified, it defaults to zero indicating that there is no session control.

A new API parameter **fileReceiveAllowed** has been introduced to enable or disable the file share at the call level. It is supported on the following methods:

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

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

Additionally, the new parameter **fileUploadAllowed** is added to allow a participant to share files in a meeting. It is supported on the following methods:

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

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

Parameter	Type/Value	Description
fileUploadAllowed	true|false	• true – Indicates that the participant can share files in the call. • false – Indicates that the participant cannot share files in the call. The usual rules for the hierarchy of calls and call profiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to false.

2.12 Summary of MMP additions and changes

Version 3.5 supports the MMP additions described in this section.

Sharing files in a meeting

The MeetingApps and Web Bridge configuration details are provided using the new MMP commands listed below:

Command / Examples	Description
meetingapps	Displays the configured parameters of MeetingApps.
meetingapps https listen <interface> <port>	Configures the interface and port for the MeetingApps to listen on.
meetingapps https listen none	Removes the interface and port configuration for the MeetingApps.
meetingapps gen-secret	Generates the key that will be used to authenticate the Web Bridge and MeetingApps connection.
meetingapps https certs <key-file> <crt-fullchain-file>	Configures the HTTPS certificates for the MeetingApps. It is recommended to use publicly trusted HTTPS certificate signed by a valid certification authority (CA).
meetingapps https certs none	Removes HTTPS certificate configuration.
meetingapps (enable|disable)	Enables or disables the MeetingApps.
meetingapps restart	Restarts the MeetingApps services.
meetingapps status	Displays the status of MeetingApps. For example, Running, Starting.

Command / Examples	Description
webbridge3 meetingapps add <hostname> <port> <secretkey>	Configures the MeetingApps hostname, port number, and the secret key generated using the **meetingapps gensecret** command.
webbridge3 meetingapps add none	Clears the MeetingApps configured on the Web Bridge.

Security enhancement - Validating server identity on the database cluster

The following command is added to configure Meeting Server to validate the server identity (hostname/IP address) of the nodes in a database cluster.

Command / Examples	Description
database cluster veri-fymode <full/ca>	Configures the database validation mode. **full** - Meeting Server along with other validations, verifies if the server identity matches with the name stored in the server certificates. **ca** - Meeting Server validates the nodes from the certificate chain upto the root certificate without validating the server identity. If not specified, the verify mode defaults to **ca**.

2.13 Summary of Event Changes

In version 3.5, a new parameter **canMoveToLobby** has been added in the **callRoster** event resource. The **canMoveToLobby** parameter indicates whether or not the participant can be moved to lobby during the meeting.

2.14 Summary of CDR Changes

In version 3.5, a new field **reasonDetails** is added to **callLegEnd** Call Detail Record of Meeting Server.

Name	Type	Description
reasonDetails	String	If the call leg ended due to a remote teardown, the parameter indicates whether the call was a WebRTC call or a SIP call.

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 3.5

This section assumes that you are upgrading from Cisco Meeting Server software version 3.4. If you are upgrading from an earlier version, then you must first upgrade to 3.4 following the instructions in the 3.4 release notes, before following any instructions in this Cisco Meeting Server 3.5 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 3.4.

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 3.5

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.

Note:
Meeting Server 3.0 introduced a mandatory requirement to have Cisco Meeting Management 3.0 (or later). Meeting Management handles the product registration and interaction with your Smart Account (if set up) for Smart Licensing support.

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

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

   Cisco_Meeting_Server_3_5_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:
   4ffb34fd59d9bcd124dc79e0181bee5ca6815b1b9486201789f321d993c61509

   Cisco_Meeting_Server_3_5_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:
   51f9999c85f339f8fc49acd5a0a0266916c4df55985d260be1b721d56ae0f555

   Cisco_Meeting_Server_3_5.ova

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

   For vSphere6, hash (SHA-512) for Cisco_Meeting_Server_3_5_vSphere-6_0.ova:
   f1b62dcad04475402a77a6dd1045d3bb0fc4890abff278b07eb01d79ad4004a54885d461afd5227df54e378eca0f1b0a56236bea02a5d612c495f89a9b66f261

   For vSphere6.5 and higher, hash (SHA-512) for Cisco_Meeting_Server_3_5_vSphere-6_5.ova:
   848bbe24ae9bc113349d258c382faf069e7fb5ef6b5c09b02b1c9ac8477af6fc7176f5b9b1cdedc2bfbf3ff18e51d6449544758bd5678108b70e5840e39a5f42

2. To validate the OVA file, the checksum for the 3.5 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.

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.

4 Bug search tool, resolved and open issues

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

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

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

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

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

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

   or,

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

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

4.1 Resolved issues

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

Issues seen in previous versions that are fixed in 3.5.

Cisco identifier	Summary
CSCwb09031	The scheduler can intermittently fail to send out the invite to participants if remote branding server is used to send customized email templates.
CSCwb43662	The spring framework version of Spring boot has been upgraded to 5.2.20.

4.2 Open issues

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

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

Cisco identifier	Summary
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.
CSCwb60392	In a coSpace meeting, if a participant sharing his screen is moved to lobby, they continue to share content in the meeting.
CSCwa40239	When the Email invites are sent using the Scheduler, all the email address in the participant list must be valid. Scheduler might not send emails to any of the participants from the list, even if one of the email address is invalid.
CSCvz01886	When a participant's role does not have permissions to share video and presentation, then the role is changed and they have permissions to share video and presentation, the presentation is not visible to other participants when they share content.
CSCvw61547	On very rare occasions, calls through a Meeting Server TURN component may fail to connect or may lack a media channel. An error similar to " TURN 437 allocation mismatch in state RefreshTurnAllocationPending" will be seen in the Call Bridge syslog.
CSCvt74033	When content is being shared and an event happens to trigger a Webex Room Panorama to drop from sending two video streams to one, the video frame rate being received by a remote endpoint from the Room Panorama can drop noticeably.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.

4.2.1 Known limitations

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

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.

A.1 Cisco Meeting Server 1000 and other virtualized platforms

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

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

A.2 Cisco Meeting Server 2000

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

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

A.3 Call capacities

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

Table 2: Call capacities across Meeting Server platforms

Type of calls	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000 M5v2
Full HD calls 1080p60 video 720p30 content	30	218
Full HD calls 1080p30 video 1080p30/4K7 content	30	218
Full HD calls 1080p30 video 720p30 content	60	437

Type of calls	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000 M5v2
HD calls 720p30 video 720p5 content	120	875
SD calls 480p30 video 720p5 content	240	1250
Audio calls (G.711)	2200	3000

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

Cisco Meeting Server platform		Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000 M5v2
Individual Meeting Servers or Meeting Servers in a cluster (notes 1, 2, 3, and 4) and Meeting Servers in a Call Bridge Group	1080p30 720p30 SD Audio calls	60 120 240 2200	437 875 1250 3000
	HD participants per conference per server	120	450
	web app call capacities (internal calling & external calling on CMS web edge): Full HD HD SD Audio calls	 60 120 240 500	 437 875 1250 1250
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 3 assumes call rates up to 2.5 Mbps-720p5 content for video calls and G.711 for audio calls. Other codecs and higher content resolution/framerate will reduce capacity. When meetings span multiple call bridges, distribution links are automatically created and also count against a server's call count and capacity. Load limit numbers are for H.264 only.

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

A.4 Cisco Meeting Server web app call capacities

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

A.5 Cisco Meeting Server web app call capacities – external calling

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

For more information on using Cisco Meeting Server web edge solution, see Cisco Meeting Server 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 X12.6 or later, earlier Expressway versions are not supported by Web Bridge 3.

Table 4: Cisco Meeting Server web app call capacities – using Expressway for external calling

Setup	Call Type	CE1200 Platform	Large OVA Expressway	Medium OVA Expressway
Per Cisco Expressway (X12.6 or later)	Full HD	150	150	50
	Other	200	200	50

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

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

A.6 Cisco Meeting Server web app capacities – mixed (internal + external) calling

Both standalone and clustered deployments can support combined internal and external call usage. When supporting a mix of internal and external participants the total web app capacity will follow Table 3 for Internal Calls and if using Cisco Meeting Server web edge solution for external calling. However, if using Expressway at the edge, the number of participants within the total that can connect from external is still bound by the limits in Table 4.

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

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

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