



Cisco Meeting Management

Release 3.1 1

(Build 3.1 1.0.40)

Release Notes

April 30, 2025

Contents

Document Revision History	1
1 Introduction	1
1.1 The software	1
2 New features and changes	2
2.1 Retain audio video settings while moving participants from one meeting to another	2
2.1.1 Points to note	3
2.2 Rotate participants in a fixed pane	3
2.2.1 Points to note	3
2.2.2 UI modifications	4
2.3 Password security enhancements	5
2.3.1 Password Expiry	5
2.3.2 Change password for first login	6
2.3.3 Password retries	6
2.4 Allow encryption for Category C and D smart accounts	6
2.5 Modifications in participant info card	8
2.6 On-screen messages via Meeting Management	8
2.6.1 Points to note	9
2.6.2 UI modifications	9
2.7 Display IP address and device type in participant details	10
2.8 Applying layouts for new participants	11
2.8.1 UI modifications	11
2.8.2 Points to note	12
2.9 Applying pane placement for new participants	13
2.9.1 UI modifications	13
2.9.2 Points to note	15
2.10 Improvements in space creation	15
2.11 Far end camera control	16
3 Upgrading, downgrading and deploying Cisco Meeting Management	18
3.1 Upgrading from previous version	18
3.2 Downgrading to previous version	19
3.3 Deploying the OVA	19
3.4 Checksums for upgrade and installation files	20

3.5	Smart Licensing	20
3.6	End of software maintenance for earlier versions	20
3.6.1	End of software maintenance	21
3.6.2	Discontinuation of CMM integration with Telepresence Management Suite	21
3.7	Meeting Management and connected Meeting Servers must run the same software version	21
3	Bug search tool and resolved and open issues	22
3.8	Using the bug search tool	22
3.9	Open issues	22
3.10	Resolved Issues	23
4	Interoperability	25
4.1	Mute/unmute and layout behaviors	25
5	Product documentation	26
5.1	Related documentation	26
	Accessibility Notice	27
6	Accessibility support features	28
6.1	Keyboard navigation	28
6.2	Screen reader support	28
	Cisco Legal Information	29
	Cisco Trademark	30

Document Revision History

Table 1: Document revision history

Date	Description
2025-04-30	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 3.11.

2.1 Retain audio video settings while moving participants from one meeting to another

From 3.11, Meeting Management administrators and video operators can move participants from one meeting to another while retaining some of the participant-level settings applied to them in the previous meeting. All/any of the following settings applied to the participant in a particular meeting can be retained when moved to another meeting:

- Send audio mute
- Send video mute
- Receive audio mute
- Receive video mute
- Content sharing restriction

The settings can be retained using the new **Audio, video and content sharing** check-box added in the **Move Participants** screen in the **Meetings** page. The check-box is activated only when at least one participant is selected.

Move Participants ×

Moving from: [selected participant] sync up meeting Audio, video and content sharing

Select who is moving Selected All

Search participants

Moving to

Search TMS conference ID or title

Select all

- Adam Johnson
- Jonathan Mounthy
- Erick Llontop
- Patric Morray

Cancel Move

2.1.1 Points to note

- This feature works for both SIP and web app participants.
- Layout and pane placement settings cannot be retained when moving participants to another meeting.
- The settings will be retained even if the participants are moved to the lobby while waiting to enter a locked meeting.
- Dial out participants can also be moved to another meeting via Meeting Management.

2.2 Rotate participants in a fixed pane

From 3.11, the administrator and/or video operator have an option to assign a pane in a pane placement model that will display all participants who are not reserved with a fixed pane in the model. This is done by assigning a pane as roll participants pane in a pane placement layout. In meetings with a medium to large number of participants, assigning panes to some participants makes other participants remain out of focus during the meeting. With this feature, each participant is displayed for a duration of 20 seconds in a rotational sequence, making it easier to manage participant visibility during meetings. However, this duration is not configurable. This applies for both SIP and web app participants.

2.2.1 Points to note

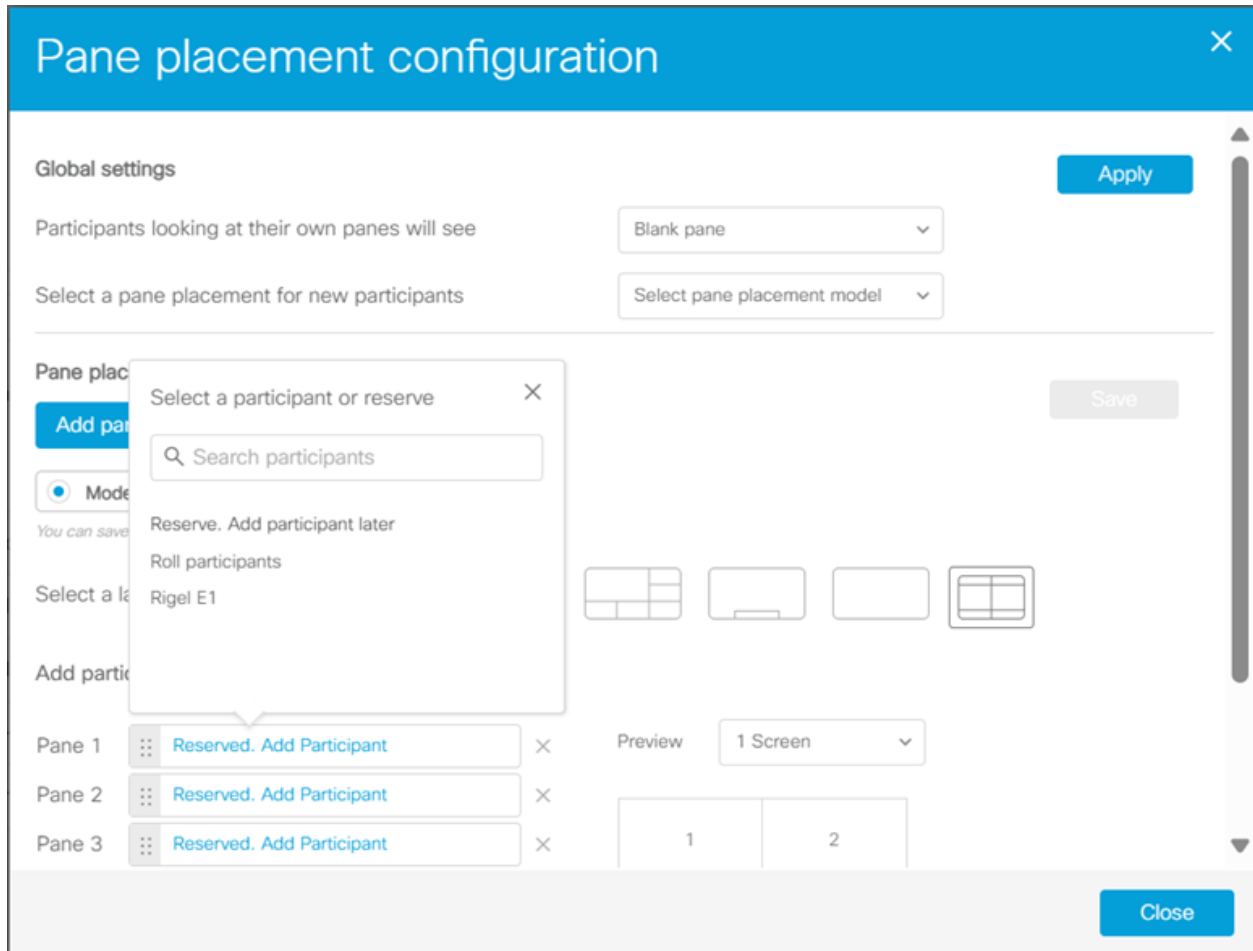
- The participant's video must be turned on throughout the meeting for the participant to be displayed in the rotate pane.
- Any pane, but only one pane, can be assigned for rolling participants in each pane placement model.
- Different models can have different panes for rolling participants.
- If placed participants are disconnected from the meeting, their panes are no longer assigned to them. Such participants will be displayed in the roll participant pane. The pane reserved for such participants will display a blank screen for other participants. Administrator/video operator will have to re-assign the panes for these participants by editing the model and then applying the model again.
- During a meeting, the administrator is allowed to change and assign a different pane for rolling participants. Once done, the administrator has to re-assign the model for the rolling participants to be displayed in the new pane.
- When a model is assigned to a single, chosen, or all participants, the roll participant pane selected in the model will also be displayed accordingly.
- If no pane placement model is applied for the meeting, this feature will remain inactive.

- Only the participants with their videos turned on will be displayed randomly in the rolling participant pane.
- In a cluster setup with multiple Meeting Management, roll participants pane assigned from a specific Meeting Management, will be applied to all participants in the meeting throughout the cluster.
- The roll participant pane will remain empty:
 - If all the participants, other than the participants shown in the fixed pane(s), have their video turned off.
 - If network connectivity causes video streaming issues for any participant.
 - If a participant turns off the video while being displayed on the roll participant pane

Note: In a clustered setup with over 25 participants, it is advised to mute everyone except the active speakers to ensure the rotate pane functions effectively.

2.2.2 UI modifications

In the **Pane placement configuration** window, after creating a model, while reserving participants in specific panes, a new option, **Roll participants**, has been added. The administrator or video operator can assign a pane for rolling participants.



2.3 Password security enhancements

2.3.1 Password Expiry

From 3.11, the password expiry feature of Meeting Management has been enhanced to alert local users when their passwords are nearing expiration. When there are 7 days or fewer left until password expiry, a warning message will be displayed in the **Notifications**, notifying the local user of the upcoming password change that is required. However, if the password is going to expire within 24 hours or less, an error message will be displayed, requiring the password to be updated immediately. If the user does not change the password after receiving the notification, their account will be locked and the administrator will have to interfere to change the password.

In case the administrator configures a password expiry period as 7 days or less, then only error messages will be displayed, and the warning message feature will be disabled. This is because the system still adheres to the default 7-day warning period, even after a local user changes their password, the warning message might continue to appear until the full 7-day duration is

reached. Hence, disabling warning message prevents confusion for the users.

13/02/2025 14:05:31 Your password will expire in 3 day(s). Please update it.

Warning

17/02/2025 13:57:47 Your password will expire in 1 day(s). Please update it.

Error


2.3.2 Change password for first login

From 3.11, Meeting Management ensures secure access by prompting users to change their password on their first log-in. Whenever a user logs in for the first time or when an administrator resets their password, they are prompted to set a new password, with a message **Please set your own password now..** The user will be prompted to enter a new password twice to avoid mistakes and to confirm that the intended password is correctly configured. This two-step process guarantees that users have complete control over their log-in credentials from the moment they access the system.

2.3.3 Password retries

From version 3.11, Meeting Management by default allows a maximum of 20 failed sign-in attempts for both LDAP and local users, after which a lockout period of 15 minutes is enforced. This restriction helps prevent unlimited password retry attempts, thereby protecting Meeting Management from brute force attacks and unauthorized access. If users attempt to sign-in after exhausting their retry attempts, they will receive the message: **Too many incorrect sign in attempts. Please try again later.**

Previously, the lockout period could only be enabled when the administrator configured the number of retry attempts for local and LDAP users within a specified interval in **Sign-in rate limiting** in **Advanced settings**. Now, even if the **Sign-in rate limiting** is disabled, the lockout will be applied once the default number of failed attempts is reached. In case **Sign-in rate limiting** is enabled by the administrator, Meeting Management follows and limits the rate of sign-in as configured by the administrator. If a local user is locked out, an administrator can manually

unlock the account by clicking the  button available next to each local user in the local users list, found in **Users > Local**. However, the list will not indicate any status whether a local user is locked out or not. For LDAP users, the lockout cannot be bypassed until the default 15-minute lockout timer expires.

2.4 Allow encryption for Category C and D smart accounts

Countries classified under category C and category D in the Cisco Smart Licensing Export Compliance Policies are not permitted to have encrypted calls. Meeting Management

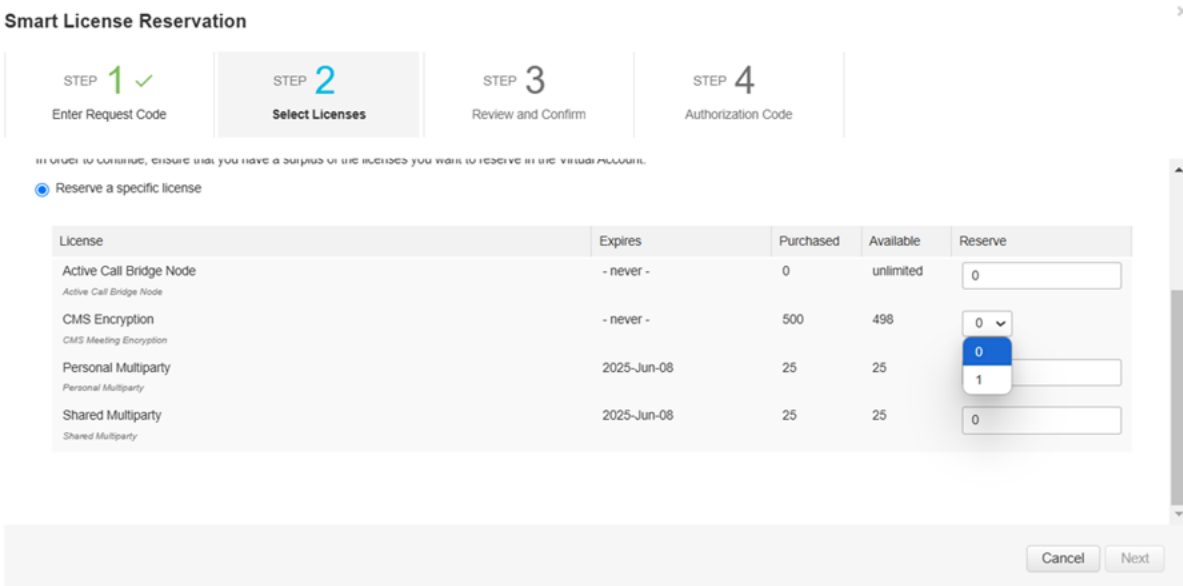
automatically disables call encryption in these restricted regions to comply with the licensing and regulatory requirements.

From version 3.11, Meeting Management introduces the reservation of a single license, LIC-CMS-ENCRYPT-S, specifically for these regions giving the users the option to encrypt the calls if required.

The table below explains the validations done by Meeting Management to allow call encryption:

Country Code	Call Encryption Status	Actions performed by Meeting Management	License reservation and encryption
A and B	Enabled by Default	Allows call encryption	License reserved and enable encryption.
C and D	Disabled by Default	Checks the availability of encryption license: LIC-CMS-ENCRYPT-S	If Yes: Single quantity license available and enable encryption
			If No: No license is reserved. No encryption.

Meeting Management identifies the country category code for C and D categories, and accordingly further validates if there is an active LIC-CMS-ENCRYPT-S to allow call encryption. Once available, it allows call encryption.



The encryption license can be enabled while reserving licenses using the Smart Account of Cisco Smart Software Licensing Manager. Generate the **Reservation Request Code** using Meeting Management and provide it in the **Enter Request Code** section of the **Smart License Reservation** tab of CSSM. The administrator can reserve a single license for call encryption from the list of all available licenses in the **Select Licenses** section before completing the license reservation.


If the Meeting Management is already registered with a virtual account that does not have an encryption license and is added later, then the user must re-register the Meeting Management for the changes to be applied. For more information on license reservation refer to [Meeting Management Administrator Guide](#).

2.5 Modifications in participant info card

From version 3.11, the **Close** button has been removed from the top-right corner of the Participant Info Card. Now, the card can be closed by clicking anywhere outside the card or by pressing the **Esc** key, improving the user experience.


2.6 On-screen messages via Meeting Management

From 3.11, Meeting Management administrators and/or video operators can broadcast on-screen messages to all the participants in an ongoing meeting. Both SIP and web app participants can view the on-screen messages and cannot be dismissed by the participants.


On the **Meetings** page, a new  **Message all** button is added, that allows administrators and video operators to customize the text, position, and duration of the on-screen message. Administrators and video operators must set the following three parameters while sending the message:

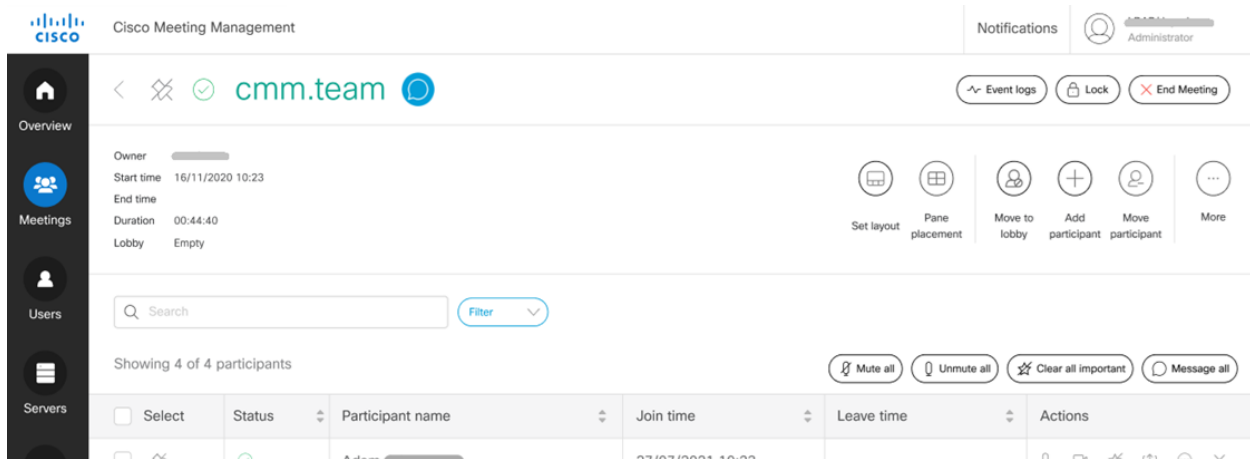
Parameter name	Parameter type	Parameter value	Default	Description
Enter Message	String	Free form text	None	The text box allows to enter the text to be displayed to all participants in the meeting. The message can include a maximum of 200 characters. Example - Weekly Meeting
Position	Drop-down options	Top, Middle, Bottom	Top	Allows to select the position to display the configured message on screen. Example - Top
Set Timer	Number	Time in seconds	0	Allows to enter time/duration in seconds to display the configured message on the participants' screens.

2.6.1 Points to note

- Administrators and video operators can send any number of messages, but only one message can be displayed at a time. The most recent message takes precedence.
- For administrators and video operators, the message button  (beside the meeting name) indicates the message is sent and is being displayed on the participants' screens. Hover the mouse on the icon to see the most recent message as a tool-tip. The icon is dismissed after the allotted time has elapsed.

2.6.2 UI modifications

On the **Meetings** page, on top of the participants table, the  **Message all** button has been added, which allows administrators and video operators to send on-screen messages.



The screenshot shows the Cisco Meeting Management interface. At the top, there is a navigation bar with the Cisco logo, 'Cisco Meeting Management', and a user profile for 'Administrator'. Below this is a meeting header for 'cmm.team' with a message icon. A toolbar contains buttons for 'Event logs', 'Lock', and 'End Meeting'. The main content area shows meeting details (Owner, Start time, End time, Duration, Lobby) and a list of participants. A search bar and a 'Filter' dropdown are present above the participants table. The participants table has columns for 'Select', 'Status', 'Participant name', 'Join time', 'Leave time', and 'Actions'. A 'Message all' button is located in the top right corner of the participants table.

Click  **Message all** to open the **Send message** pop-up window that includes the following parameters:

- Enter message:** The message that should be displayed on the participants' screen can be provided using the string parameter type. A Maximum of 200 characters are allowed in a message.
- Position:** Select positions (Top/Middle/Bottom) for the on-screen message. If no position is selected then **Top** will be set as the default option.
- Set timer:** Time in seconds for on-screen message.

Send message
✕

To: Everyone

Enter message

Position: Middle ▼

Set timer: 15 seconds


Cancel
Send

Meeting Management shows appropriate notifications when a message is successfully sent, fails, and if the message exceeds the 200-character limit.

2.7 Display IP address and device type in participant details

From version 3.11, Meeting Management administrators and video operators will be able to view the IP address and device information of the participants present in a meeting. This includes the device type and browser version used for joining the meeting. This information can be accessed from the participant information card.

For web app participants:



Adam Johnson ✎

adjohn@cisco.call.ciscospark.com

✕

Join time:	01/21/2025 11:35	CMS:	PreAlpha CMS 1000
Call type:	web app	IP address:	10.110.171.101
Direction:	Incoming	Device type:	Safari/18

For SIP participants:



Triangle Board55 
107719656@blrtmslab.com

Join time:	04/08/2025 12:18	CMS:	bpaidipa
Encryption:	None	IP address:	10.77.196.56
Call type:	SIP	Device name:	Triangle Board55
Direction:	Outgoing		

Meeting Server extracts these details from call details records or logs and will be available in read-only mode in Meeting Management. The device information is not dynamically updated during the call, except for when a participant reconnects after being disconnected. The device details are not updated if there is any change in IP address or device name due to manually changing name or VPN updation or browser update during the call.

The details are stored even after the participant leaves or ends the meeting. This applies to both SIP and web app participants. The browser name and version will be displayed for web app participants, and the device name will be displayed for participants joining from SIP endpoints. If the device name is not configured or not present at SIP endpoints, the SIP URI will be displayed instead of the device name.

2.8 Applying layouts for new participants

From version 3.11, Meeting Management administrators and video operators can assign layouts for the new participants joining an ongoing meeting. Previously, only connected participants could view the layouts set by the Meeting Management administrator and/or video operator. Any new participant joining the meeting after the layouts have been applied, or those who reconnect after being disconnected, could only see the default standard layout. They needed the administrator's and/or video operator's intervention to re-apply the required layout.

With this release, administrators can preset a layout for participants who are newly joining, and the same layout is applied to the placed participants who rejoin after getting disconnected from the meeting, providing a seamless experience.

This feature works for both SIP and web app participants. The layout set by a meeting participant on the web app will override the administrator's layout setting for that participant.

2.8.1 UI modifications

A new drop-down called **Select a screen layout for new participants** has been added to the **Change screen layout** pop-up window, which lists all the available Standard and Custom

layouts. The selection of this drop-down is optional. If a layout is not selected, then the layout defaults to **None**, and the newly joining participants will get the standard layout. If a layout is selected from the available list, the standard or custom layout selected will be applied for new participants joining the meeting. A new check-box called **Same as connected participants layout** is also added using which the administrators or video operators can apply the same layout that is selected for all connected participants to the new participants joining a meeting in one click, eliminating the need for manual scrolling of layouts using the drop-down.

Change screen layout
✕


Select a screen layout for new participants


Select layout ▼


 Same as connected participants layout


Select a screen layout for all connected participants


Standard layouts


Auto



Equal



Prominent



Overlay



Single


Custom layouts


Custom 1


Custom 2


Custom 3


Custom 4


Custom 5

[See more](#)

Cancel

Apply

Two new buttons, **Apply** and **Cancel**, have also been added. The **Apply** button allows the administrator and/or video operator to apply the updates made while selecting different layout options. The **Cancel** button cancels the changes without applying them.

2.8.2 Points to note

- The layout once selected for the new participants, will be retained till the meeting is in progress.
- If the layout is not selected or if the **None** option is selected for new participants, then the standard layout is applied for the new participants, even if a layout is applied for the meeting.
- In a cluster setup with multiple Meeting Management, the layout applied for new participants from a specific Meeting Management will be applied to all new participants joining the meeting throughout the cluster.

2.9 Applying pane placement for new participants

From 3.11, Meeting Management administrators and video operators can assign pane placement for the new participants joining an ongoing meeting. Previously, different pane placement arrangements, called models, were defined and applied for only connected participants in a meeting. Participants newly joining the meeting or who rejoined after getting disconnected from the meeting would not have any models applied and required the administrators to apply the models again.

From this release, administrators can preset a model for participants who are newly joining, and the same model is applied to the placed participants who rejoin after getting disconnected from the meeting. This eliminates the intervention of an administrator and/or video operator for applying the model every time a participant joins an ongoing meeting. New participants joining the meeting will view the same model as set by the administrator, thus allowing a seamless experience.

This feature works for both SIP and web app participants.

2.9.1 UI modifications

A new drop-down **Select a Pane Placement for new participants** has been added to the **Global Settings** in the **Pane Placement Configuration** pop-up window. It will be disabled unless the administrator and/or video operator create at least one pane placement model.

✕

Pane placement configuration

Global settings

Participants looking at their own pane will see Self-view

Select a pane placement for new participants Select pane placement model

Apply

Pane placement model

Add pane placement model

Model 1
 ✕

Model 2
 ✕

You can save max 3 pane placement models

Save

Select a layout for pane placement

Add participants to panes

⋮ Reserved. Add Participant ✕

⋮ Reserved. Add Participant ✕

⋮ Reserved. Add Participant ✕

⋮ Reserved. Add Participant ✕

⋮ Reserved. Add Participant ✕

+ Add another pane

Preview

1 Screen
 2 Screens

3	4	5	6
1		2	
7	8	9	10

Close

This drop-down allows:

- Administrator and/or video operator to select a model from the list of models configured using the **Pane placement model** section.
- The new participants to view selected model for pane placement.
- Administrator and/or video operator to select the **None** option to remove any model applied for new participants joining the meeting.

2.9.2 Points to note

- Pane Placement per Participant can be applied only to the connected participants in the meeting. When new participants join, they will view the model that an administrator or video operator has assigned using the **Select a Pane Placement for new participants** drop-down.
- When pane placement for new participants is not set or if the **None** option is selected in the **Select a Pane Placement for new participants** drop-down, then the new participants joining the meeting will have random pane placement applied, unless the administrator or video operator assign a model to such participants.
- In a cluster setup with multiple Meeting Management, the model applied for new participants from a specific Meeting Management will be applied to all new participants joining the meeting throughout the cluster.
- If pane placement for new participants and layout for new participants, both are applied to a meeting, pane placement for new participants takes precedence, and the new participants joining the meeting will view the layout selected in the pane placement model that is applied for new participants.
- Model selected for the new participants will be retained till the meeting is in progress unless an administrator and/or video operator modifies it.
- If the model applied for the new participants is deleted by the administrator or video operator, it will still be listed in the Pane placement for new participants drop-down with a deleted label.
- The following table will help in understanding the output applied for the new participant with various layout and pane placement settings:

Layout for new participant	Pane Placement for new participant	New participants will view
Set	Set	The layout selected in the Pane Placement Model.
Set	Not Set	The layout selected applied using layout for new participant drop-down.
Not Set	Set	The layout selected in the Pane Placement Model.
Not Set	Not Set	Standard layout.

2.10 Improvements in space creation

From 3.11, the video address generated using Meeting Management includes the space name and domain name. Previously, when creating a space, the video address generated consisted of random numbers and did not include the domain name.

Improvements have been made to restrict the creation of multiple spaces with the same space name and template. Error notifications are displayed accordingly.

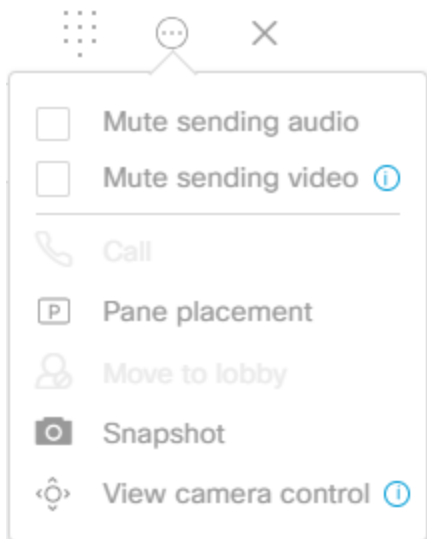
2.11 Far end camera control

From version 3.11, Meeting Management administrators and video operators can control far-end cameras of SIP participants in an ongoing meeting. This feature provides manual control over the participant's camera to move and reposition it around the participant for a greater focus.

This feature will require:

- The participant's camera to have Pan, Tilt, and Zoom (PTZ) capability.
- Snapshot license in Meeting Management.

The administrators can zoom in, zoom out, and position the camera to the left, right, up, and down on the participant's video. This feature is implemented by including a **View Camera Control** option within the **More** button. If this option is chosen and the snapshot license is not available in the Meeting Management, the administrator is notified with an appropriate message.



After clicking, the participant's video appears in a pop-up with camera controls (Zoom In, Zoom Out, Positioning - Left, Right, Up, and Down). The <, >, ^, and v buttons are used to modify camera position, while the + and - buttons are used to zoom in and out.



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.

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_11_0.zip`
- Name of upgrade image: `Cisco_Meeting_Management_3_11_0.img`
- MD5 checksum for upgrade image: `4d9ff9d91966e5c1688b35ec7fc78ad0`
- SHA256 checksum for upgrade image:
`0f3fcc9dd5f1cc95c02d66738a31e86721380aceb10ed179e06ca237bf2c2183`
- SHA512 checksum for upgrade image:
`4920c7f3996258553111b6790e7dd07c9b74150bdd934186b0595c2efbc962abdb3e832d9e1245712aa051285f3076eb6a7a9763f83736f4b3768a1df6967bb9`

OVA for new installation on vSphere 7.0:

- File name: `Cisco_Meeting_Management_3_11_0_vSphere-7_0.ova`
- MD5 checksum for image: `54d1bc1bbe2709c83bf50f29f274f5ec`
- SHA256 checksum for image:
`21865fc09ac7d89376e66012745a03285fe10f7d93b05a34cd9d23862665a74f`
- SHA512 checksum for image:
`982610ac22267f4cdf87b7ff5fb7f22bc19ea59b131aefa3f02b918350c550552e8d8d3b0c810a11623db530d099ad2e8f81a15148b3dfb5c8cc0a3f3ec431bd`

Note: This release of version 3.11 supports ESXi 8.0 U3d and ESXi 7.0 U3s.

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 3.9	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Management version 3.9.x is October, 2025.

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/). (<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
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.
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.

Reference	Issue
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 checkbox 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 3.11 (Build 3.11.0.40)

Reference	Issue
CSCwm05909	Space created on Meeting Management do not have the domain name in the video address.

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.

© 2025 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)