Cisco Meeting Management

Release 3.13.1

(Build 3.13.0.19)

Release Notes

June 04, 2026

Contents

Document Revision History

Table 1: Document revision history

Date	Description
2026-06-04	Updated for version 3.13.1 See Resolved issues section and Smart Licensing.
2026-05-04	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.

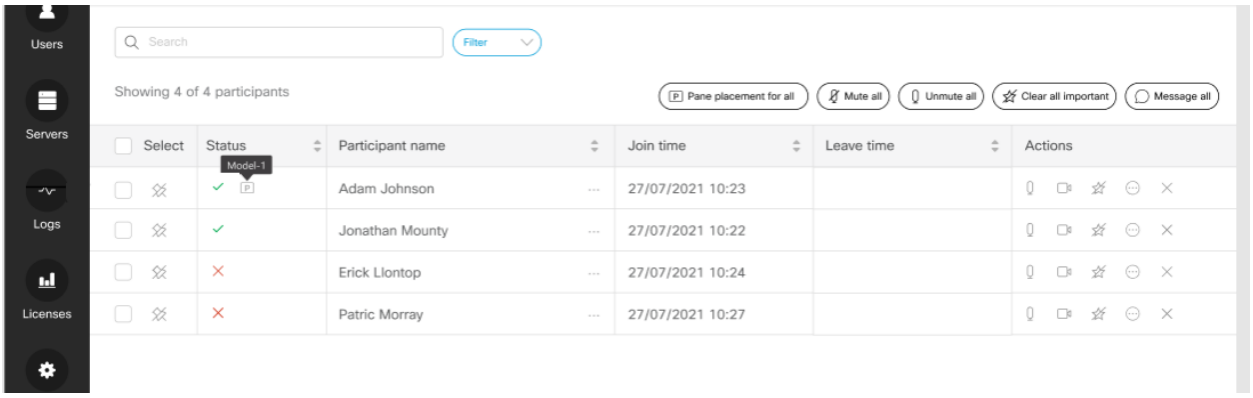
For security, there is no user access to configuring via the console after first run. Except for the installation process, all use of Meeting Management is via a browser interface.

2 New features and changes

In this section you can see what is new in 3.13.

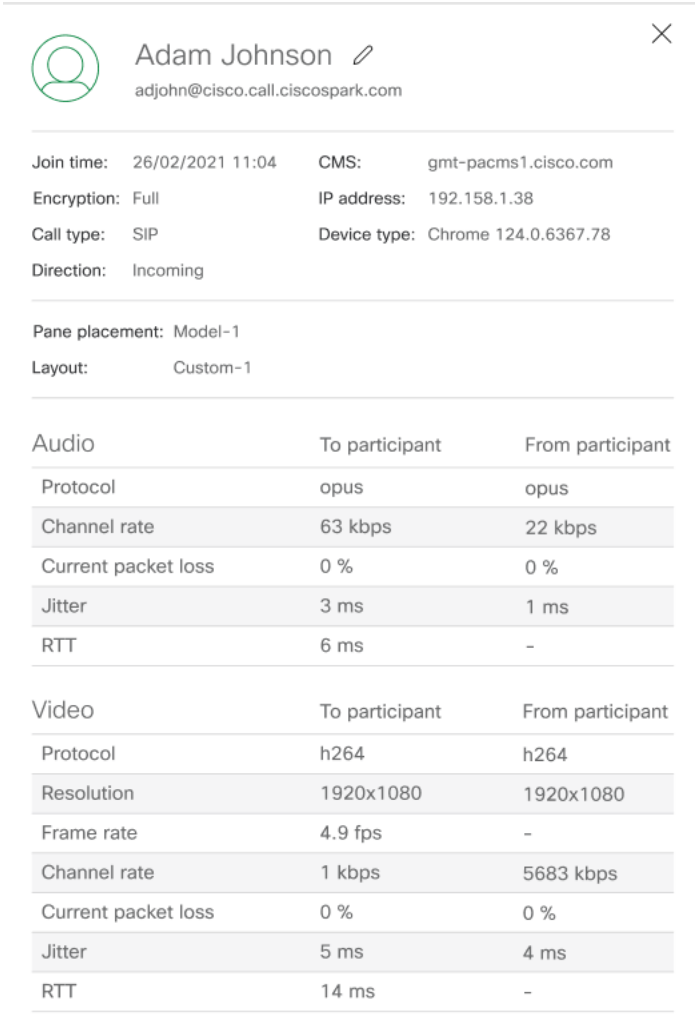
2.1 Display pane placement model name for participants

Meeting Management administrators and video operators can now view the name of the pane placement model applied to each participant by hovering over the [P] indicator icon available in the **Status** section next to the participant's name. This enhancement provides visibility into the pane placement model and layout applied during a meeting, enabling administrators and video operators to make informed decisions and manage layout configurations effectively.



Additionally, the **Participant details** panel displays the pane placement model and layout name as follows:

- **When no layout or pane placement is applied:** The panel displays **N/A** against **Pane placement** model name and the layout currently configured on the Meeting Server in **Layout**.
- **When pane placement is applied**: The panel displays model name and layout name based on selections made during model creation.
- **When a layout is set followed by enabling pane placement**: If a layout is initially applied via **Set layout for all** and a pane placement model is subsequently applied to all or specific participants, the panel displays the applied model name. The layout name will reflect the latest layout associated with that specific pane placement model.



Adam Johnson
adjohn@cisco.call.ciscospark.com

Join time:	26/02/2021 11:04	CMS:	gmt-pacms1.cisco.com
Encryption:	Full	IP address:	192.158.1.38
Call type:	SIP	Device type:	Chrome 124.0.6367.78
Direction:	Incoming		

Pane placement: Model-1
Layout: Custom-1

Audio	To participant	From participant
Protocol	opus	opus
Channel rate	63 kbps	22 kbps
Current packet loss	0 %	0 %
Jitter	3 ms	1 ms
RTT	6 ms	-

Video	To participant	From participant
Protocol	h264	h264
Resolution	1920x1080	1920x1080
Frame rate	4.9 fps	-
Channel rate	1 kbps	5683 kbps
Current packet loss	0 %	0 %
Jitter	5 ms	4 ms
RTT	14 ms	-

2.1.1 Points to note

- The [P] indicator tooltip does not appear when new participants join a meeting. In addition, the **Pane placement** and **Layout** fields display **N/A** on the **Participant details** page.
- If Meeting Management is restarted, the [P] indicator tooltip does not appear for all participants or for individual participants. The **Pane placement** and **Layout** fields display **N/A** on the **Participant details** page.

2.2 Enhancement to Blast Dial Timer

The initial blast dial timer in Meeting Management has been enhanced, allowing the delay before dialing-out to participants to be as short as 2 seconds, compared to the previous default of 10 seconds. This improvement enables faster participant connections and increases overall meeting responsiveness.

Note that the delay may not always be exactly 2 or 3 seconds, as the process is interactive. For example, if an active participant record is received within 2 seconds, the blast dial is triggered immediately. If the participant record takes longer to arrive, Meeting Management will wait an additional 2 seconds before triggering the blast dial, resulting in a total delay of 4 seconds, and so on.

3 Upgrading, downgrading and deploying Cisco Meeting Management

3.1 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.

Note:

- Prior to upgrading to version 3.13, ensure that a fully qualified domain name (FQDN) is configured in the network settings. Using an incomplete hostname may result in login failures.
- If the hostname in Network settings is not set to an FQDN before upgrading, Meeting Management can still be accessed via its IPv4 address, and the hostname can be updated to the FQDN afterward.

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.

3.2 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

3.3 Deployments

From version 3.13, Meeting Management supports deployments on VMware and Nutanix clusters.

3.3.1 VMware ESXi Deployment

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.

Note: This release of version 3.13.1 supports ESXi 8.0 U3e

3.3.2 Nutanix Deployment

Version 3.13.1 adds support to deploy Meeting Management on Nutanix clusters with the following specifications:

AHV: 10.3.1.2

AOS: 7.3.1.2

3.4 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_13_1.zip`**
- Name of upgrade image: **`Cisco_Meeting_Management_3_13_1.img`**
- MD5 checksum for upgrade image: **`603b876aa3998fb22000fd4023b6ec37`**
- SHA256 checksum for upgrade image:
  `c0daddf698893526eb97c143369a6533e1fc5d864535dacb7be2035b451a6662`
- SHA512 checksum for upgrade image:
  `d49eab8bc2d5a1d22e48bd91a39efe458c97026bf142ef0954c466bc885a428480d5b6c4055351da52f8581e184d8c3f1d4b977f6c3fe04eff97a3e015ba6a7a`

OVA for new installation on vSphere 8.0:

- File name: **`Cisco_Meeting_Management_3_13_1.ova`**
- MD5 checksum for image: **`5d526e9ce6935cd1b93dd4dc638a30f9`**
- SHA256 checksum for image:
  `83b9785026d5b4ea293a2a73a051bb205f915e59b538d2b30506c699b264a66a`
- SHA512 checksum for image:
  `938c80496cebd26d0bc2ad5aad72bc06404c3be1eaaa62ed901df5c122d24a1187342f9017cd38633b0e64181d1a7887f92077afd5adfa9034ffb17132184dcc`

Note: This release of version 3.13.1 supports ESXi 8.0 U3e and Nutanix clusters with the following specifications, **AHV:** 10.3.1.2 and **AOS:** 7.3.1.2 .

3.5 Smart Licensing

Smart licensing is mandatory for Meeting Management. All web proxy configurations used for Smart Licensing must be established as an HTTPS proxy.

To maintain secure communication, the proxy must support end-to-end HTTPS connectivity between the Meeting Management client, the proxy, and the Cisco Smart Software Manager (CSSM).

Note: This requirement represents an update from previous versions (prior to 3.13), where a standard HTTPS-capable proxy was sufficient. This change has been implemented to align with updated security standards and to ensure a more robust, secure connection for your environment.

For more information on Smart Licensing and upgrading , see Cisco Meeting Management User Guide for Administrators.

3.6 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.

3.6.1 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 3.11	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Management version 3.11.x is October, 2026

3.6.2 Discontinuation of CMM integration with Telepresence Management Suite

The integration of Telepresence Management Suite and Meeting Management will be discontinued in future releases due to Telepresence Management Suite approaching its end of life.

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

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

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.

3.8 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.

3.9 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
CSCwr59626	During an ongoing meeting, if Meeting Management is restarted, the blue indicator does not appear when applying a template at the per-participant level, potentially causing pane placement for new participants to malfunction.
CSCwr77094	The pane placement configuration icon displays the blue indicator even after disabling pane placement for all participants using the **Select All** check box.
CSCwo81112	When the Meeting Management administrator or video operator attempts to control a SIP participant's camera via the **front-end camera control** option, the participant receives no notification while their camera is being controlled.

Reference	Issue
CSCwo81113	Creating space using Meeting Management do not include webBridgeAddresses in the **Join Link**, which is configured on the webBridgeProfiles in Meeting Server, causing an issue in joining this space via the web app.
CSCwo81114	When a guest participant is moved from one meeting to another meeting, the Device IP and Device Type are being displayed as N/A in the participant info card.
CSCwo81116	When an administrator or video operator mutes a participant's audio and video in a meeting, and the participant is moved to another meeting with the **retain audio-video settings** check-box enabled, they cannot unmute their audio or video until the administrator manually re-enables them.
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."

3.10 Resolved Issues

Resolved in 3.13.1 (Build 3.13.0.19)

Reference	Issue
CSCwu48216	In Meeting Management 3.13.0, the DNS resolution logic fails to perform a failover to the secondary DNS server wherein the primary DNS server was reachable but returned an error for a specific FQDN causing the system to incorrectly terminate the resolution process.
CSCwu22082	Meeting Management 3.13.0 experiences a systemic failure to resolve any Fully Qualified Domain Names (FQDNs)–such as Meeting Server, LDAP, or Smart Licensing, when configured with a static IP address. This issue occurs because the interface incorrectly assigns two IP addresses, disrupting communication with essential services.

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 Space" 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.

© 2026 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

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