Cisco Meeting Server and web app

Release 3.10

Release Notes

29 November, 2024

Contents

What's changed 4

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

2 What's new in Cisco Meeting Server 8
- 2.1 API enhancements to set pane placement per participant 8
- 2.2 Sharing content in AV1 (1080p) 11
- 2.3 Support for ESXi 8.0 11
- 2.4 Audio notifications in web app 11
- 2.5 Support for TLS 1.3 12
- 2.6 Support to display participant name in Hindi language 12
- 2.7 Summary of API additions and changes 12
- 2.8 Related user documentation 13

3 What's new in Cisco Meeting Server web app 14
- 3.1 Restrict access of non-members to space 14
  - 3.1.1 Known limitations 14
- 3.2 In-meeting audio notifications 15
- 3.3 Notification on cookies usage 15
- 3.4 Accessibility improvements 15
- 3.5 Browser versions tested 16

Important note for users using iOS 13 or later and macOS 10.15 or later 17

Important note about screen sharing on Chrome on macOS 10.15 or later 17
- 3.5.1 Important note about accessibility settings in Safari browsers 17
- 3.5.2 Important note about group policy settings in Microsoft Edge 17

- 3.6 Product documentation 18

4 Upgrading, downgrading and deploying Cisco Meeting Server software version 3.10 19
- 4.1 Upgrading to Release 3.10 19
- 4.2 Downgrading 21
- 4.3 Cisco Meeting Server Deployments 22
  - 4.3.1 Points to note 23

5 Bug search tool, resolved and open issues 24
5.1 Resolved issues in Cisco Meeting Server 25
5.2 Open issues in Cisco Meeting Server 25
5.2.1 Known limitations 26
5.3 Resolved issues in Cisco Meeting Server web app 26
6.1 Open issues in Cisco Meeting Server web app 27

Appendix A: Meeting Server platform maintenance 28
Cisco Meeting Server 1000 and other virtualized platforms 28
Cisco Meeting Server 2000 28
Call capacities 28
Cisco Meeting Server web app call capacities 31
Cisco Meeting Server web app call capacities — external calling 31
Cisco Meeting Server web app capacities – mixed (internal + external) calling 32

Appendix B: Apps feature comparison 33

Accessibility Notice 37

Accessibility Support Features 38

Cisco Legal Information 39

Cisco Trademark 40

What's changed

Version	Change
September 27, 2024	First release for version 3.10

1 Introduction

This document describes the new features, improvements and changes in version 3.10 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 3.10 is required with Meeting Server 3.10.

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

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

1.2 Cisco Meeting Server web app

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

1.2.1 Using the web app

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

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

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

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

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

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

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

1.3 Smart Licensing

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

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

1.4 End of Software Maintenance

On release of Cisco Meeting Server software version 3.10, 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
Meeting Server 3.8	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.8.x is March, 2025

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

2 What's new in Cisco Meeting Server

This section of the document lists the following new features and changes implemented in Meeting Server 3.10:

- API enhancements to set pane placement per participant
- Sharing content in AV1 (1080p)
- Audio notifications in web app
- Support for ESXi 8.0
- Support for TLS 1.3
- Support to display participant name in Hindi language

2.1 API enhancements to set pane placement per participant

From version 3.10, Meeting Server supports creating and applying different pane placement arrangements at the participant level. The Administrators can create different pane placement layouts for every participant. This feature is implemented by adding API enhancements to the participant related methods and is supported on SIP endpoints and Web app.

The participant related method is modified to accept a new parameter, **`importanceData`**, that accepts JSON content format comprising **`highestImportance`** and **`importanceData`**, which is a list of JSON entries with participant guid and importance. The JSON file can take up to 25 entries.

For example,

POST/GET /DELETE to **`http://localhost:<port>/api/v1/participants/participant ID/importanceData/`**

```
{
 "highestImportance":numeric,
 "importanceData":
[
{
"id":"ID",
"importance":numeric
},
{
"id":"ID",
"importance":numeric
}
]
}
```

Let us consider an example of the following pane placement assignment for all the participants in a meeting.

Figure 1:

Bob	**Sally**
Andy	**Mark**

During the meeting, the Administrator can assign a different pane placement view to a particular participant, for example to Andy.

Mark	**Andy**
Sally	**Bob**

In an allEqualQuarters layout with **`panePlacementHighestImportance`** set to 4 and **`panePlacementSelfPaneMode`** set to **self**:

- pane #1 is reserved for a participant with importance set to 4, Mark
- pane #2 is reserved for a participant with importance set to 3, Andy
- pane #3 is reserved for a participant with importance set to 2, Sally
- pane #4 is reserved for a participant with importance set to 1, Bob

For Andy to view the panes in the above arrangement, the following Meeting Server POST request is sent:

```
POST /participants/<Andy participant ID>/importanceData
Body:
{
"highestImportance":"4",
"importanceData":
[
{ "id": "Mark participant ID", "importance": 4},
{ "id": "Andy participant ID", "importance": 3},
{ "id": "Sally participant ID", "importance": 2},
{ "id": "Bob participant ID", "importance": 1}
```

```
]
}
```

All the other participants, other than Andy, will view the arrangement as indicated in Figure 1.

Note:

- Any Global level settings that have previously been applied, such as active speaker or self pane mode, will be retained when pane placement for a specific participant is applied.
- The participant level configuration overrides the meeting level configuration of the pane placement layout. For details on meeting level configuration see Administrator Quick Reference Guide Screen Layouts, Pane Placement, and Customizable Layouts.

2.1.0.1 API additions

A new parameter **`importanceData`** is introduced on the following Participant Related methods.

- POST **`/participants/<participant ID>/importanceData`**
- GET **`/participants/<participant ID>/importanceData`**
- DELETE **`/participants/<participant ID>/importanceData`**

<table>
<tr><th>Parameter</th><th>Type/ Value</th><th>Description/ Notes</th></tr>
<tr><td>highestIm-portance</td><td>Numeric</td><td>This will take the highest importance value that can be assigned to a particular participant. When highestImportance=n is set, the first n panes are placed with participants who have the importance value assigned to them, ranging from n to 1. Set the minimum value to 0 to disable pane placement for particular participant.</td></tr>
<tr><td>importanceData</td><td>List of JSON</td><td>List of JSON data where one object contains participant guid and importance.
<table>
<tr><th>Parameters</th><th>Type/ Value</th><th>Description/ Notes</th></tr>
<tr><td>id</td><td>ID</td><td>The user Jid (<participant id>) associated with the participant whose pane needs to be updated.</td></tr>
<tr><td>importance</td><td>Numeric</td><td>The importance value assigned to a specific participant.</td></tr>
</table>
Note: The JSON list can have a maximum of 25 entries, as it is the maximum number of panes that a screen can have.</td></tr>
</table>

2.2 Sharing content in AV1 (1080p)

Sharing content in AV1 format was introduced as a beta feature in version 3.9; it supported content sharing (send and receive) in AV1 format for web app participants. From version 3.10, this is a fully supported feature with an added enhancement of content transmission in 1080p resolution and supports content sharing (receive only) in AV1 format..

AV1 support can be enabled or disabled using the MMP command **`callbridge AV1 enable/disable`**. After enabling/disabling using the MMP command, restart the Call Bridge to ensure the change is applied.

AV1 support can be verified using one of the following methods:

- Using the existing **`callbridge`** command to list all the services that are enabled in the server or
- Webadmin displays the following log to indicate AV1 is enabled. **`AV1 Video Codec Enabled for Content: 0/1`**, with 0 indicating disable and 1 indicating enable.

Note:

- AV1 transmission from web app relies on browsers to support encoding. If AV1 support is enabled in the Meeting Server, but the browsers do not support it, content is transmitted in the browser supported codec.
- AV1 transmission has been tested and qualified on Chromium based browsers only. However, it is observed that chrome browsers negotiate AV1 for receiving content but not transmitting in AV1.
- AV1 is currently not supported on Safari and Firefox browsers.

2.3 Support for ESXi 8.0

Version 3.10 introduces support for ESXi version 8.0. Meeting Server and Meeting Management now supports ESXi 7.0 Update 3q and ESXi-8.0U3.

Note: 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.

2.4 Audio notifications in web app

From version 3.10, web app participants will get audio notifications when a participant joins or leaves an ongoing meeting. Previously, only SIP participants received audio notifications when

the **joinToneParticipantThreshold** and **leaveToneParticipantThreshold** parameters in the **callLegProfile** were set to a non-zero number. With this release, configuring these parameters will play audio notifications for both web app and SIP participants. The parameters can take a maximum value of 100. A value of 0 “disables” the feature.

2.5 Support for TLS 1.3

Version 3.10 of Meeting Server now fully supports TLS 1.3. After the upgrade, the default TLS version for Meeting Server will be changed to TLS 1.3.

TLS 1.3 will be negotiated using best efforts over HTTP/SIP interfaces, with a fallback to TLS 1.2 if the remote end does not support it.

Note:

- All components have been upgraded to support TLS 1.3, with the exception of the Scheduler component which does not negotiate TLS 1.3 with webbridge.
- TLS 1.3 supports Cisco Unified Communications Manager with SIP interface, however it has not been validated for Cisco Unified Communications Manager IM & Presence interop scenarios and will be validated in the upcoming releases.
- There have been no changes to the DTLS version. Meeting Server continues to support DTLS 1.2 and below, with 1.2 as the default.
- TLS 1.3 support for cipher configurations have not been validated.
- Meeting Server currently does not support configuring the minimum version to TLS 1.3.
- Support for TLS 1.0 and 1.1 will be removed in the upcoming releases.

2.6 Support to display participant name in Hindi language

In a meeting initiated through Meeting Server, the names of participants entered in Hindi language are rendered accurately in the video pane, participant list, and speaking tab. This feature is supported on web app and SIP endpoints.

2.7 Summary of API additions and changes

API functionality for Meeting Server 3.10 includes the following new API parameters.

A new parameter is introduced on the Participant Related methods.

- **importanceData** is introduced on:
    - POST **/participants/<participant id>**

- GET `/participants/<participant id>`
- DELETE `/participants/<participant id>`

API parameter enhanced to receive audio notifications in web app.

- `joinToneParticipantThreshold` and `leaveToneParticipantThreshold:`
  - POST, PUT and GET methods on `callLegProfile`

2.8 Related user documentation

The following sites contain documents covering installation, planning and deployment, initial configuration, operation of the product, and more:

- Release notes (latest and previous releases): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-release-notes-list.html
- Install guides (including VM installation, Meeting Server 2000, and using Installation Assistant): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-guides-list.html
- Configuration guides (including deployment planning and deployment, certificate guidelines, simplified setup, load balancing white papers, and quick reference guides for admins): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html
- Programming guides (including API, CDR, Events, and MMP reference guides and customization guidelines): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html
- Open source licensing information: https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-licensing-information-listing.html
- Cisco Meeting Server FAQs: https://meeting-infohub.cisco.com/faq/category/25/cisco-meeting-server.html
- Cisco Meeting Server interoperability database: https://tp-tools-web01.cisco.com/interop/d459/s1790

3 What's new in Cisco Meeting Server web app

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

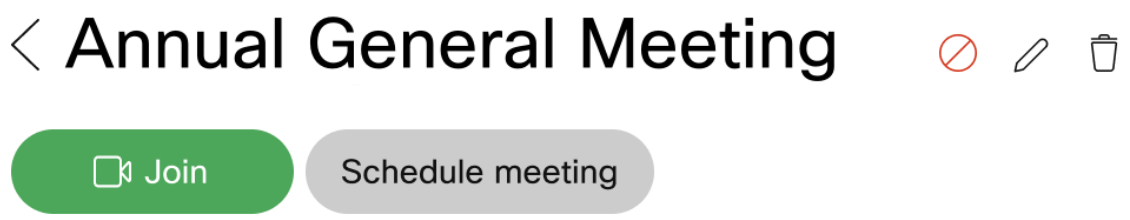
- Restrict access of non-members to space
- In-meeting audio notifications
- Notification on cookies usage
- Accessibility improvements

3.1 Restrict access of non-members to space

From version 3.10, a web app space owner has the option to allow only space members to join a meeting of that space and restrict participants who are not part of the space.

Previously, administrators allowed/restricted non-members' access to meetings by setting the API **`nonMemberAccess`** to True/False in the Meeting Server. With this release, space owners can provide/restrict access on web app as well.

On the web app space information page, a new button ⊘ has been added that, when enabled [⊘], restricts meeting access for non-members.



Note: SIP participants cannot join a meeting that has non-members access restricted.

3.1.1 Known limitations

- When a signed-in space member joins a space meeting and refreshes the web app meeting page, the participant is temporarily redirected to the join meeting page before being automatically reconnected to the meeting.
- All space members can enable/disable 'Restrict Access' button in web app space.
- When **`nonMemberAccess`** is set to **False** in the Meeting Server, the space owner and space

members cannot enter the space meeting using the join links generated in email invite and dial/join information.

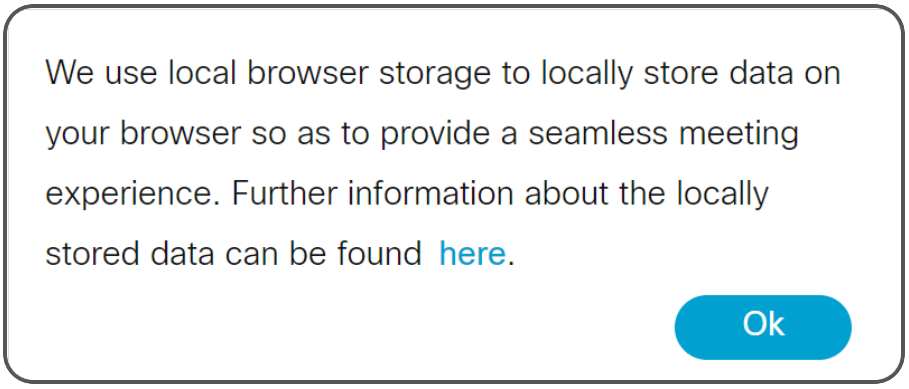
3.2 In-meeting audio notifications

From version 3.10, all participants in a web app meeting will be notified with appropriate audio alerts when a participant joins or leaves an ongoing meeting.

3.3 Notification on cookies usage

Web app saves user settings—also known as cookies—in the browser's cache to improve user experience during meetings. A new pop-up message has been added in web app to notify users about cookie usage and the type of data that is stored, thereby making it compliant with data privacy regulations such as GDPR and CCPA and protecting user privacy.

When a web app participant signs in for the first time, the following notification pop-up is displayed about the cookies usage. The message is displayed for both signed-in and guest participants.



- Click **here** in the pop-up notification to see more information on the type of variables stored in the browser by web app.
- Select **Ok** to accept and dismiss the pop-up.

Note: The pop-up notification is displayed until the participant accepts it by clicking **Ok**. The cookies are stored until the browser cache is cleared by the participant.

3.4 Accessibility improvements

In version 3.10, web app supports the following accessibility improvements:

- When using keyboard to navigate through web app, the shifting of focus now follows a logical order

    - In chat window, chat history, and while dismissing the chat window.
    - In **Join Meeting** page.
    - For **More ways to join** and **Settings** options in **Join Meeting** page.
    - In **Participants** panel in a meeting.
    - In **Add Members** panel in web appspace.
- Use up and down arrow keys on keyboard to navigate chat history and My Spaces.
- Screen reader correctly announces **More ways to join** options as list items, and Meeting Server logo as Cisco Meeting Server Home button.

Accessibility improvements in web app online help:

- Text contrast for hyperlinks.
- Focus visibility when navigating with 'Tab'.
- Headers and captions for tables.
- Alternative text for images and icons.
- Proper header hierarchy level.
- Fixed issues with pop-up images and expand/collapse buttons.

3.5 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)	128.0.6613.120
Mozilla Firefox (Windows)	130.0

Browsers	Versions
Chromium-based Microsoft Edge (Windows)	128.0.2739.67
Apple Safari for macOS	17.6
Apple Safari for iOS	17.6
Yandex (Windows)	24.7.2.1098

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

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

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

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

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

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

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

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

3.5.1 Important note about accessibility settings in Safari browsers

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

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

3.5.2 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.

3.6 Product documentation

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

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

4 Upgrading, downgrading and deploying Cisco Meeting Server software version 3.10

This section assumes that you are upgrading from Cisco Meeting Server software version 3.9. If you are upgrading from an earlier version, then you must first upgrade to 3.9 following the instructions in the 3.9 release notes, before following any instructions in this Cisco Meeting Server 3.10 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 3.9.

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.

4.1 Upgrading to Release 3.10

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 software download pages of the Cisco website:

   Cisco_Meeting_Server_3_10_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:a03c4bf442c5cb029f403afc25c9c83a9a793a2bd2253e2436997f9844ec2b92

   Cisco_Meeting_Server_3_10_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:0b75de6bc4fbd73192874cc90c5807447dbdedbcab38b6ef3e9ad6ef59f31124

   Cisco_Meeting_Server_3_10_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_10_vSphere-7_0.ova:
   808df6e578b6b283c00aed4581dcdf954788e3bd8ebfd03e61407e6a1d843e39331069d4f6595a03da191e96ac41cc10cbc2fabaf573e94234def80f2f5585dd

2. To validate the OVA file, the checksum for the 3.10 release is shown in a pop up box that appears when you hover over the description for the download. In addition, you can check the integrity of the download using the SHA-512 hash value listed above.

   Note: Version 3.10 introduces support for ESXi version 8.0. Meeting Server and Meeting Management now supports ESXi 7.0 and ESXi 8.0 versions. This release supports ESXi 7.0 Update 3q and ESXi-8.0U3.

   ---

3. Using an SFTP client, log into the MMP using its IP address. The login credentials will be the ones set for the MMP admin account. If you are using Windows, we recommend using the WinSCP tool.

   Note: If you are using WinSCP for the file transfer, ensure that the Transfer Settings option is 'binary' not 'text'. Using the incorrect setting results in the transferred file being slightly smaller than the original and this prevents successful upgrade.

   Note:
   a) You can find the IP address of the MMP's interface with the **`iface a`** MMP command.
   b) The SFTP server runs on the standard port 22.

   ---

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

5. To validate the upgrade file, issue the **`upgrade list`** command.
   a. Establish an SSH connection to the MMP and log in.
   b. Output the available upgrade images and their checksums by executing the upgrade list command.

      `upgrade list`
   c. Check that this checksum matches the checksum shown above.
6. To apply the upgrade, use the SSH connection to the MMP from the previous step and initiate the upgrade by executing the **`upgrade`** command.
   a. Initiate the upgrade by executing the upgrade command.
      `upgrade <image_name>.img. For example: upgrade upgrade_spa.img`
   b. The Server/ virtualized server restarts automatically: allow 10 minutes for the process to complete.
7. Verify that Meeting Server is running the upgraded image by re-establishing the SSH connection to the MMP and typing:
   `version`
8. Update the customization archive file when available.
9. You have completed the upgrade.

4.2 Downgrading

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

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.

4.3 Cisco Meeting Server Deployments

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

- single combined Meeting Server – all Meeting Server components (Call Bridge, Web Bridge 3, Database, Recorder, Uploader, Streamer and TURN server) are available, the Call Bridge and Database are automatically enabled but the other components can be individually enabled depending upon the requirements of the deployment. All enabled components reside on a single host server.
- single split Meeting Server – in this model the TURN server, Web Bridge 3, and MeetingApps are enabled on a Meeting Server located at the network edge in the DMZ, while the other components are enabled on another Meeting Server located in the internal (core) network.
- the third model covers deploying multiple Meeting Servers clustered together to provide greater scale and resilience in the deployment.

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

4.3.1 Points to note

4.3.1.1 Cisco Meeting Server 2000

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

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

4.3.1.2 Cisco Meeting Server 1000 and specification-based VM server

- The Cisco Meeting Server 1000 and specification-based VM servers have lower call capacities than the Cisco Meeting Server 2000, but all components (Call Bridge, Web Bridge 3, Database, Recorder, Uploader, Streamer and TURN server) are available on each host server. The Web Bridge 3, Recorder, Uploader, Streamer and TURN server require enabling before they are operational.
- When uploading OVA to Vcenter and deploying, the Publisher field should show (Trusted certificate). If you see a warning for an invalid certificate and not-trusted cert when importing the OVA, see this article: https://kb.vmware.com/s/article/84240. You may have to add the intermediate and root certificates corresponding to the certificate used to sign the OVA, to the VECS Store. To procure intermediate or root certificates or any other issues, contact Cisco Technical Support.

5 Bug search tool, resolved and open issues

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

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

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

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

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

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

   or,

   in the **Product** field select **Series/Model** and start typing `Cisco Meeting Server`, then in the **Releases** field select **Fixed in these Releases** and type the releases to search for example 3.10.
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 3.10.

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 CiscoSSH version has been upgraded from CiscoSSH-1.13.46 to CiscoSSH-1.13.48 which has patch to fix vulnerability on top of OpenSSH9.1p1(without need to upgrade OpenSSH9.1p1) Note: CiscoSSH version used in Meeting Server is based on OpenSSH 9.1p1. Customer vulnerability scan tool will still show OpenSSH9.1p1 used in Cisco Meeting Server as vulnerable, but it is false positive as OpenSSH does not back-port CVE fixes or security patches. However, CiscoSSH team has back-ported CVE patches in CiscoSSH1.13.48.
CSCwi54831	Meeting Server 2000 crashes as a result of incorrectly rendered participant labels.
CSCwi06649	Audit logs are not sent to syslog server after Meeting Server reboot, while TLS is enabled.
CSCwj73763	In a distributed call setup with call bridges having a single signed-in participant, peer link is not re-established, when the participants attempt to rejoin a meeting after getting disconnected due to network drop or a graceful exit.
CSCwh97546	Conferences hosted on Meeting Server with streamer are getting disconnected due to streamer getting spiked or delayed RTP packets.

5.2 Open issues in Cisco Meeting Server

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

Cisco identifier	Summary
CSCwm56132	Active speaker is not updated appropriately on the participant with pane placement per participant setting.
CSCwh41791	Failed to access webbridge intermittantly, on Meeting Server 2000.
CSCwd89530	If the packet capture is not stopped gracefully using Ctrl+C and the terminal is closed abruptly, further packet captures are not possible until CMS reboot.
CSCwb77929	In a deployment with multiple Web Bridge, web app participants can see the Meeting notes only if they are connected to the same webbridge where the notes was saved and published initially.

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.
CSCvz01886	When a participant's role does not have permissions to share video and presentation, then the role is changed and they have permissions to share video and presentation, the presentation is not visible to other participants when they share content.
CSCvt74033	When content is being shared and an event happens to trigger a Webex Room Panorama to drop from sending two video streams to one, the video frame rate being received by a remote endpoint from the Room Panorama can drop noticeably.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.

5.2.1 Known limitations

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

5.3 Resolved issues in Cisco Meeting Server web app

The table below lists issues seen in previous versions that are fixed in 3.10.

Cisco Identifier	Summary
CSCwk47397	When web app presenter auto-reconnects to a meeting after a network issue, the 'Presentation Only' setting is not preserved, and the presenter lacks option to disable their camera. After reconnection, all meeting participants can see and hear the presenter, and vice-versa.
CSCwj08910	When two participants use two separate/different Meeting Servers to join a distributed call, one participant cannot participate in the survey created by the other participant.
CSCwm56138	UI text changes in Survey Results window: Changed **questions:** and **% participated:** to **Total Questions:** and **Participation:** respectively.
CSCwk07254	Web app participants are unable to join meetings using Firefox browser versions 126 and 127.

6.1 Open issues in Cisco Meeting Server web app

Cisco Identifier	Summary
CSCwi05238	Web app briefly shows an error message 'Sign in failed' when participant is logging in.
CSCwh48464	When a web app participant applies virtual background to their video and then refreshes the browser tab, the virtual background appears black on Google Chrome and Mozilla Firefox browsers.
CSCwc76769	In Google Chrome browser, when a participant applies blur to their video and leaves the web app meeting, the camera is still on and does not close.
CSCwa17363	In web app, the participants who are moved to lobby from Meeting Management can see 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 capacities (internal calling & 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	160,000	875,000	1,296,000

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.

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

Appendix B: Apps feature comparison

Table 6:Feature comparison for Cisco Meeting Server web app

Feature	Web app 3.10	Web app 3.9	Web app 3.8	Web app 3.7
General				
Cisco Meeting Server version	3.10	3.9	3.8	3.7
Managing access for members	Yes	Yes	Yes	Yes
User-level permissions (e.g. can create space)	Yes	Yes	Yes	Yes
Support for localization	Yes	Yes	Yes	Yes
Branding	Yes	Yes	Yes	Yes
Online help	Yes	Yes	Yes	Yes
Encryption	Yes	Yes	Yes	Yes
Single sign on	Yes	Yes	Yes	Yes
Arabic language support	Yes	Yes	Yes	Yes
Czech language support	Yes	Yes	Yes	No
Join using video address (URI)	Yes	Yes	Yes	Yes
Notifications				
Audio notification when participant joins/leaves	Yes	No	No	No
Connection resiliency (Auto reconnect in bad network)	Yes	Yes	No	No
Schedule a meeting				
View list of scheduled meeting	Yes	Yes	Yes	Yes
Schedule a meeting	Yes	Yes	Yes	Yes
Modify a scheduled meeting	Yes	Yes	Yes	Yes
Delete a scheduled meeting	Yes	Yes	Yes	Yes

Feature	Web app 3.10	Web app 3.9	Web app 3.8	Web app 3.7
Space Management				
Space member roles	Yes	Yes	Yes	Yes
Restrict access of non-members to space	Yes	No	No	No
Create / edit space	Yes	Yes	Yes	Yes
Activate newly provisioned spaces	Yes	Yes	Yes	Yes
Add / edit / delete space members	Yes	Yes	Yes	Yes
Directory look up for Add Members feature	Yes	Yes	Yes	Yes
View information for space	Yes	Yes	Yes	Yes
Send invitation	Yes	Yes	Yes	Yes
Audio and video				
Audio	OPUS	OPUS	OPUS	OPUS
Video	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8
Mic/camera configuration controls	Yes	Yes	Yes	Yes
Speaker configuration controls	Yes	Yes	No	No
Blur your background	Yes	Yes	Yes	Yes
Virtual background	Yes	Yes	Yes	Yes
Far end camera control	Yes	Yes	Yes	Yes
Auto prioritization of audio and video	Yes	Yes	Yes	Yes
Screen share				
Content magnification	Yes	Yes	Yes	Yes
Reset content zoom	Yes	Yes	Yes	Yes
View screen share	Yes	Yes	Yes	Yes
Desktop sharing	Yes	Yes	Yes	Yes
Application sharing	Yes	Yes	Yes	Yes

Feature	Web app 3.10	Web app 3.9	Web app 3.8	Web app 3.7
View screen share in a new window	Yes	Yes	Yes	Yes
Re-size the video pane	Yes	Yes	Yes	Yes
Share content audio	Yes	Yes	Yes	Yes
Optimize for Text (Share screen in 1080p)	Yes	Yes	Yes	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
Chat (Private)	Yes, in meeting only	Yes, in meeting only	Yes, in meeting only	No
In-call				
On-screen messages	Yes	Yes	Yes	Yes
Full-screen view	Yes	Yes	Yes	Yes
Layout control	Yes	Yes	Yes	Yes
Name labels	Yes	Yes	Yes	Yes
Recording	Yes	Yes	Yes	Yes
Streaming	Yes	Yes	Yes	Yes
Active speaker label (Beta support)	Yes	Yes	Yes	Yes
Self-view	Yes	Yes	Yes	Yes
Pin self-view	Yes	Yes	Yes	Yes
Mirror self-view	Yes	Yes	Yes	Yes
Move self-view	Yes	Yes	Yes	Yes
HD/SD selection	Yes	Yes	Yes	Yes
Pin presentation preview	Yes	Yes	Yes	Yes
Move presentation preview	Yes	Yes	Yes	Yes
Meeting notes	Yes	Yes	Yes	Yes
Closed captioning	Yes	Yes	Yes	Yes
Share files	Yes	Yes	Yes	Yes

Feature	Web app 3.10	Web app 3.9	Web app 3.8	Web app 3.7
Network health indicator and media statistics	Yes	Yes	Yes	Yes
Content share metrics	Yes	Yes	Yes	Yes
Logo support	Yes	Yes	Yes	Yes
Surveys	Yes	Yes	Yes	No
Participants				
Move participant	Yes	Yes	Yes	Yes
Add participant	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)
Remove participants	Yes	Yes	Yes	Yes
Admit participants to a locked meeting	Yes	Yes	Yes	Yes
Change a participant's role	Yes	Yes	Yes	Yes
Make participant important	Yes	Yes	Yes	Yes
Mute/Unmute other participants' audio and video individually	Yes	Yes	Yes	Yes
Mute/Unmute all participants' audio and video	Yes	Yes	Yes	Yes
Send diagnostics during a meeting	Yes	Yes	Yes	Yes
Send invite	Yes	Yes	Yes	Yes
View call info	Yes	Yes	Yes	Yes
Mic / Camera controls during call	Yes	Yes	Yes	Yes
Raise hand	Yes	Yes	Yes	Yes
Move call				
Use this device for screen share and call management only (while another device is used for audio and video)	Yes	Yes	Yes	Yes

Accessibility Notice

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

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

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

You can find more information about accessibility here:

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

Accessibility Support Features

Keyboard navigation

You can use your keyboard to navigate through web app.

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

Screen reader support

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

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

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

Cisco Legal Information

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

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

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

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

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

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

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

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

© 2024 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

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