Cisco Meeting Management

Release 3.9.1

(Build 3.9.0.20)

Release Notes

October 28, 2024

Contents

Document Revision History

Table 1: Document revision history

Date	Description
2024-10-28	3.9.1 Maintenance Release
2024-03-05	Document published

1 Introduction

Cisco Meeting Management is a management tool for Cisco's on-premises video meeting platform, Cisco Meeting Server. You can use the tool to monitor and manage meetings that are running on the platform, and it also provides information about which Cisco licenses you are using.

Meeting Management, with its current feature set, is included within existing Cisco Meeting Server licensing.

These release notes describe new features, improvements, and changes to Cisco Meeting Management.

1.1 The software

Meeting Management is a virtualized appliance. Specifications of the VM (virtual machine) depend on how many simultaneous actions your Meeting Management has to perform or observe. See the *Installation and Configuration Guide* for specifications and requirements, including our estimates on sizing related to the number of Call Bridges you are managing.

For security, there is no user access to configuring via the console after first run. Except for the installation process, all use of Meeting Management is via a browser interface.

1.2 Upgrading from previous version

Before you upgrade:

- Please make sure you have an up-to-date backup of your Meeting Management.

  See the *Installation and Configuration Guide* for instructions.
- Check that your deployment meets the requirements of the version you are upgrading to.
- Plan your upgrade so no important monitored meetings are taking place while you are performing the upgrade.
- Notify other users before you start upgrading.

  Note: All users, both video operators and administrators, will be signed out without warning, and data for ongoing and recent meetings will be lost when you upgrade.

- Make sure that you are ready to upgrade all connected Meeting Servers immediately after you upgrade Meeting Management. To avoid any issues caused by an older version of Meeting Management, we strongly recommend that you first upgrade Meeting Management, then upgrade the connected Meeting Servers.

Upload keys to verify upgrade images:

Cisco Meeting Management embeds a signature within the upgrade image which Meeting Management uses to confirm whether or not the image is genuine.

Image signatures are only verified when upgrading from a signed image. So manual verification is still advised when upgrading from an unsigned image to a signed one. i.e. if you upgrade from 3.6 to 3.7, or downgrade to earlier versions, you are still advised to manually verify the hashes. This feature will be fully effective when upgrading from 3.7 and beyond.

From version 3.7, upgrading to a special build will require uploading a special key. The **Upload Key** button is introduced to enable administrators to upload the public key and verify the upgrade images. However, the administrators will perform this action only when upgrading to a special build.

To upload public keys:

1. On the **Settings** page, go to **Upgrade** tab.
2. Click **Upload key** then browse and select the public key. The selected public key is verified and uploaded.

Note: Upgrades from a signed production/ special build to another signed production build will not require any action from the administrator. Meeting management verifies the upgrade images automatically without the need for manual verification of the hashes.

To upgrade Meeting Management:

1. Sign in to the download area of cisco.com
2. Download the upgrade image file and save it in a convenient location.
3. Sign in to Meeting Management.
4. Go to the **Settings** page, **Upgrade** tab.
5. Click **Upgrade**.
6. Click **Upload upgrade file**.
7. Select the upgrade image file and click **Open**.
8. Check that the checksums are the same as the ones listed below, then **Confirm**.

   If the checksums do not match, do not install the upgrade, as the file may have been corrupted.
9. **Restart** Meeting Management to complete the upgrade.

1.3 Downgrading to previous version

If you need to downgrade to a previous version:

- Use the regular upgrade procedure and choose the image file for the appropriate version as the upgrade file.
- When using Reservation mode(SLR/PLR), ensure that you deregister from the reservation and then downgrade to a previous version. For more information on deregistering license reservation refer to Returning reserved licenses

1.4 Deploying the OVA

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.

1.5 Checksums for upgrade and installation files

Before you install or upgrade Meeting Management you should always check that the files have not been corrupted. See file names and checksums for this release below.

Upgrade image:

- Name of download file: `Cisco_Meeting_Management_3_9_1.zip`
- Name of upgrade image: `Cisco_Meeting_Management_3_9_1.img`
- MD5 checksum for upgrade image: `3af237f5a7eddf8359240ac61213528c`
- SHA256 checksum for upgrade image:
  `c4ddf2d42072200c7359f5aeda728548e27ecb247d094a6223d98d42fa82e5da`
- SHA512 checksum for upgrade image:
  `263f7f60a0a43125d87a46fce5698c5f81defba0f52979a545ec30e11f8d5fad7f8d02d34d93bf19df706d6dbca0dbbcf73200c4c9453d8b89fa5be72d237931`

OVA for new installation on vSphere 7.0:

- File name: `Cisco_Meeting_Management_3_9_1_vSphere-7_0.ova`
- MD5 checksum for image: `5e16f9287f8c75af192ec9246bb364d0`
- SHA256 checksum for image:
  `aae3fb4de87a54a6cc5fbbf96a2783080c6eb20211ad9118231d9e350777872d`
- SHA512 checksum for image:
  `92b8e6c5d309c8570d04cbfeaa7586576fbbf39641f5c575b1004a7ec5ab95a734b0e8dc64fcd0497876315086653b3a0fa0cf0fa5ad10df6842693923f7e84b`

Note: VMware has discontinued support for ESXi 6.x versions and Meeting Management will no longer be tested in any of the 6.x versions. This release of version 3.9.1 supports ESXi 7.0 U3o. Support for ESXi 8.0 will be added in upcoming releases.

1.6 Smart Licensing

From the 3.4 release onwards, Smart licensing is mandatory for Meeting Management. 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 , see Cisco Meeting Management User Guide for Administrators.

1.7 End of software maintenance for earlier versions

We support two full versions of Meeting Management at a time. This means that we give notice of end of maintenance and support for any given release when the subsequent two full versions have been released. For more information, see End of maintenance and support policy for Cisco Meeting Server, Cisco Meeting App and Cisco Meeting Management software.

1.7.1 End of software maintenance

Table 2: Timeline for End of Software Maintenance for versions of Meeting Management

Cisco Meeting Management version	End of Software Maintenance notice period
Cisco Meeting Management version 3.7	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Management version 3.7.x is August, 2024.

1.8 Meeting Management and connected Meeting Servers must run the same software version

Meeting Management and connected Meeting Servers must run the same software version.

Before 3.0, every version of Meeting Management supported the same Meeting Server as well as the two previous ones. From 3.0, each Meeting Management version only supports Meeting Servers running the same version.

Note: To avoid any issues, we strongly recommend that you always upgrade Meeting Management before you upgrade the connected Meeting Servers. We have edited Upgrading from previous version to reflect this change.

2 New features and changes

In this section you can see what is new in 3.9.

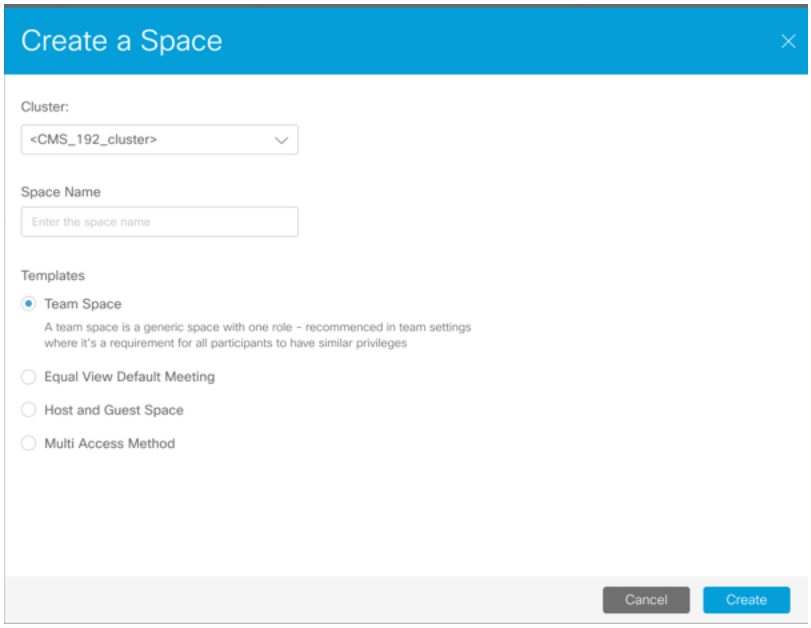
2.1 Create Spaces using Meeting Management

From version 3.9, Meeting Management allows administrators to create meeting spaces. Previously, spaces could be created through web app or using APIs on Meeting Server and Meeting Management only listed them. With this release, administrators can now create and edit spaces through Meeting Management. Space(s) created in Meeting Management will not be visible in web app.

The **Spaces** page is enhanced to include the **Create Spaces** button, that allows administrators to create spaces on Meeting Server clusters.

Follow these steps to create a space in Meeting Management:

1. On the **Spaces** page, click **Create space** button to launch **Create a Space** pop-up window.
2. Select the Meeting Server cluster from the drop-down menu.
3. Enter a unique name for the space in **Space name**, with a maximum character limit of 200.



4. Select appropriate space template from **Templates**. If the templates are not available, it has to be created from the Meeting Server.
5. Click **Create** button.

The created space will be listed in the **Spaces** page. Spaces with ongoing or active meetings will be displayed with  icon. Here, the number on the icon represents the total participants

attending the meeting. Hovering over the icon displays a message, in this case, **Active meeting with 4 participants.**

Administrators can edit or delete only the spaces created in Meeting Management. Spaces created in web app will be in view only mode for Meeting Management administrators.

On selecting a space from the list, administrator can view join information and configure blast dial.

On the meeting space created in Meeting Management, administrators can:

- View, edit, and delete the space(s) created in Meeting Management.
- Obtain join information as email template and share it with the participants.
- Enable or disable blast dial feature.

Space name can be modified using the edit icon. The delete icon available against the space name can be used to delete space. Administrator can also send the join information as email to the participants by copying the join information using icon available against each role.

Note: Meeting Management will display the join link only if the port is configured in the Meeting Server.

To modify the join information used by the members to access the space:

1. Click edit icon to launch **Edit access role** pop-up window.
2. Make necessary changes to **Passcode**, **Visibility** and **Video address**,

   Note:

   - The new passcode entered should be an integer value and must contain a minimum length as defined in the dial-in security profile in space templates.
   - In case the entered video address is already available in Meeting Server, administrator will be prompted to enter a different video address.

3. Click **Save** button.

2.2 Passphrase verifier

Passphrase verifier checks the quality of user password against a reference list/dictionary that contains commonly used words, repetitive or sequential characters such as -aaaaa', -1234abcd', etc. The list will also include context specific words, such as service name, username, product name, and derivatives.

Meeting Management administrators can define and upload a .txt file for the dictionary, using the **Upload dictionary** button available in the **Local configuration** section in **Users** tab. If the user chosen password matches one from the list, the passphrase verifier rejects the password and notifies the user to choose a different value.

If a dictionary is present when backing up Meeting Management, it will be included in the backup file. When the backup file is restored, the dictionary will also be restored.

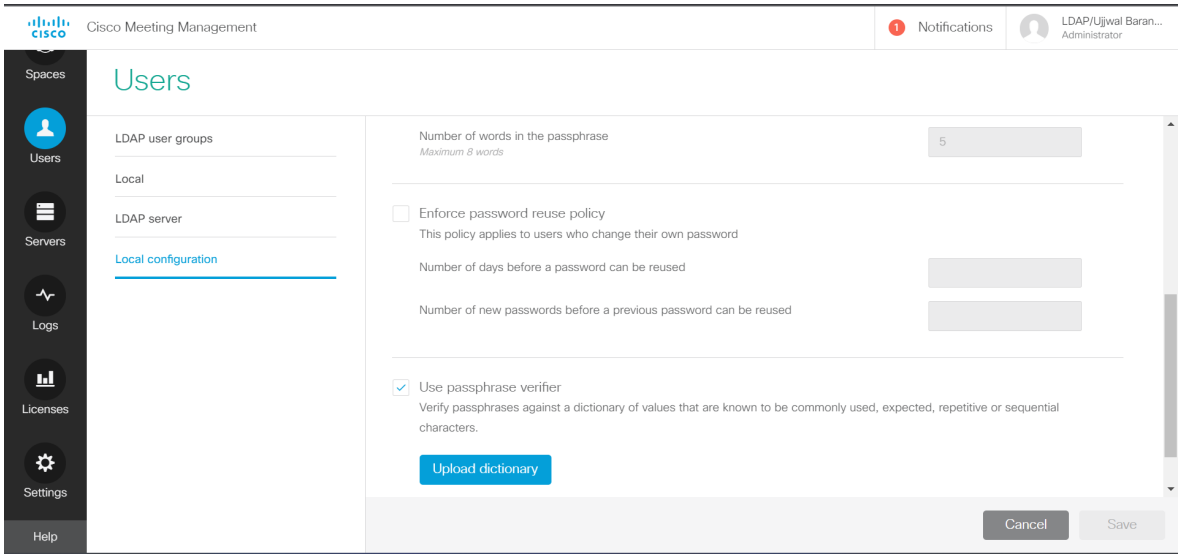
Dictionary requirements:

- The dictionary must be a text file with one word in each line.
- Characters must be UTF-8 encoded.
- The file must not contain any null characters.
- Maximum file size is 10 MB.

Note: Meeting Management does not provide a default dictionary. The administrators must define the dictionary and upload it.

To enable passphrase verifier:

1. In **Local configuration** section, scroll down to **Use passphrase verifier** and check the checkbox.
2. To upload the dictionary, click **Upload dictionary** button and select a .txt file containing a list of passphrases that do not meet the security requirements.



3. To remove existing dictionary file, click **remove**.

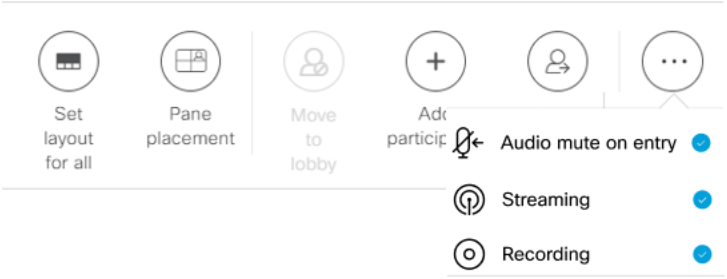
2.3 UI Modifications

In 3.9, **Meetings** page of Meeting Management has been redesigned by grouping the buttons for better user experience. The changes include:

- Moving **Lock** button 

up the line to place all global meeting settings in one line.

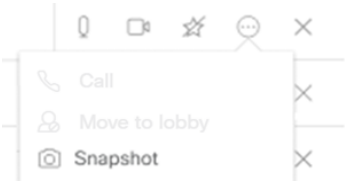
- Adding a new **More** button  in meeting level settings and placing **Audio mute on entry**, **Recording** and **Streaming** buttons underneath.

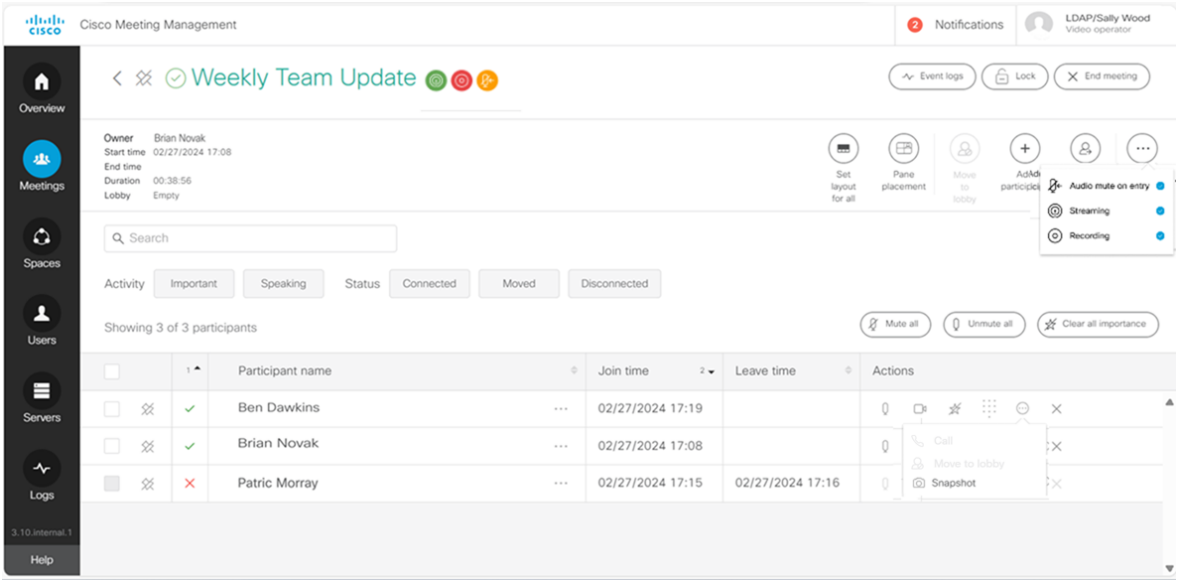


- Notifying users by displaying correponding icons near the meeting name, whenever **Audio mute on entry** is clicked or when **Recording** and/or **Streaming** is started.

- Moving **Mute**, **Unmute**, **Clear all importance** buttons above the participants' list.

- Adding a new **More** button  against each participant and moving **Call**, **Move to lobby** and **Snapshot** underneath.





2.4 Accessibility improvements

In version 3.9, Meeting Management introduces the following accessibility improvements:

- In **Overview** page > **Smart licensing**, use arrow keys on the keyboard to access dates inside the date picker.
- The invisible extra tabs are now removed from the **Server** screen.
- Use arrow keys to navigate Radio buttons in **Users**, **Spaces**, and **Settings** tabs.
- Keyboard and screen reader users can now use **Esc** key to close tool tip/help and other interactive elements available in the **Licenses** page.

3 Bug search tool and 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.

3.1 Using the bug search tool

1. Using a web browser, go to the Bug Search Tool. (https://bst.cloudapps.cisco.com/bugsearch/)
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 Management`, then in the **Releases** field select **Fixed in these Releases** and type the releases to search for, for example `3.5`.
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.

3 Open issues

The following are known issues in this release. If you require more details on any of these please contact Support, https://www.cisco.com/support.

Reference	Issue
CSCwj07820	When pane placement is active during a meeting, the **Clear importance for all** button is active and displays the tool-tip **Pane placement is enabled for this meeting and participant importance cannot be modified.**
CSCwj07818	If the participant details is opened after opening the drop-down available in the global level **More** option in **Meetings** page, the drop-down does not close and stays overlaid on the participant details section.
CSCwa37575	License registration fails when the generated SLR code has more than one customization license. After generating SLR code which has more than one customization license, uploading the authorization code in Meeting Management displays an error message **There is some issue with Authentication file**. Refreshing the page shows status of Meeting Management as registered, but in **Licenses** tab it still displays status as **Unlicensed**.
CSCwa44321	When collecting logs for servers on the **CMS Log Bundle** tab, if administrator searches the servers by their name and selects multiple servers, only a single server stands selected.
CSCvz30358	In Meeting Management, while using Installation Assistant to add or configure a new Meeting Server, user can click the disabled **Next** button in several panels to move to the next panel without configuring the mandatory parameters.
CSCvt64327	If an administrator uses special characters in a template name, then these may appear differently in status messages, displaying escape characters instead.
CSCvt64329	For meetings hosted on Meeting Server 2.9 and later the lock button looks like it is enabled for gateway calls, although it has no effect. The Meeting Server ignores the lock status. Workaround: There is no workaround but we do not expect that participants would want to lock gateway calls.
CSCvt64330	If you are using Smart Licensing and move a Meeting Management deployment to a different virtual account, then the information will not be updated in its user interface. Workaround: Manually renew registration now.
CSCvt00011	If the connection to one of the Call Bridges in a cluster is lost, then Meeting Management may not receive details about the space a meeting takes place in, and streaming may not work.
CSCvr87872	If CDRs are lost, Meeting Management may not reflect changes for participants who need activation. For instance, Meeting Management may keep displaying participants in the lobby when they have already been activated and moved to the meeting.
CSCvq73184	The user interface does not indicate that you cannot turn pane placement off if it is turned on for the space where the meeting takes place.

Note: Due to macOS updates, some certificates will no longer work for macOS users using Chrome. You should check that your certificate complies with the requirement "TLS server certificates must contain an ExtendedKeyUsage (EKU) extension containing the id-kp-serverAuth OID."

3 Resolved Issues

Resolved in 3.9.1 (Build 3.9.0.20)

Reference	Issue
CSCwi88558	Meeting Management web application fails to apply restrictions at the API level allowing non-administrative video operator to bypass administrative level controls and directly execute certain privileged commands on the endpoints using the emulated SSH session.

Resolved in 3.9 (Build 3.9.0.17)

Reference	Issue
CSCwf45189	In Meeting Management **Servers** page, while adding a server, the option to select **Configure New Server** is not accessible.

4 Interoperability

Interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco conferencing products.

4.1 Mute/unmute and layout behaviors

For more information on endpoint mute/unmute and layout control behaviors when used with Meeting Server and managed by Meeting Management, see:

- How will my endpoint mute/unmute controls behave when used with Cisco Meeting Server and managed by Cisco Meeting Management?
- How will my endpoint layout controls behave when used with Cisco Meeting Server and managed by Cisco Meeting Management?

5 Product documentation

The following site contains documents covering installation, initial configuration, and operation of the product:

https://www.cisco.com/c/en/us/support/conferencing/meeting-management/tsd-products-support-series-home.html

5.1 Related documentation

Documentation for Cisco Meeting Server can be found at:

https://www.cisco.com/c/en/us/support/conferencing/meeting-server/tsd-products-support-series-home.html

Documentation for Cisco Meeting App can be found at:

https://www.cisco.com/c/en/us/support/conferencing/cisco-meeting-app/tsd-products-support-series-home.html

Accessibility Notice

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

The Voluntary Product Accessibility Template (VPAT) for Cisco Master Project 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

6 Accessibility support features

6.1 Keyboard navigation

You can use your keyboard to navigate through Meeting Management.

- Use **Tab** to navigate between areas in Meeting Management. 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.

6.2 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 **Create Space** button, the screen reader will announce "Create Sapce" and to enter a space name.

Cisco Legal Information

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

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

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

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

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

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

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

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

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: