Cisco Meeting Management

Release 3.10

(Build 3.10.0.26)

Release Notes

September 27, 2024

Cisco Systems, Inc. www.cisco.com

Contents

Document Revision History

Table 1: Document revision history

Date	Description
2024-09-27	Document published - 3.10

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 3.10.

2.1 Pane Placement Per Participant

From 3.10, Meeting Management administrators and video operators will be able to create different pane placement arrangements for every participant. Previously, a single pane placement arrangement was applied to all participants in the meeting. From this release, different pane placement arrangements, called as models, can be defined and applied for each participant. Pane placement models enable a particular participant to view other participants in different order/panes/arrangements. For example, the hosts or invited speakers of an ongoing meeting can have different pane placement models assigned based on their preferences.

This feature works for SIP and web app participants.

Points to note:

- Each meeting can have a maximum of three pane placement models defined, which can be modified or deleted at any time while the meeting is active. However, the modified model must be re-applied for the modifications to take effect on the participants' screen.
- The defined pane placement models can be assigned to an individual participant, multiple participants, or all participants at once. This reduces the time taken in assigning the arrangement to each participant.
- The models will be available and can be assigned only until the meeting is active.
- Each participant may only be assigned one model at a time, but the same model can be assigned to multiple participants.
- Pane placement can be set only after the meeting has started, and only active participants can be assigned to panes. If placed participants are disconnected from the meeting, their pane is no longer assigned to them.

  This means that the pane that was assigned to them will be displayed as a blank pane. If you want placed participants to be placed in the same pane after they reconnect, you must assign the model again to these participants.
- Participants newly joining, or if placed participants are disconnected from the meeting, their panes are no longer assigned to them. Such participants will get a default layout and no pane placement will be applied to this participant.
- If a model is applied for a particular participant A in a meeting and later another model is applied for all the participants in this meeting. Then the model applied later will take precedence and override the model which was previously applied for participant A.
- Before a model is applied, if all participants with reserved panes in that model are dropped out of the meeting, then that model cannot be applied to other participants.

- If the models are deleted during a meeting after pane placement has been applied for all or some of the participants, the pane placement button on the meeting level and per participant level stays enabled. The administrator must manually disable the pane placement using the **Disable** button.
- When there are multiple Meeting Management setups:
  - Models created in one Meeting Management will not be available on other Meeting Management setups to edit or apply.
  - You can disable pane placement models from any Meeting Management by selecting the **Disable** option available in the **Pane placement for all** drop-down.
  - If there are models created in multiple setups, the last/latest model applied for pane placement from any of the Meeting Management takes precedence.

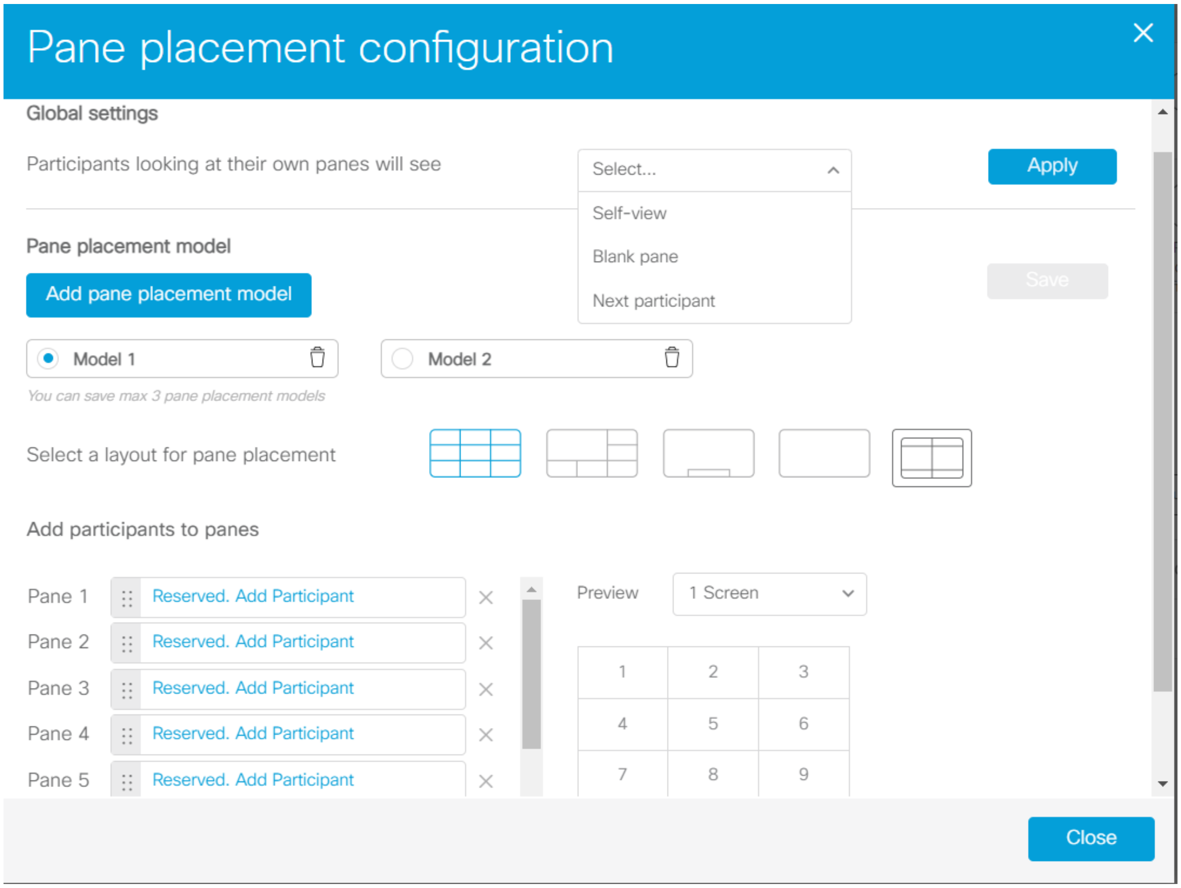
2.1.1 UI modifications:

2.1.1.1 Define Pane Placement Models

On the **Meetings** page, the existing **Pane placement** button has been changed to **Pane placement configuration**. Clicking this button opens **Pane placement configuration** pop-up window that includes the following sections:

1. **Global Settings** – As was in the earlier versions, this section allows the administrators/video operators to assign one of the following options for the participants to see on their screen.
   - Self view
   - Blank pane
   - Next participant

2. **Pane placement model** - This option allows administrators/video operators to create, edit, save and delete pane placement models.



Pane placement configuration

Global settings

Participants looking at their own panes will see: Select...
- Self-view
- Blank pane
- Next participant

Pane placement model

○ Model 1 ○ Model 2

You can save max 3 pane placement models

Select a layout for pane placement

Add participants to panes

Pane 1	Reserved. Add Participant
Pane 2	Reserved. Add Participant
Pane 3	Reserved. Add Participant
Pane 4	Reserved. Add Participant
Pane 5	Reserved. Add Participant

Preview: 1 Screen

1	2	3
4	5	6
7	8	9

2.1.1.2 *Apply pane placement layouts*

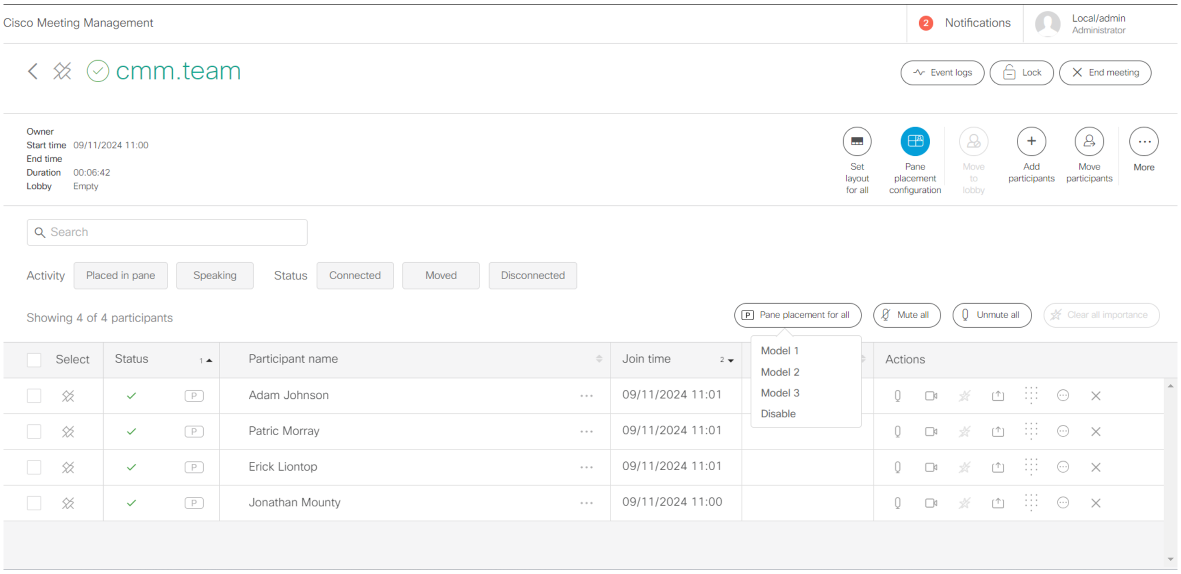
The defined pane placement models can be applied to a single participant, multiple participants selected at once or all the participants in the meeting.

- **To apply the defined pane placement models for all or selected participants:**

  A new **Pane Placement for all** button that lists all the available models, has been added above the participant list.

  Select the **all** checkbox or choose the required participants from the list and click the **Pane Placement for all** button. Choose the required pane placement model from the list to apply. Additionally, the drop-down will also include the option to disable pane placement model, if already applied.

  An indicator P will be displayed in the **Status** column for participants who have pane placement model applied.



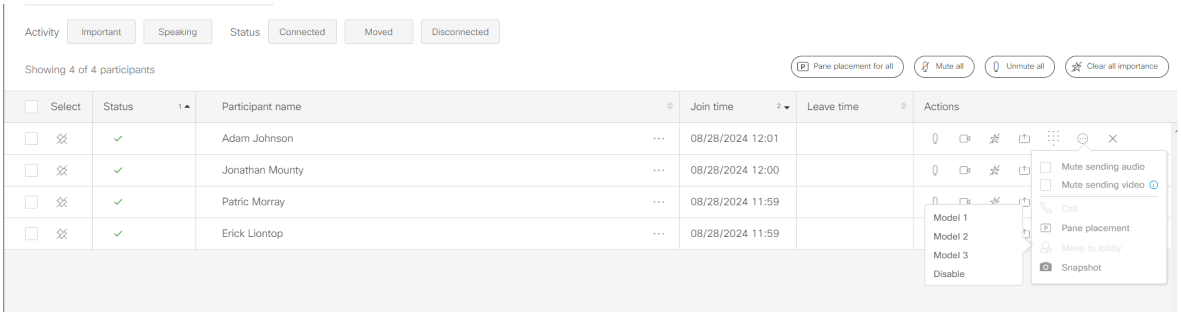
Owner
Start time 09/11/2024 11:00
End time
Duration 00:06:42
Lobby Empty

Showing 4 of 4 participants

Select	Status	Participant name	Join time	Actions
□	✓ P	Adam Johnson	09/11/2024 11:01	
□	✓ P	Patric Morray	09/11/2024 11:01	
□	✓ P	Erick Liontop	09/11/2024 11:01	
□	✓ P	Jonathan Mounty	09/11/2024 11:00	

- **To apply pane placement for a particular participant:**

  The ⋯ **More** option available against each participant now includes a new **Pane Placement** option that lists the available pane placement models. Select the required model from the list to apply the model for a particular participant. Follow the same procedure to override any existing pane placement and to apply a different model for a particular participant in a meeting.



Showing 4 of 4 participants

Select	Status	Participant name	Join time	Leave time	Actions
□	✓	Adam Johnson	08/28/2024 12:01		
□	✓	Jonathan Mounty	08/28/2024 12:00		
□	✓	Patric Morray	08/28/2024 11:59		
□	✓	Erick Liontop	08/28/2024 11:59		

2.2 Security Enhancements

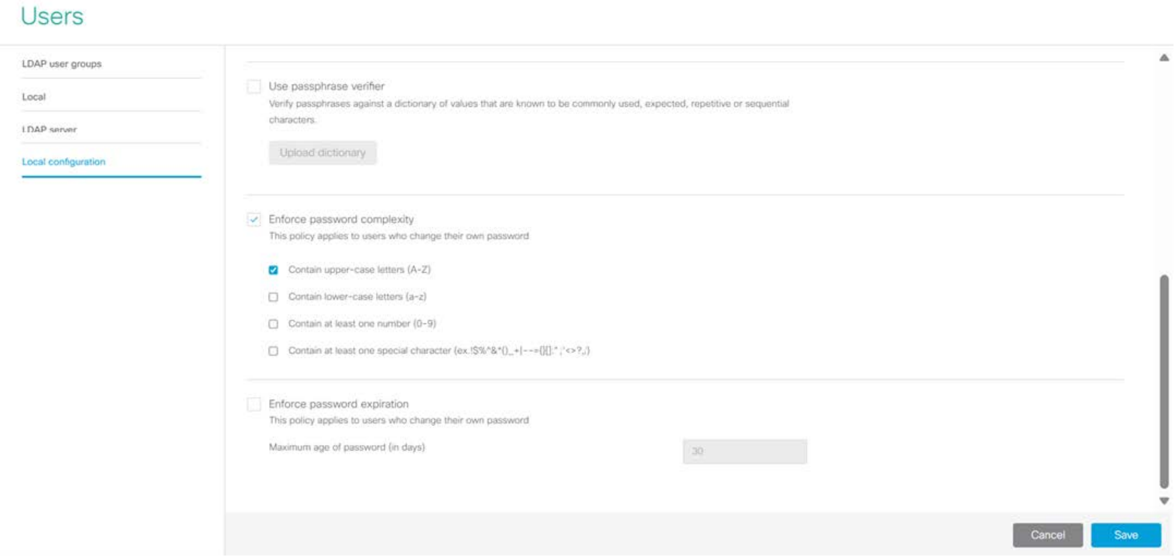
2.2.1 Enforce password complexity

Password complexity checks the strength of the password. Meeting Management administrators may set the level of complexity required in passwords when users create them. Administrator, while setting up security policies for users, can select any or all of the following options on the **Users** page in the **Local configuration** tab under **Enforce password complexity**:

- Contain upper-case letters (A-Z)
- Contain lower-case letters (a-z)
- Contain at least one number (0-9)
- Contain at least one special character (!$%^&*()_+|~-={}[]:";'<>?,/)

To enable password complexity:

1. In **Users > Local configuration** tab, enable **Enforce password complexity** checkbox.
2. Select the checkbox options that are necessary in the user's password.



□ Use passphrase verifier
Verify passphrases against a dictionary of values that are known to be commonly used, expected, repetitive or sequential characters.

☑ Enforce password complexity
This policy applies to users who change their own password

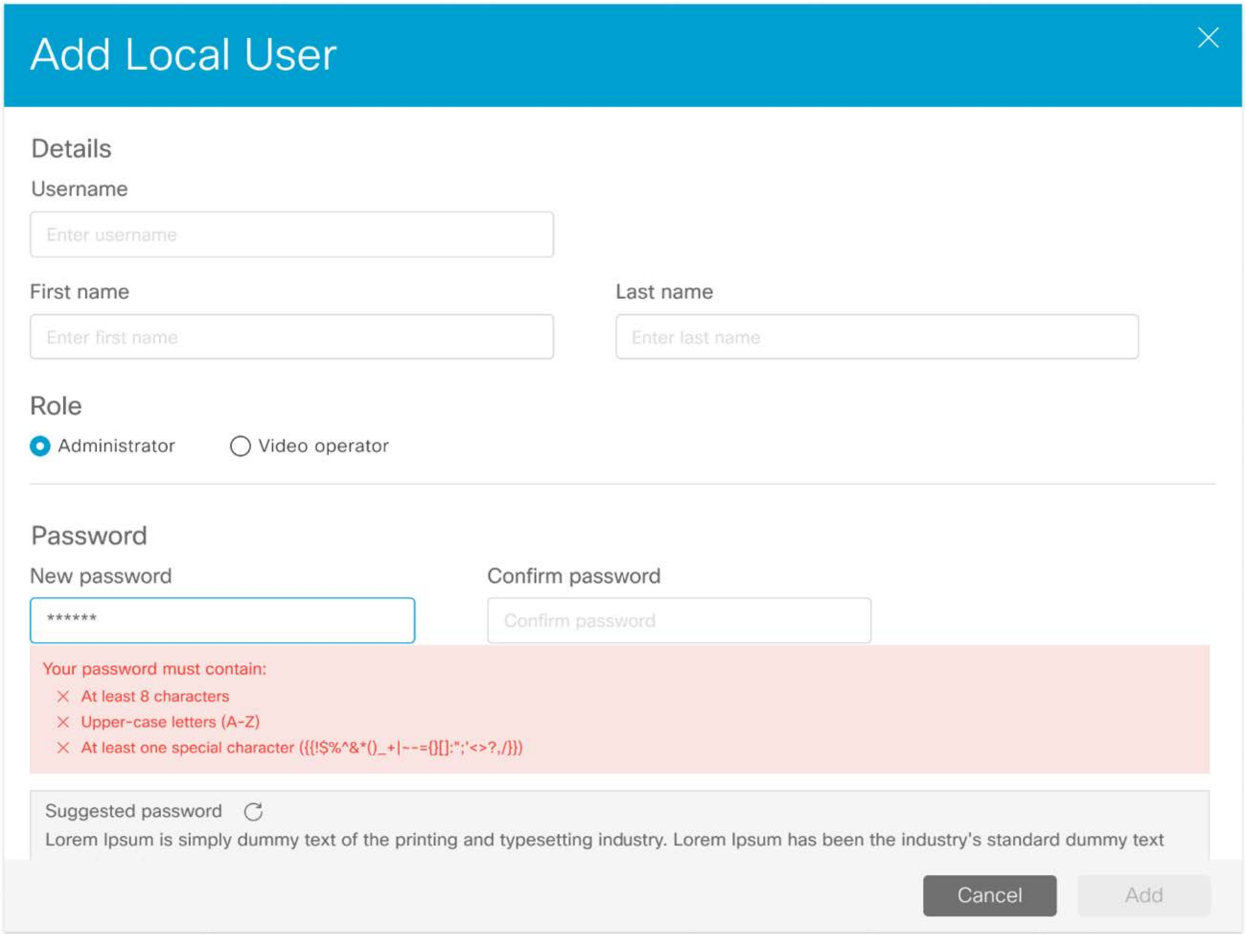
☑ Contain upper-case letters (A-Z)
□ Contain lower-case letters (a-z)
□ Contain at least one number (0-9)
□ Contain at least one special character (ex.!$%^&*()_+|~-={}[]:";'<>?,/)

□ Enforce password expiration
This policy applies to users who change their own password

Maximum age of password (in days) 30

3. Click **Save**.

While adding or editing a local user in **Users > Local** tab, if the password set by the user in **Add Local User** pop-up window does not meet the criteria configured by the administrator, Meeting Management now notifies the user to include the necessary character(s) to meet the password strength.



Add Local User

Details

Username

Enter username

First name

Enter first name

Last name

Enter last name

Role

● Administrator ○ Video operator

Password

New password

******

Confirm password

Confirm password

Your password must contain:

- ✕ At least 8 characters
- ✕ Upper-case letters (A-Z)
- ✕ At least one special character ({{!$%^&*()_+|~-={}[]:";'<>?,/}})

Suggested password

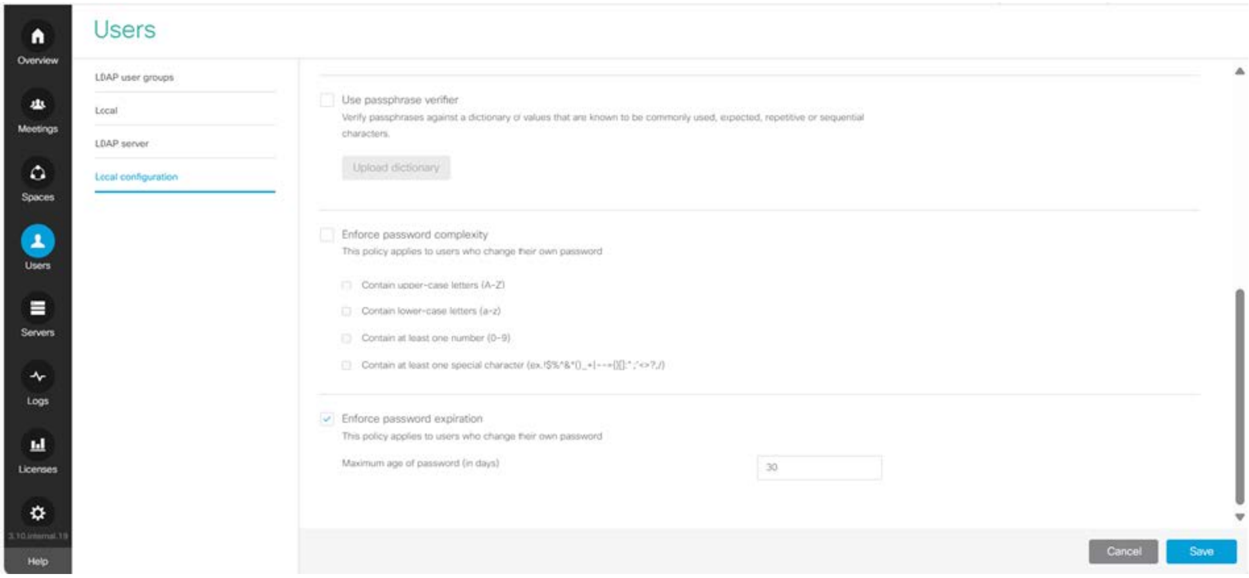
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text

2.2.2 Enforce password expiration

Password expiration allows administrators to configure the duration (in days) a password can be used. When the password expires, Meeting Management disables the user’s access and notifies them to change the password.

To enable password expiration:

1. In **Users > Local configuration** tab, enable **Enforce password expiration** checkbox.
2. Enter the number of days in the **Maximum age of password (in days)** field.
3. Click **Save**.



□ Use passphrase verifier
Verify passphrases against a dictionary of values that are known to be commonly used, expected, repetitive or sequential characters.

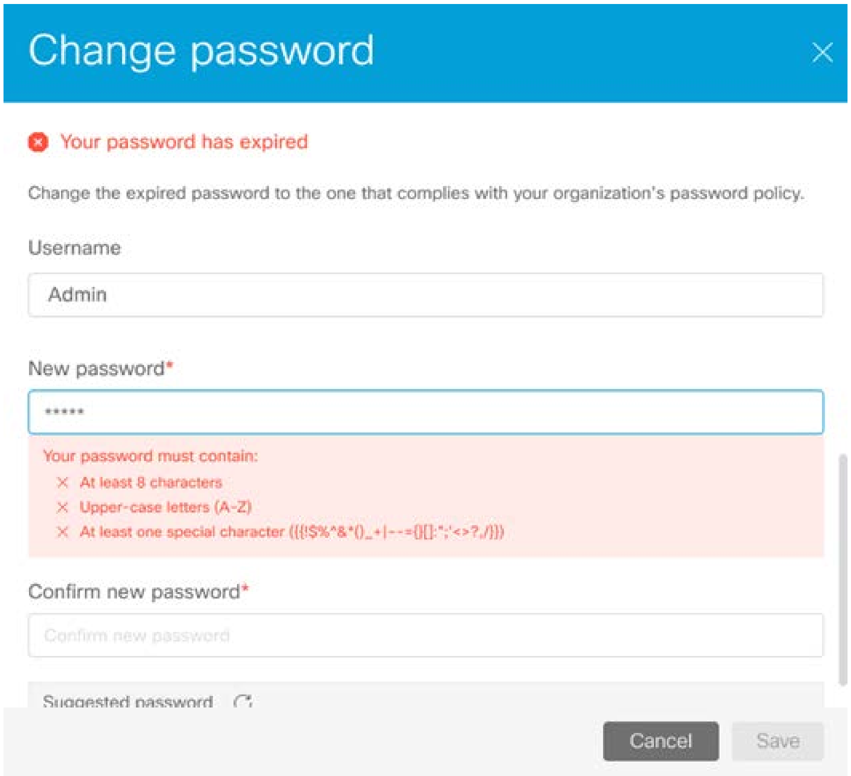
□ Enforce password complexity
This policy applies to users who change their own password

□ Contain upper-case letters (A-Z)
□ Contain lower-case letters (a-z)
□ Contain at least one number (0-9)
□ Contain at least one special character (ex.!$%^&*()_+|~-=\{}[]:";'<>?,/)

☑ Enforce password expiration
This policy applies to users who change their own password

Maximum age of password (in days) 30

Once enabled, Meeting Management notifies the user to create a new password when the user logs-in after the current password is expired.



Your password has expired

Change the expired password to the one that complies with your organization's password policy.

Username
Admin

New password*
*****

Your password must contain:
- ✕ At least 8 characters
- ✕ Upper-case letters (A-Z)
- ✕ At least one special character ({{!$%^&*()_+|~-={}[]:";'<>?,./}})

Confirm new password*
Confirm new password

2.3 Restrict content sharing at participant level

From version 3.10 of Meeting Management, administrators/video operators can enable or disable content sharing privileges for selected participants during an ongoing meeting. When content sharing is restricted for selected participants, they will not be able to share/present it to other participants in the meeting. Any ongoing content sharing will be blocked immediately if the selected participant is presenting. Participants cannot enable their access to content sharing.

A new button has been added in participant-level settings that allows content sharing. On clicking this button against a participant, the icon changes to and stops/restricts the content sharing ability for the selected participant. Once restricted, the other participants in the meeting will not be able to view the content that is being shared.

This feature:

- is applicable for both SIP and web app participants.
- is applicable for participants joining through audio/video mode and Presentation-only mode.

If the content sharing is disabled when the participant is presenting in an ongoing meeting, then:

- For the presenter:
    - Content sharing is stopped immediately, however, the presenter will still be able to view the content sharing notification bar and the shared window in picture mode. The presenter can exit the presentation mode using the stop sharing button on the sharing notification bar.
- For other participants:
    - Content sharing will be stopped immediately for both SIP and web app. However, in case of web app, presenting icon continues to be displayed against the presenter's name in the participant list.

Note:

- If using different end points that offer other sharing options like whiteboard, the content sharing of such options will not be restricted.
- When the sharing option is disabled, the share button available on the endpoints does not get disabled/hidden, but on clicking, an appropriate error message will be displayed.

2.4 Show participant name for blast dial

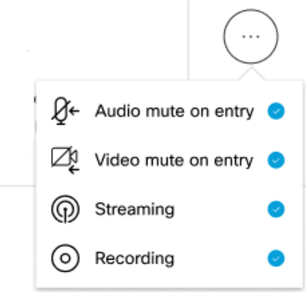
In version 3.10, the blast dial feature is enhanced to display the participant name along with their number when the participant is dialed out using blast dial.

Previously, although participant names and phone numbers were added during the blast dial configuration, while dialing out, it still displayed only the participant's number, making it difficult to identify the participant being dialed out. With this release of Meeting Management, the administrator and web app participants can identify the participant being dialed out by name rather than just by phone number.

2.5 Video Mute on Entry - UI Modifications

This feature allows the administrator/video operator to disable or mute the participant’s video while joining a meeting, regardless of their video settings. This prevents any interruption caused while joining an ongoing meeting. Video muted participants will stay video muted until they unmute their video themselves or administrator/video operators unmutes the video. This option will only affect new participants; those already present in the meeting will not be affected.

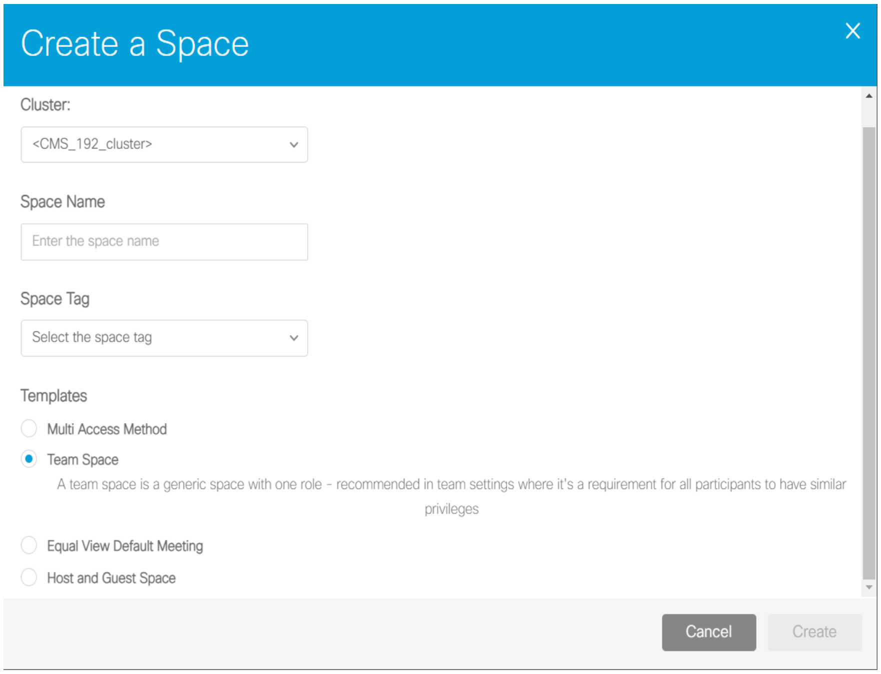
This feature is implemented by including a **Video mute on entry** button within the **More** button pop-over in meeting level settings.



This option is disabled by default. Once enabled, a Video mute on entry icon is displayed near the meeting name to inform that the participants are being video muted on entry. The new participants joining this meeting will see the notification **Your video has been disabled**. The participants have the option to stay disabled or enable their video whenever required. Once the meeting is locked and a participant tries to join the meeting with video enabled, the video still gets disabled as soon as the participant enters and waits in the lobby.

2.6 Support for video operators to create spaces

From version 3.10, besides administrators, video operators can also create and edit spaces. The **Create space** button in the **Spaces** page enables the video operators to create spaces. Furthermore, a new **Space tag** drop-down has been added in the **Create a Space** pop-up window that allows the video operator to assign tags to the spaces. The drop-down lists the tags associated with the respective video operator.



Create a Space

Cluster:

<CMS_192_cluster>

Space Name

Enter the space name

Space Tag

Select the space tag

Templates

○ Multi Access Method

● Team Space

A team space is a generic space with one role - recommended in team settings where it's a requirement for all participants to have similar privileges

○ Equal View Default Meeting

○ Host and Guest Space

The created space will be listed in the **Spaces** page. On the meeting space created in Meeting Management, video operators can:

- View, edit, and delete the space(s) created in Meeting Management.
    - Spaces created in web app will be in view only mode in Meeting Management and cannot be edited or deleted.
    - The video operators can edit or delete spaces created by them or those they are tagged with. The following table explains the access enabled for tagged and untagged video operators to the spaces created in Meeting Management:

Users	Tagged spaces	Untagged spaces
Tagged video operator	Access to view, edit, delete	No access
Untagged video operator	No access	Access to view, edit, delete

- Obtain join information as email template and share it with the participants.

Note:

- The administrators can view, edit and delete the spaces created by the video operators.
- Meeting Management will display the join link only if the port is configured in the Meeting Server.
- Spaces created on Meeting Management will not have the domain name in the video address, while the spaces created in web app will have the domain name.

- Enable or disable blast dial feature.

2.7 Support to mute audio and video transmission to participants

From version 3.10, Meeting Management administrators/video operators, in an ongoing meeting, can restrict the meeting audio and video from being transmitted to selected participants. Selected meeting participant(s) will not hear audio or view video of other participants in the meeting. Ongoing screen sharing will also be blocked for such participants. Meeting participants do not have the control to enable their access to audio/ video.

Two new checkboxes, **Mute sending audio** and **Mute sending video**, have been added under the **More (...)** option button in the participant level settings. These checkboxes will be unchecked by default. Enabling these checkboxes will restrict only audio/ video from being transmitted to the selected participant. This participant can still perform a screen share or send audio/video. To restrict this, administrators/video operators will have to use the existing **Mute audio** or **Stop video** buttons.

Note:

- This option is available for both SIP and web app participants.
- A web app participant with audio or video blocked by administrator/video operator will still be able to view **who is speaking** or **who is presenting** , in the participant list.

3 Upgrading, downgrading and deploying Cisco Meeting Management

This section assumes that you are upgrading from Cisco Meeting Management 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 Management 3.10 Release Notes.

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.

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 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.

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_10_0.zip`
- Name of upgrade image: `Cisco_Meeting_Management_3_10_0.img`
- MD5 checksum for upgrade image: `371f196045d2eaaa592c08fa2f174986`
- SHA256 checksum for upgrade image: `f8d8d03e6bba3f21392351594ad0e43bab353845b7c4952a55dbcffcdb641e97`
- SHA512 checksum for upgrade image: `1b28b56ff298d44cc0c6af5dedbf13e9f7d5914543d611f4af8d6aa7a1680ae58ad9291e484557d7958a74d06a7bccf3acdfc2178b0409ddd2bc28fdec36fafe`

OVA for new installation on vSphere 7.0:

- File name: `Cisco_Meeting_Management_3_10_0_vSphere-7_0.ova`
- MD5 checksum for image: `f294adb83d829b7ce5dd7e0c5c6ae26f`
- SHA256 checksum for image: `b04ece6d1ab5fc8670734b5b8af347a8689aeb96ffbf440db49bd6af91eacaff`
- SHA512 checksum for image: `e681cde82438567b91f89ea22a67c0db705a8fca8e3f55e67f781487b7e3d287d9d17208a7ef127cfc9d1d3d5eb1288d46d10883277179b6cc170d2303e6a6ac`

Note: This release of version 3.10 supports ESXi 8.0 U3 and ESXi 7.0 U3q.

3.5 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.

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 3.5.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Management version 3.5.x is July 15, 2023.
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.
Cisco Meeting Management version 3.8	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Management version 3.8.x is March 14, 2025.

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.

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.

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
CSCwk97638	In a multiple Meeting Management setup wherein the setup is managed by one Meeting Management, there is no notification displayed indicating that the setup is managed by one Meeting Management and the experience on other Meeting Managements will be disjoint.
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.

Reference	Issue
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 3.10 (Build 3.10.0.26)

Reference	Issue
CSCwe65616	Taking snapshots is only allowed on Meeting Management for a licensed snapshot version. For the unlicensed version, it returns an error message.
CSCwm52351	On upgrading Meeting Management, the user tags assigned for Local User video operator are not persistent.

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.

© 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)