Cisco Meeting Server

Cisco Meeting Server Release 2.5.4

Release Notes

October 16, 2019

Contents

What's changed 4

1 Introduction 5
1.1 Interoperability with other Cisco products 6
1.2 Cisco Meeting Server platform maintenance 6
1.2.1 Cisco Meeting Server 1000 and other virtualized platforms 6
1.2.2 Cisco Meeting Server 2000 6
1.3 Interactive API Reference Tool 6
1.4 End Of Software Maintenance 7
1.5 Using the Cisco Expressway-E as the edge device in Meeting Server deployments . 7
1.6 Using the Cisco Expressway-C with the Meeting Server in the core network 10
1.6.1 Using the Cisco Expressway H.323 gateway component 11

2 New Features/Changes in version 2.5 12
2.1 New features introduced in version 2.5.4 12
2.1.1 Beta support for Yandex browser in WebRTC app 12
2.1.2 Joining options with no microphone or camera for WebRTC app 12
2.2 New features introduced in version 2.5.3 13
2.2.1 Additional browser support for WebRTC app 13
2.3 New features introduced in version 2.5.2 13
2.3.1 Additional browser support for WebRTC app 13
2.4 New features introduced in version 2.5.1 14
2.4.1 Additional browser support for WebRTC app 14
2.4.2 Important note about audio and video source selection 14
2.4.3 New Media Module Status field in the Web Admin interface 14
2.5 Hosting branding files locally 15
2.5.1 WebRTC App Customization 15
2.5.2 IVR Message, SIP/Lync Call Message and Invitation Text Customization 16
2.5.3 Limitations 17
2.5.4 Removing locally hosted branding files 17
2.5.5 Changing from web server (or default) branding to locally hosted branding . 18
2.5.6 Changing from locally hosted to web server branding: 18
2.5.7 Mixing locally hosted and web server customization 19
2.5.8 Testing customized invitation_template.txt 19
2.6 WebRTC App support using Safari on iOS and Microsoft Edge 19
2.6.1 Comparing features between the Cisco Meeting Apps 20

2.7 New serviceability features 20
2.8 Summary of MMP additions 21
2.9 Summary of API Additions & Changes 21
2.10 Summary of CDR Changes 21
2.11 Summary of Additions and Changes to Events 21

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 2.5 22
3.1 Upgrading to Release 2.5 22
3.2 Downgrading 24
3.3 Cisco Meeting Server 2.5 Deployments 25
3.3.1 Deployments using a single host server 25
3.3.2 Deployments using a single split server hosted on a Core server and an Edge server 26
3.3.3 Deployments for scalability and resilience 26

4 Bug search tool, resolved and open issues 27
4.1 Resolved issues 27
4.2 Open issues 31

Cisco Legal Information 34

Cisco Trademark 35

What's changed

Version	Change
2.5.4	"Resolved in 2.5.4" section updated. (Oct 16, 2019)
2.5.4	"Resolved in 2.5.4" section updated. (Oct 1, 2019)
2.5.4	Beta support for Yandex and new meeting join options introduced. (Sept 30, 2019) Added section "Resolved in 2.5.4". Hashes updated.
2.5.3	Additional browser support for WebRTC app introduced (April 25, 2019) Added section "Resolved in 2.5.3". Hashes updated.
2.5.2	Second maintenance release. (March 6, 2019) Support for Google Chrome 73 introduced. Added section "Resolved in 2.5.2". Hashes updated.
2.5.1	Note added on audio source selection in browsers. (February 18, 2019)
2.5.1	Section 4.1 and Section 4.2 updated. (January 28, 2019)
2.5.1	First maintenance release. (January 22, 2019) Support for Google Chrome 72 introduced. New Media Module status field introduced in the Web Admin. Added section "Resolved in 2.5.1". Hashes updated.
2.5.0	Minor corrections to upgrade section. (January 18,2019)
2.5.0	Added hyperlink to Feature Comparison Matrices mentioned in Section 2.6.1. (December 13, 2018)
2.5.0	New release of Cisco Meeting Server software. (December 12, 2018)

1 Introduction

These release notes describe the new features, improvements and changes in 2.5.4 of the Cisco Meeting Server software.

The Cisco Meeting Server software can be hosted on:

- the Cisco Meeting Server 2000, a UCS 5108 chassis with 8 B200 blades and the Meeting Server software pre-installed as the sole application.
- the Cisco Meeting Server 1000, a Cisco UCS server preconfigured with VMware and the Cisco Meeting Server installed as a VM deployment.
- the Acano X-Series hardware.
- or on a specification-based VM server. Note: From version 2.4, the Meeting Server software no longer supports Microsoft Hyper-V.

Throughout the remainder of these release notes, the Cisco Meeting Server software is referred to as the Meeting Server.

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

Note about certificate validation: From version 2.4, the Web Bridge correctly validates the XMPP Server's TLS certificate. If WebRTC app users have difficulty logging in after you upgrade the Meeting Server, then check that the uploaded XMPP certificate follows the advice in the Certificate Guidelines. Specifically, that the SAN field holds the domain name of the XMPP server. Prior to version 2.4 there were issues in XMPP certificate validation.

Note about Microsoft RTVideo: support for Microsoft RTVideo and consequently Lync 2010 on Windows and Lync 2011 on Mac OS, will be removed in a future version of the Meeting Server software.

Note about incoming calls: By default incoming calls are not allowed. To allow incoming calls to Cisco Meeting App users, set parameter **`canReceiveCalls=true`** for API object **`/user/profiles/<user profile id>`**.

Note about chat message board: For existing deployments that use chat message boards, chat will remain enabled when you upgrade to 2.5. Otherwise, you will need to use the API to create a callProfile with parameter **`messageBoardEnabled`** set to true.

1.1 Interoperability with other Cisco products

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.

1.2 Cisco Meeting Server platform maintenance

It is important that the platform that the Cisco Meeting Server software runs on is maintained and patched with the latest updates.

1.2.1 Cisco Meeting Server 1000 and other virtualized platforms

The Cisco Meeting Server software runs as a virtualized deployment on the following platforms:

- Cisco Meeting Server 1000
- specification-based VM platforms.

Note: From version 2.4, Cisco Meeting Server software no longer supports Microsoft Hyper-V virtualized deployments.

CAUTION: Irrespective of which virtualized platform is running the Cisco Meeting Server software, ensure the platform is up to date with the latest patches. Failure to maintain the platform may compromise the security of your Cisco Meeting Server.

1.2.2 Cisco Meeting Server 2000

The Cisco Meeting Server 2000 is based on Cisco UCS technology running Cisco Meeting Server software as a physical deployment, not as a virtualized deployment.

CAUTION: Ensure the platform (UCS chassis and modules managed by UCS Manager) is up to date with the latest patches, follow the instructions in the Cisco UCS Manager Firmware Management Guide. Failure to maintain the platform may compromise the security of your Cisco Meeting Server.

1.3 Interactive API Reference Tool

We recently introduced a new interactive API reference tool enabling you to see a high level view of the API objects and drill down to lower levels for the detail. There are also learning labs to help you get started, these will be added to over time. We encourage you to try out this tool; sometime in the future we will discontinue publishing the pdf version of the API Reference Guide.

https://developer.cisco.com/cisco-meeting-server/

Steps to use the tool:

1. Click **View the docs**

2. Select a category from the list in the left pane. For example: Call Related Methods.

3. Click on any method to see URI: GET/POST/PUT. Refer to the table of parameters and response elements with descriptions. For example: GET https://ciscocms.docs.apiary.io/api/v1/calls?

Note: If you are using a POST/PUT methods, the related 'Attributes' with descriptions appear on the right-hand pane when you select the method.

Learning labs

https://learninglabs.cisco.com/modules/cisco-meeting-server

The learning labs are intended as a starting point, covering a broad cross-section of what is possible with the Cisco Meeting Server API. Every learning lab is a step-by-step tutorial which takes you through the steps to complete the task from start to finish.

Example: The 'Setting up host and guest access with Cisco Meeting Server API' provides instructions to configure ways in which users can join meetings in a space with different options.

1.4 End Of Software Maintenance

On release of Cisco Meeting Server software version 2.5, Cisco announced the time line for the end of software maintenance for the software in Table 1.

Table 1: Time line for End Of Software Maintenance for versions of Cisco Meeting Server and Cisco Meeting App software

Cisco Meeting Server software version	End of Software Maintenance notice period
Cisco Meeting Server version 2.3.x	4 months after first release of Cisco Meeting Server version 2.5 (12th April 2019)
Cisco Meeting App version 1.10.x	4 months after first release of Cisco Meeting Server version 2.5 (12th April 2019)

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

1.5 Using the Cisco Expressway-E as the edge device in Meeting Server deployments

Over the previous few releases of Cisco Expressway software, edge features have been developed to enable the Cisco Expressway-E to be used as the edge device in Meeting Server deployments. Use the TURN server capabilities in Cisco Expressway-E to connect:

- participants using the WebRTC app to conferences hosted on the Meeting Server,
- remote Lync and Skype for Business clients to conferences hosted on the Meeting Server.

In addition, the Cisco Expressway-E can be used as a SIP Registrar to register SIP endpoints or to proxy registrations to the internal call control platform (Cisco Unified Communications Manager or Cisco Expressway-C).

Table 1 below indicates the configuration documentation that covers setting up Cisco Expressway-E to perform these functions. Table 3 below shows the introduction of the features by release.

Note: Cisco Expressway-E can not be used to connect remote Cisco Meeting App thick clients (Windows/Mac desktop or iOS) to conferences hosted on the Meeting Server. Nor can the Cisco Expressway-E be used between on premises Microsoft infrastructure and the Meeting Server. In deployments with on-premises Microsoft infrastructure and the Meeting Server, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization.

Note: If you are configuring dual homed conferencing between on-premises Meeting Server and on-premises Microsoft Skype for Business infrastructure, then the Meeting Server automatically uses the TURN services of the Skype for Business Edge.

Table 2: Documentation covering Cisco Expressway as the edge device for the Meeting Server

Edge feature	Configuration covered in this guide
Connect remote WebRTC apps	Cisco Expressway Web Proxy for Cisco Meeting Server Deployment Guide
Connect remote Lync and Skype for Business clients	Cisco Meeting Server with Cisco Expressway Deployment Guide
SIP Registrar or to proxy registrations to the internal call control platform	Cisco Expressway-E and Expressway-C Basic Configuration (X8.11)

Table 3: Expressway edge support for the Meeting Server

Cisco Expressway-E version	Edge feature	Meeting Server version
X8.11	Supported: - load balancing of clustered Meeting Servers, - Microsoft clients on Lync or Skype for Business infrastructure in other organizations, or Skype for Business clients on Office 365 (not "consumer" versions of Skype). - interoperability between on-premise Microsoft infrastructure and on-premise Meeting Server, **where no Microsoft calls traverse into or out of the organization.** - standards based SIP endpoints. - standards based H.323 endpoints. - Cisco Meeting App thin client (Web RTC app) using TCP port 443. Not supported: - off premise Cisco Meeting App thick clients (Windows/Mac desktop or iOS). - interoperability between on-premise Microsoft infrastructure and on-premise Meeting Server **where Microsoft calls traverse into or out of the organization**, in this scenario, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization. See Cisco Meeting Server with Cisco Expressway Deployment Guide (2.4/X8.11.4).	2.4
X8.10	Supported: - Microsoft clients on Lync or Skype for Business infrastructure in other organizations, or Skype for Business clients on Office 365 (not "consumer" versions of Skype), - standards based SIP endpoints, - Cisco Meeting App thin client (Web RTC app) using UDP port 3478 to connect to the Meeting Server via the Expressway reverse web proxy. Not supported: - load balancing of clustered Meeting Servers, - off premise Cisco Meeting App thick clients (Windows/Mac desktop or iOS) or Cisco Meeting App thin client (Web RTC app) using TCP port 443, - interoperability between on premises Microsoft infrastructure and Meeting Server; in this scenario, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization. See Cisco Expressway Web Proxy for Cisco Meeting Server	2.3

Cisco Expressway-E version	Edge feature	Meeting Server version
X8.9	Supported: - Microsoft clients on Lync or Skype for Business infrastructure in other organizations, or Skype for Business clients on Office 365 (not "consumer" versions of Skype), - standards based SIP endpoints. Not supported: - load balancing of clustered Meeting Servers,, - off-premise Cisco Meeting App thick clients (Windows/Mac desktop or iOS) and Cisco Meeting App thin client (WebRTC app), - interoperability between on premises Microsoft infrastructure and Meeting Server; in this scenario, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization See Cisco Expressway Options with Meeting Server and/or Microsoft Infrastructure	2.2

You are encouraged to migrate your Meeting Server deployments from using the Meeting Server edge components to using the Expressway X8.11 (or later) TURN server. The SIP edge, TURN server, internal Firewall and H.323 gateway components will be removed from the Meeting Server software at some point in the future

1.6 Using the Cisco Expressway-C with the Meeting Server in the core network

In addition to deploying Cisco Expressway-E at the edge of the network, Cisco Expressway-C can be deployed in the core network with the Meeting Server. If deployed between the Meeting Server and an on-premises Microsoft Skype for Business infrastructure, the Cisco Expressway-C can provide IM&P and video integration. In addition the Cisco Expressway-C can provide the following fuctionality:

- a SIP Registrar,
- an H.323 Gatekeeper,
- call control in Meeting Server deployments with Call Bridge groups configured to load balance conferences across Meeting Server nodes.

Table 4:Additional documentation covering Cisco Expressway-C and the Meeting Server

Feature	Configuration covered in this guide
Call control device to load balance clustered Meeting Servers	Cisco Meeting Server 2.4+, Load Balancing Calls Across Cisco Meeting Servers
SIP Registrar	Cisco Expressway-E and Expressway-C Basic Configuration (X8.11)

Feature	Configuration covered in this guide
H.323 Gatekeeper	Cisco Expressway-E and Expressway-C Basic Configuration (X8.11)

Note: When planning the dial plan on Expressway, each Meeting Server in a cluster requires its own neighbour zone on the Cisco Expressway. For more information see Appendix A in the white paper Load Balancing Calls Across Cisco Meeting Servers.

1.6.1 Using the Cisco Expressway H.323 gateway component

In line with Cisco's goal of a single Edge solution across the Cisco Meeting Server and Cisco Expressway, Cisco plans to end of life the Meeting Server H.323 Gateway component. From version 2.4 of the Meeting Server software, there will be no further bug fixes for the H.323 Gateway component. The H.323 component will be removed from the Meeting Server software in a future release. Customers are encouraged to start evaluation of the more mature H.323 Gateway component in the Cisco Expressway, and plan their migration over.

Any H.323 endpoints registered to Expressway-E or Expressway-C will not consume Rich Media Session (RMS) licenses when calling into the Cisco Meeting Server from Expressway version X8.10 onwards.

2 New Features/Changes in version 2.5

Version 2.5 of the Meeting Server software adds the following:

- host branding files locally on the Meeting Server, rather than using a separate web server,
- additional browser support for the WebRTC app,
- a couple of features improving serviceability which will help Cisco Support in diagnosing Meeting Server issues,
- a new MMP command that allows specific pre-release features to be switched on and off.

In addition, support for more video streams over distribution links, first previewed in version 2.3, is still a preview feature. The feature creates a more consistent video experience from remote single, dual and three screen end point systems

You are advised not to use beta (or preview) features in a production environment. Only use them in a test environment until they are fully released.

Note: Cisco does not guarantee that a beta or preview feature will become a fully supported feature in the future. Beta features are subject to change based on feedback, and functionality may change or be removed in the future.

Note: The term spaces is used throughout the documentation apart from the API guide which still uses the old terminology of coSpaces.

2.1 New features introduced in version 2.5.4

2.1.1 Beta support for Yandex browser in WebRTC app

Version 2.5.4 introduces Beta support for Cisco Meeting App for WebRTC using Yandex browsers on Windows. This is beta quality in current version.

2.1.2 Joining options with no microphone or camera for WebRTC app

Version 2.5.4 introduces some new joining call options.

While joining a meeting, you can now choose 'no camera' or 'no microphone' from the **Joining options** screen. This can be useful if you have a faulty camera or microphone and you can see and hear other participants in the call, but other participants cannot see or hear you.

Note: We do not recommend changing options during a meeting.

To add a camera or a microphone whilst you are in a meeting:

1. Click **Back** to navigate to the main screen. You will still be in the meeting.
2. Click on  to open the **Settings** screen. Select a camera and microphone from the options shown.
3. Click **Return to meeting** to return to the in-meeting screen and continue your meeting with the new options selected.

2.2 New features introduced in version 2.5.3

2.2.1 Additional browser support for WebRTC app

Version 2.5.3 introduces support for Cisco Meeting App for WebRTC using:

- Apple Safari on iOS 12.3
- Apple Safari 12.2 on macOS
- Mozilla Firefox 68

All these browsers are currently in beta (at time of first publication).

See Cisco Meeting App WebRTC Important Information for the latest browser support details.

2.3 New features introduced in version 2.5.2

2.3.1 Additional browser support for WebRTC app

Version 2.5.2 introduces support for Cisco Meeting App for WebRTC using Google Chrome version 73.

The expected release date for this version of Chrome is March 12th, 2019. Meeting Server must be upgraded to version 2.5.2 otherwise sharing presentation on WebRTC calls on Meeting Server using Google Chrome, as described below, will not work after updating Chrome to version 73 or above, if the camera permissions are not granted.

For more information, see the Software Advisory notice here and the Bug Search details for CSCvo51143.

Table 5:Cisco Meeting Server support for Google Chrome

Cisco Meeting Server software version	Validated Google Chrome versions
2.5.2	72 and 73 beta

Impact of Chrome 73 on versions earlier than Meeting Server 2.5.2

- When using the WebRTC app on Chrome browser version 73, joining a meeting/call can fail if used in the 'Management and Presentation' mode, and
- If a user has previously blocked the Camera and Microphone permissions, or cannot grant them, they will be impacted if using Chrome 73.

However, if the user has previously granted permission to the browser whilst using the WebRTC app to use the Camera and Microphone, they will **not** be impacted by Chrome 73. The WebRTC app prompts for these permissions the first time a user tries to join a meeting except in cases where they chose to join using the 'Management and Presentation' mode.

2.4 New features introduced in version 2.5.1

2.4.1 Additional browser support for WebRTC app

Version 2.5.1 introduces support for the WebRTC app using Google Chrome version 72.

The expected release date for this version of Chrome is January 29th, 2019. Meeting Server **must** be upgraded to version 2.5.1 otherwise Chrome users will not be able to use the WebRTC app once version 72 is released.

Table 6:Cisco Meeting Server support for Google Chrome

Cisco Meeting Server software version	Validated Google Chrome versions
2.5.1	71 and 72 beta

2.4.2 Important note about audio and video source selection

Camera and microphone selection in the browsers is not very reliable, so we recommend using the Operating System's audio source selection instead of the browser's. We also recommend changing options before a call rather than during the call. To ensure reliability, speaker selection via the browser was removed from WebRTC app in Meeting Server version 2.5.1.

2.4.3 New Media Module Status field in the Web Admin interface

Version 2.5.1 introduces a new field for **Media module status** on the Status page (**System > General**). This field shows the number and status of media modules that are operational on the Meeting Server. For example:

- VM: 1/1
- X-series X1: 1/1
- X-series X2: 5/5

- X-series X3: 11/11
- CMS 2K: 7/7

2.5 Hosting branding files locally

Note: Hosting branding files locally on Acano X Series servers is beta quality in 2.5.x.

Prior to version 2.5, using branding files for the Meeting Server required you to configure a separate web server to hold the branding files (voice prompts and lobby screen branding assets). From version 2.5 one set of branding files can be held locally on the Meeting Server. These locally hosted branding files are available to the Call Bridge and Web Bridge once the Meeting Server is operational, removing the risk of delays in applying customization due to problems with the web server. The images and audio prompts replace the equivalent files built into the Meeting Server software; during start up, these branding files are detected and used instead of the default files. Locally hosted branding files are overridden by any remote branding from a web server.

You can change these locally hosted files simply by uploading a newer version of the files and restarting the Call Bridge and Web Bridge. If you remove the locally hosted files, the Meeting Server will revert to using the built-in (US English) branding files after the Call Bridge and Web Bridge have been restarted, providing a web server has not been set up to provide the branding files.

Note: To use multiple sets of branding files, you still need to use an external web server.

2.5.1 WebRTC App Customization

The branding files for the WebRTC app are held within an archive (zip) file, from version 2.5 this zip file can be locally hosted on the Meeting Server. If you are changing from using a web server to hosting the files locally then follow the guidance in Section 2.5.7 before following the steps below.

The following steps provide an overview of the customization procedure, for a detailed procedure refer to the Customization Guidelines.

Note: The commands in the following steps are for console/terminal environments (i.e. command prompt or terminal) and not for SFTP clients such as WinSCP.

1. Create a zip archive file named **`web_branding.zip`** containing these files:
   - sign_in_settings.json
   - sign_in_logo.png

- sign_in_background.jpg

Note: This zip file must be named **web_branding.zip**, it cannot have a different filename.

2. For each Meeting Server with an enabled Web Bridge which will locally host this zip archive:
   a. Connect your SFTP client to the IP address of the MMP.
   b. Log in using the credentials of the MMP admin user.
   c. Upload the zip file **web_branding.zip**. For example:
      ```
      PUT web_branding.zip
      ```
   d. Connect your SSH client to the IP address of the MMP.
   e. Log in using the credentials of the MMP admin user.
   f. Restart the Web Bridge
      ```
      webbridge restart
      ```

The new branding will be picked up after the restart. The Web Bridge retrieves the locally hosted branding file for the WebRTC app, rather than relying on the Call Bridge to pass the file.

Note: For branding files held on a web server, there is no change in how the branding files are handled; the Call Bridge will continue to retrieve the archive file from the web server and push it to the Web Bridge.

2.5.2 IVR Message, SIP/Lync Call Message and Invitation Text Customization

If you are changing from using a web server to hosting the files locally then follow the guidance in Section 2.5.7 before following the steps below.

To locally host the IVR messages , SIP/Lync call messages and invitation text you need to create a Call Bridge branding zip file.

The following steps provide an overview of the customization procedure, for a detailed procedure refer to the Customization Guidelines.

1. Create the call branding zip file, this file must be named **call_branding.zip** to ensure it is processed correctly.
   a. Create a single folder with the files listed in Chapter 3 of the Customization Guidelines, these are the same files that are used if a web server is deployed.

      Note: In locally hosted branding, only **background.jpg** will be used for the call background and ivr background images; **passcode_background.jpg**, **passcode_or_blank_required_background.jpg**, **passcode_or_blank_timeout_ background.jpg**, **deactivated_background.jpg** and **ivr_background.jpg** are ignored.

b. Add the file **invitation_template.txt** containing the invitation text to the folder, as described in Chapter 4 of the guidelines .

Note: For this call branding zip file, you must use the filename **invitation_template.txt** even if you are already using a different filename on a web server.

c. Zip up the files in the folder, all files should be at the top level of the zip file (no folders nested in the zip file), the filename must be **call_branding.zip**.

2. Install the IVR, call and invitation customization on every Call Bridge. For each Meeting Server:
   a. Connect your SFTP client to the IP address of the MMP.
   b. Log in using the credentials of the MMP admin user.
   c. Upload the zip file **call_branding.zip**. For example:
      ```
      PUT call_branding.zip
      ```
   d. Connect your SSH client to the IP address of the MMP.
   e. Log in using the credentials of the MMP admin user.
   f. Restart the Call Bridge
      ```
      callbridge restart
      ```

The new branding will be picked up after the restart.

2.5.3 Limitations

- Only one background image file, **background.jpg**, is used in locally hosted branding, other image files will be ignored.
- If you want different image backgrounds in different situations, for example during pass code entry or IVR, the only way is to use a web server for customization as described in the Customization Guidelines.
- To use multiple sets of branding files, you still need to use an external web server.

Note: If files are too large, missing or otherwise invalid then they will be treated in the same way as their web server equivalents and will not be used. There will be no attempt to fall back to default resources. Any missing audio prompts are simply not played, and an invalid or omitted background.jpg file is replaced with a solid black background.

2.5.4 Removing locally hosted branding files

Follow these steps for each Meeting Server hosting local branding files.

1. Connect your SFTP client to the IP address of the MMP.
2. Log in using the credentials of the MMP admin user.
3. Remove the locally hosted branding files from the Web Bridge
   `RM web_branding.zip`
4. Remove the locally hosted branding files from the Call Bridge
   `RM call_branding.zip`
5. Connect your SSH client to the IP address of the MMP.
6. Log in using the credentials of the MMP admin user.
7. Restart the Web Bridge
   `webbridge restart`
8. Restart the Call Bridge
   `callbridge restart`

2.5.5 Changing from web server (or default) branding to locally hosted branding

If changing from web server (or default) branding to locally hosted branding, follow these recommendations:

- for every Call Bridge ensure:
  - the **`resourceLocation`** parameter for the IVR messages is not set; use a PUT method to set the **`resourceLocation`** parameter as blank on **`/ivrBrandingProfile/<ivr branding profile id>`**,
  - the **`resourceLocation`** parameter for the call messages is not set; use a PUT method to set the **`resourceLocation`** parameter as blank on **`/callBrandingProfile/<call branding profile id>`**,
  - the **`invitationTemplate`** parameter for the call messages is not set; use a PUT method to set the **`invitationTemplate`** parameter as blank on **`/callBrandingProfile/<call branding profile id>`**.
- for every Call Bridge which has a configured Web Bridge, make sure the **`resourceArchive`** field is not set in that configuration; use the PUT method to set the **`resourceArchive`** parameter as blank on API object **`/webBridges/<web bridge id>`**.
- stop using web server URLs in scripts and configurations of call leg profiles,
- configure **`call_branding.zip`** files on every Call Bridge, as described above,
- configure **`web_branding.zip`** files on every Web Bridge, as described above.

2.5.6 Changing from locally hosted to web server branding:

If changing from locally hosted to web server branding, then follow these recommendations:

- remove locally hosted **`call_branding.zip`** files from every Call Bridge as described above,
- remove locally hosted **`web_branding.zip`** files from every Web Bridge as described above,
- change all your scripts and configurations to use http://mywebserver/... as documented in the Customization Guidelines.

2.5.7 Mixing locally hosted and web server customization

If you install branding zip files on your Meeting Servers, but also deploy a web server and use it to serve branding resource files, then note the following:

For IVR, call and invitation customization:

- customization using the web server will override the locally hosted files,
- leaving the API fields blank or unset will cause the locally hosted files to be used.

For WebRTC customization:

- customization using the web server will override the locally hosted files
- it is possible to configure the same Web Bridge in the configuration of more than one Call Bridge. In this case, a configured resource archive from a Call Bridge on another Meeting Server may override the locally hosted branding file for a Web Bridge. Because this might be unexpected, we recommend NOT mixing the two configurations.

2.5.8 Testing customized **`invitation_template.txt`**

The invitation template is delivered from the Meeting Server to Cisco Meeting App clients and cached locally, so after customization on the Meeting Server there may be a delay before clients begin to use the new text. Logging the client out and in again should fetch the new version immediately, but any clients which stay logged in will not see the new text until their cache times out.

From version 2.5, this delay has been reduced to at most 1 hour. For clients which have cached text from a Meeting Server running an older version, the delay could be as much as 24 hours in the worst case.

2.6 WebRTC App support using Safari on iOS and Microsoft Edge

Prior to version 2.5, the only supported browsers for the WebRTC app for Cisco Meeting App were:

- Google Chrome (Windows, macOS and Android) version 66 or later,
- Mozilla Firefox (Windows and macOS) version 60 or later.
- Apple Safari for macOS version 11.1 or later.

The WebRTC app enables users to:

- participate in video and audio conferences hosted on a Meeting Server or in dual homed conferences,
- pair with SIP endpoints,
- receive and share a presentation.

Version 2.5 supports additional browsers, these are:

- Safari on iOS for iPads, running the latest version of iOS (recommended). iOS 11.0 is the minimum supported release.
- Safari on iOS for iPhones, running the latest version of iOS (recommended). iOS 11.0 is the minimum supported release. (This is beta quality in version 2.5.x).

  Note: We have tested the WebRTC app using the Safari browser on iPad Air 2 and iPad Pro 12.9 inch (2nd generation) with iOS 11.4.1, iPad (6th generation) with iOS 12.0.1, iPhone 6 on iOS12, iPhone 7 on iOS 12 and 12.1, iPhone 8 Plus on iOS12 and 12.1, and iPhone X on iOS 11.4.1.

- the latest version of Microsoft Edge (Microsoft Edge 42/Microsoft EdgeHTML 17) on Microsoft Windows 10 (this is beta quality in version 2.5.x).

  Note: There are limitations using the WebRTC app with Microsoft Edge and Mozilla FireFox browsers:

  - Using the WebRTC app with Microsoft Edge will not work if using the TURN server in Cisco Expressway or using the Meeting Server TURN with TCP.
  - Using the WebRTC app with Firefox will not work if using the TURN server in Cisco Expressway with TCP, but will work with the Meeting Server TURN with TCP.

  See Cisco Meeting App WebRTC Important Information for further details on these and other limitations.

2.6.1 Comparing features between the Cisco Meeting Apps

There are two Feature Comparison Matrix, one for Cisco Meeting App version 1.11 comparing the features available across the Desktop (Windows and macOS), iOS and WebRTC platforms, the other for the WebRTC app for Cisco Meeting App comparing features across supported web browsers.

2.7 New serviceability features

These serviceability features will help Cisco Support in diagnosing Meeting Server issues. The improvements include:

- a mechanism for identifying which syslog messages belong to the same SIP connection. The identification can be undertaken manually or by writing a script.
- a method to easily determine which log message belongs to which call/conference.

Neither of these serviceability features are intended for use by customers, however Cisco Support may request syslogs from a customer, and will use these new features to determine any issues.

2.8 Summary of MMP additions

These additional MMP commands in version 2.5 should not be used unless under instruction from Cisco Support or Cisco EFT, no features in version 2.5.4 require switching on.

Command	Description
webbridge options <feature_name1 feature_name2>	Switches on the specified features, if more than one feature is to be enabled then separate the feature_names with a space. Only use this command under instruction from Cisco Support or Cisco EFT. These features are not suitable for production use. The features will remain enabled across reboots, but will be automatically cleared when using the upgrade command
webbridge options none	Switches off all features that were previously switched on using the **webbridge options <feature_name>** command. Only use under instruction from Cisco Support or Cisco EFT.

2.9 Summary of API Additions & Changes

There are no new additions or changes to the API objects or parameters for version 2.5.

2.10 Summary of CDR Changes

There are no new CDR records or parameters for version 2.5.

2.11 Summary of Additions and Changes to Events

There are no new additions or changes to the Events for version 2.5.

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 2.5

This section assumes that you are upgrading from Cisco Meeting Server software version 2.4. If you are upgrading from an earlier version, then Cisco recommends that you upgrade to 2.4 first following the instructions in the 2.4.x release notes, before following any instructions in these Cisco Meeting Server 2.5 Release Notes. This is particularly important if you have a Cisco Expressway connected to the Meeting Server.

Note: Cisco has not tested upgrading from a software release earlier than 2.4.

To check which version of Cisco Meeting Server software is installed on a Cisco Meeting Server 2000, Cisco Meeting Server 1000, or previously configured VM deployment, use the MMP command **`version`**.

If you are configuring a VM for the first time then follow the instructions in the Cisco Meeting Server Installation Guide for Virtualized Deployments.

3.1 Upgrading to Release 2.5

The instructions in this section apply to Meeting Server deployments which are not clustered. For deployments with clustered databases read the instructions in this FAQ, before upgrading clustered servers.

CAUTION: Before upgrading or downgrading Meeting Server you must take a configuration backup using the **`backup snapshot <filename>`** command and save the backup file safely on a different device. See the MMP Command Reference document for full details. Do **not** rely on the automatic backup file generated by the upgrade/downgrade process as it may be inaccessible in the event of a failed upgrade/downgrade.

Upgrading the firmware is a two-stage process: first, upload the upgraded firmware image; then issue the upgrade command. This restarts the server: the restart process interrupts all active calls running on the server; therefore, this stage should be done at a suitable time so as not to impact users – or users should be warned in advance.

To install the latest firmware on the server follow these steps:

1. Obtain the appropriate upgrade file from the software download pages of the Cisco website:

   `Cisco_Meeting_Server_2_5_4_CMS2000.zip`

This file requires unzipping to a single upgrade.img file before uploading to the server. Use this file to upgrade Cisco Meeting Server 2000 servers.

Hash (SHA-256) for upgrade.img file:
f6cca939e556796eca0ca333d4236c09a188b13fd48899cca1ae76155c45a973

`Cisco_Meeting_Server_2_5_4_vm-upgrade.zip`

This file requires unzipping to a single upgrade.img file before uploading to the server. Use this file to upgrade a Cisco Meeting Server virtual machine deployment.

Hash (SHA-256) for upgrade.img file:
fd129757f954d9d76c08dbd6f042d7d0c648bc790b1add9cd03ba6198ec9de28

`Cisco_Meeting_Server_2_5_4_x-series.zip`

This file requires unzipping to a single upgrade.img file before uploading to the server. Use this file to upgrade Acano X-series servers.

Hash (SHA-256) for upgrade.img file:
695ce0f2654cbe6dbd49289dbd5f321b21bcced9896c834ef1efcb3e4af50f31

`Cisco_Meeting_Server_2_5_4.ova`

Use this file to deploy a new virtual machine via VMware.

For vSphere6, hash (SHA-512) for Cisco_Meeting_Server_2_5_4_vSphere-6_0.ova file:
a096b89396f90a4e18becb77f0882949bd4836b1744444572b0f6e22db1058816d944e1fadd821ea62a483603053c1ee1dfe93d45950f771a54a300440a6eba3

For vSphere6.5 and higher, hash (SHA-512) for Cisco_Meeting_Server_2_5_4_vSphere-6_5.ova file:
774a5a492fd2d8f3d2cc45d905f6550bec7139f6f7f8fcb5563eecffecf379334ead00caa9fdc0dd1773a05887cce1b9b22b352f28cd437cb4988667d3b27a31

2. To validate the OVA file, the checksum for the 2.5.4 release is shown in a pop up box that appears when you hover over the description for the download. In addition, you can check the integrity of the download using the SHA-512 hash value listed above.
3. Using an SFTP client, log into the MMP using its IP address. The login credentials will be the ones set for the MMP admin account. If you are using Windows, we recommend using the WinSCP tool.

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

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

---

4. Copy the software to the Server/ virtualized server.
5. To validate the upgrade file, issue the **`upgrade list`** command.

a. Establish an SSH connection to the MMP and log in.
b. Output the available upgrade images and their checksums by executing the upgrade list command.

   upgrade list
c. Check that this checksum matches the checksum shown above.

6. To apply the upgrade, use the SSH connection to the MMP from the previous step and initiate the upgrade by executing the **upgrade** command.
   a. Initiate the upgrade by executing the upgrade command.
      upgrade
   b. The Server/ virtualized server restarts automatically: allow 10 minutes for the process to complete.
7. Verify that the Meeting Server is running the upgraded image by re-establishing the SSH connection to the MMP and typing:
   version
8. Update the customization archive file when available.
9. If you are deploying a scaled or resilient deployment read the Scalability and Resilience Deployment Guide and plan the rest of your deployment order and configuration.
10. If you have deployed a database cluster, be sure to run the **database cluster upgrade_schema** command after upgrading. For instructions on upgrading the database schema refer to the Scalability and Resilience Deployment Guide.
11. You have completed the upgrade.

3.2 Downgrading

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

1. Copy the software to the Server/ virtualized server.
2. To apply the downgrade, use the SSH connection to the MMP and start the downgrade by executing the **upgrade <filename>** command.

   The Server/ virtualized server will restart automatically – allow 10-12 minutes for the process to complete and for the Web Admin to be available after downgrading the server.
3. Log in to the Web Admin and go to **Status > General** and verify the new version is showing under **System status**.
4. Use the MMP command **factory_reset app** on the server and wait for it to reboot from the factory reset.

5. Restore the configuration backup for the older version, using the MMP command **`backup rollback <name>`** command.

   Note: The **`backup rollback`** command overwrites the existing configuration as well as the license.dat file and all certificates and private keys on the system, and reboots the Meeting Server. Therefore it should be used with caution. Make sure you copy your existing cms.lic file and certificates beforehand because they will be overwritten during the backup rollback process. The .JSON file will not be overwritten and does not need to be re-uploaded.

   The Meeting Server will reboot to apply the backup file.

   For a clustered deployment, repeat steps 1-5 for each node in the cluster.

6. In the case of XMPP clustering, you need to re-cluster XMPP:
   a. Pick one node as the XMPP master, initialize XMPP on this node
   b. Once the XMPP master has been enabled, joining any other XMPP nodes to it.
   c. Providing you restore using the backup file that was created from the same server, the XMPP license files and certificates will match and continue to function.
7. Finally, check that:
   - the Web Admin interface on each Call Bridge can display the list of coSpaces.
   - dial plans are intact,
   - XMPP service is connected
   - no fault conditions are reported on the Web Admin and log files.
   - you can connect using SIP and Cisco Meeting Apps (as well as Web Bridge if that is supported).

   The downgrade of your Meeting Server deployment is now complete.

3.3 Cisco Meeting Server 2.5 Deployments

To simplify explaining how to deploy the Meeting Server, deployments are described in terms of three models: the single combined Meeting Server, the single split Meeting Server and the deployment for scalability and resilience. All three different models may well be used in different parts of a production network.

3.3.1 Deployments using a single host server

If you are deploying the Meeting Server as a single host server (a “combined” deployment), we recommend that you read and follow the documentation in the following order:

1. Appropriate Installation Guide for your Cisco Meeting Server (Cisco Meeting Server 2000, Cisco Meeting Server 1000 and virtualized deployments, or the installation guide for Acano X-Series Server).
2. The Single Combined Meeting Server Deployment Guide enabling all the solution components on the single host. This guide refers to the Certificate Guidelines for Single Combined Server Deployments for details on obtaining and installing certificates for this deployment.

Note: The Cisco Meeting Server 2000 only has the Call Bridge, Web Bridge, XMPP server and database components. It can be deployed as a single server on an internal network, but if a deployment requires firewall traversal support for external Cisco Meeting App clients, then TURN server and Load Balancer edge components need to be deployed on a separate Cisco Meeting Server 1000 or specification-based VM server - see the" single split" deployment below.

3.3.2 Deployments using a single split server hosted on a Core server and an Edge server

If you are deploying the Meeting Server in a split server model, we recommend that you deploy the XMPP server on the Core server, and deploy the Load Balancer on the Edge server.

Read and follow the documentation in the following order:

1. Appropriate Installation Guide for your Cisco Meeting Server
2. The Single Split Meeting Server Deployment Guide. This guide refers to the Certificate Guidelines for Single Split Server Deployments for details on obtaining and installing certificates for this deployment.

3.3.3 Deployments for scalability and resilience

If you are installing the Meeting Server for scalability and resilience using multiple host servers, we recommend that you deploy the XMPP server on Core servers, and deploy Load Balancers on the Edge server.

Read and follow the documentation in the following order:

1. Appropriate Installation Guide for your Cisco Meeting Server
2. The Scalability and Resilience Deployment Guide. This guide refers to the Certificate Guidelines for Scalable and Resilient Server Deployments for details on obtaining and installing certificates for this deployment.

4 Bug search tool, resolved and open issues

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

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

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

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

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

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

   or,

   in the **Product** field select **Series/Model** and start typing **`Cisco Meeting Server`**, then in the **Releases** field select **Fixed in these Releases** and type the releases to search for example **`2.5.4`**.
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.

4.1 Resolved issues

Issues seen in previous versions that are fixed in 2.5.4

Cisco identifier	Summary
CSCvq19622	This issue has been filed to evaluate the product against the vulnerability released by the Netflix on June 17th affecting FreeBSD and Linux kernels, identified by CVE IDs: - CVE-2019-11477: SACK Panic - CVE-2019-11478: SACK Slowness or Excess Resource Usage - CVE-2019-11479: Excess Resource Consumption Due to Low MSS Values Cisco has reviewed this product and concluded that it is affected by this vulnerability as it contains a vulnerable version of Linux Kernel.
CSCvq24159	On Meeting Server 2000, some media modules are failing after a reboot / upgrade or callbridge restart.
CSCvq30379	Calls into a conference featuring no other local participants do not result in distribution links being created to other call bridges that do have active participants for the conference in other regions.

Cisco identifier	Summary
CSCvp06073	When a presentation is shared from WebRTC when using the 'Management and Presentation' joining method, the negotiated bandwidth for the presentation stream is capped which leads to poor quality being seen by the receivers.
CSCvo91844	Degraded audio may occur on a fully loaded Meeting Server with many audio participants.
CSCvo10678	In a distributed call with recording started, whenever the distributed call is dropped, the recording/streaming is stopped, even though there are participants remaining in the conference.
CSCvq11136	When cross launching to a native Meeting App client (desktop or iOS) when a language other than English is set, the message "You are no longer in the meeting" equivalent is displayed in the browser.
CSCvq39444	When a guest user joins and the default camera is not working the user gets redirected to a 'Could not join meeting' page and then back to the webbridge landing page shortly after.
CSCvq84608	A splash screen momentarily displays (< 1 second) on the upper left video pane when a participant joins a conference. This occurs so quickly that the newly joined participant may not notice it.
CSCvq14738	When Guest and Host profiles are set up such that one URI is used to invoke Guest mode and a different URI for Host mode on a given space, the conference activation doesn't work as intended.
CSCvp64154	Occasionally the peer link call leg does not present and so participants hosted on different Call bridges in a cluster cannot see and hear each other.

Issues seen in previous versions that are fixed in 2.5.3

Cisco identifier	Summary
CSCvp29391	WebRTC calls on Meeting Server using Apple Safari will not work after updating to Apple Safari on iOS 12.3 or later, and Apple Safari 12.2 on macOS and later.
CSCvp37201	WebRTC calls on Meeting Server using Mozilla Firefox will not work after updating to version 68.
CSCvp33496	On WebRTC app, Input Method Editors (IME) not submitting fields correctly on Internet Explorer.
CSCvp38323	Frozen video seen on some Skype for Business participants when Meeting Server sends dual video streams to an AVMCU conference.
CSCvo82633	Occasionally the Recorder does not record for SIP calls when the CallProfile is set to Automatic

Cisco identifier	Summary
CSCvp12123	Meeting Server's Callbridge component may restart unexpectedly when a SIP participant joins a conference whilst Skype for Business content share is in progress
CSCvp38354 and CSCvp38536	In rare circumstances, Meeting Server 2000's Callbridge component may restart unexpectedly when under heavy load.
CSCvp12120	Meeting Server 2000, Media modules may report "presumed lost: no response to ping" or "media modules now not responding" under heavy call load.
CSCvp12118	Frozen video seen on some Skype for Business participants when Cisco Meeting Server sends dual video streams to an AVMCU conference.
CSCvn63172	On rare occasions, temporary poor video quality can be seen on immersive systems (TX9000 or IX5000) connected to a Meeting Server.
CSCvk22499	In rare circumstances, Meeting Server's Callbridge component may restart unexpectedly when a participant joins a meeting.
CSCvp13683	Currently the 'Join Meeting' button is greyed out and not in use when using the 'Open Cisco Meeting App' tab. This button can cause confusion for a guest as they could think they need to do something before being able to join the meeting with Meeting App.
CSCvo31960	WebRTC app (using Google Chrome) is unable to update input video source and join the meeting.
CSCvo24717	When joining a space from a Skype for Business client via the IVR, no video is seen on the Skype for Business client.
CSCvp56060	Improvements to call connection times under high load conditions.

Issues seen in previous versions that are fixed in 2.5.2

Cisco identifier	Summary
CSCvo51143	Support for the WebRTC app using Google Chrome version 73. See New features introduced in 2.5.2 for further information.
CSCvo60648	MMP commands not functioning, resulting in inability to perform a PKI Inspect as well as inability to gather log bundles etc.
CSCvo17329	Cisco Meeting Server can become overloaded if audio-only calls are used. This is due to increased media processing load on distributed peer link calls for coSpaces with audio-only participants.
CSCvo56197	Guest participants joining a Meeting Server conference may be left at the lobby screen even after a host participant has already joined the conference.
CSCvo37179	Unable to remove or overwrite a local branding file call_branding.zip from the Meeting Server.

Cisco identifier	Summary
CSCvn63372	When two endpoints join a conference hosted on the Meeting Server, the padlock icon showing that the call is encrypted disappears from the first endpoint when the second endpoint joins, even though the conference is encrypted.
CSCvm93493	Chat does not work on one webbridge part of a cluster when using the guest WebRTC join path.
CSCvn00288	During call replacing with VCS, the display name of the replaced call is not retained and the SIP URI is rendered instead.
CSCvo13844	WebRTC client occasionally fails to login when one server in a cluster is offline/unavailable.
CSCvo11654	When joining a call using the WebRTC app, no video is received after a network interruption occurs.
CSCvo37253	Cisco Meeting Server's Callbridge component may restart unexpectedly in a dual homed meeting when it is unmuted by the Skype for Business host.
CSCvo37254	On very rare occasions when a Media Module restarts it could reconnect twice resulting the module status reporting that the Media Module is presumed lost with no response to ping for long a time.
CSCvo51337	When cross launching from a browser to Meeting App 1.11.13 the browser displays "You are no longer in the meeting".
CSCvo11426	On Meeting Server, the Webbridge is spamming the logs "… Session <GUID> is pending destroy. Performing partial detach… "

Issues seen in previous versions that are fixed in 2.5.1

Cisco identifier	Summary
CSCvn81865	Support for the WebRTC app using Google Chrome version 72. See New features introduced in 2.5.1 for further information.
CSCvo02066	Cisco Meeting App users experience intermittent failures when authenticating with Cisco Meeting Server.
CSCvn14138	The "media module status" line in the logs is not followed by the usual numbers to indicate the health of the media framework on Cisco Meeting Server 2000.
CSCvn37841	No video/audio received from a remote participant in a distributed call on clustered Cisco Meeting Server 2000.
CSCvm95156	When running a trunk debug on Meeting Server 2000 it returns an error that the file is not found.
CSCvk67533	When recording a session it stops after 1-3 hours of recording due to a recorder "keepalive failure".

Cisco identifier	Summary
CSCvj13390	In clustered environments with multiple TURN Servers configured, if one TURN server is becoming unavailable, the webbridge does not correctly detect this in order to fail-over to the other available TURN servers - it continues to advertise the non available one to WebRTC clients.
CSCvn04352	When cross launching Meeting App client through IE browser it connects as "guest" when using the host passcode for a meeting.

Issues seen in previous versions that are fixed in 2.5.0

Cisco identifier	Summary
CSCvn59240	If you join a call using the Safari browser to open the Web RTC app, but then open another tab in the browser with another web page displayed, Safari will stop sending video to the other participants in the conference. Sending video is resumed if you switch back to the tab containing the WebRTC app.
CSCvn16684	If the XMPP component drops, then Cisco Meeting App users paired to SIP endpoints are logged out and removed from the meeting.
CSCvm38925	Calls to CTS endpoints fail due to the Meeting Server sending outbound SIP calls without cisco-tip or x-cisco-multiple-screen in the contact header, when connecting using TCP or TLS.
CSCvk067078	Joining a conference on a Meeting Server using Jabber for Windows (desk phone mode), after placing the call on Hold the video quality is degraded to a lower resolution/frame rate when it is Resumed.
CSCvk03337	Some TIP calls fail with TIP negotiation timeout.
CSCvn26366	When the uploader is enabled, the session timeout is not extended properly and it may cause login failures from Meeting Server to VBrick Rev.

4.2 Open issues

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

Cisco identifier	Summary
CSCvr16426	The "Participant add" ActiveControl option can be seen on ActiveControl-compatible endpoints that are members of a Dual Home meeting, even though the function is not supported and will not work correctly.
CSCvo66473	Microphone selection on Cisco Meeting App for WebRTC doesn't work on Safari on Mac. Use Google Chrome if you need to use microphone selection or disable the extra microphones prior to joining a Meeting App meeting.

Cisco identifier	Summary
CSCvn65208	If Call Bridge Groups are in use and the API parameters loadBalanceOutgoingCalls and loadBalanceUserCalls are set to true, if a WebRTC app attempts to make a call using the "Use my phone for audio" option and this call lands on a different Call Bridge to the one that the Cisco Meeting App user is instantiated on, then the Web Bridge will lose communication with other components or devices. Existing WebRTC app sessions will cease to work and no new WebRTC app logins are possible. Restarting the Web Bridge from the MMP interface will restore functionality.
CSCvn65112	For locally hosted branding, if the audio prompt files are omitted then the default built-in prompts are used instead. To suppress all audio prompts use a zero-byte file, rather than no file at all.
CSCvn63172	Low quality audio and video experienced on TIP endpoints that join conferences hosted on Meeting Server 2000 with a heavy conference load.
CSCvm56734	In a dual homed conference, the video does not restart after the attendee unmutes the video.
CSCvj49594	ActiveControl does not work after a hold/resume when a call traverses Cisco Unified Communications Manager and Cisco Expressway.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.
CSCvh23036	DTLS1.2, which is the default DTLS setting for Meeting Server 2.4, is not supported by Cisco endpoints running CE 9.1.x. ActiveControl will only be established between Meeting Server 2.4 and the endpoints, if DTLS is changed to 1.1 using the MMP command `tls-min-dtls-version 1.0`.
CSCvh23028	Changing the interface that the Web Bridge listens on or receiving a DHCP lease expire, will cause the Web Bridge to restart. WebRTC App users may have to log in again.
CSCvg62497	If the NFS is set or becomes Read Only, then the Uploader component will continuously upload the same video recording to Vbrick. This is a result of the Uploader being unable to mark the file as upload complete. To avoid this, ensure that the NFS has read/write access.
CSCve64225	Cisco UCS Manager for Cisco Meeting Server 2000 should be updated to 3.1(3a) to fix OpenSSL CVE issues.
CSCve60309	Cisco UCS Manager 3.1(3a) reports 'DIMM A1 on server 1/1 has an invalid FRU' as the CMS 2000 DIMMs are not listed in the 3.2(3e)T catalog.
CSCve37087 but related to CSCvd91302	One of the media blades of the Cisco Meeting Server 2000 occasionally fails to boot correctly. Workaround: Reboot the Fabric Interconnect modules.

In addition there is the following limitation:

CAUTION: The maximum number of concurrent XMPP clients supported by the current Meeting Server software is 500.This maximum is a total number of all different clients (Cisco Meeting App, WebRTC Sign-in and WebRTC Guest clients) registered at the same time to clustered

Meeting Servers. If the number of concurrent XMPP registrations exceeds 500 sessions, some unexpected problems with sign in may occur or it may lead to a situation where all currently registered users need to re-sign in, this can cause a denial of service when all users try to sign in at the same time.

Note: The increased call capacity of 700 HD (720p30) or 350 full HD (1080p30) calls on a Cisco Meeting Server 2000 only applies to a single Meeting Server or cluster of Meeting Servers. The HD call capacity of Meeting Servers within a Call Bridge group remains at 500.

Note: There are limitations using the WebRTC app with Edge and FireFox browsers. Using the WebRTC app with Edge will not work if using the TURN server in Cisco Expressway or using the Meeting Server TURN with TCP. Using the WebRTC app with Firefox will not work if using the TURN server in Cisco Expressway with TCP, but will work with the Meeting Server TURN with TCP. Refer to the Cisco Meeting App (WebRTC) 2.5.x Release Notes for further details on these and other limitations if using the WebRTC app.

Cisco Legal Information

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

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

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

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

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

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

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

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

Cisco Trademark