Cisco Meeting Server

Cisco Meeting Server Release 2.3.0

Release Notes

April 26, 2018

Contents

What's changed

Version	Change
2.3.0	Documentation omission – XMPP client limit added (April 25, 2018)
2.3.0	Added example to choosing Call Bridge mode for dual homed conferencing. (April 17, 2018)
2.3.0	Upgrade URLs corrected. (March 05, 2018)
2.3.0	New release.

1 Introduction

These release notes describe the new features, improvements and changes in release 2.3 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.

  Note: release 2.3 of the Cisco Meeting Server software is not yet available for the Cisco Meeting Server 2000, it will follow later.

- 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: Microsoft Hyper-V will no longer be supported from version 2.4 of the Meeting Server software.

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 SIP edge: From version X8.9, the Cisco Expressway supports traversal of SIP traffic at the edge of the network, to and from the Meeting Server; we recommend upgrading to the latest version of the Cisco Expressway software. You are advised to use the Cisco Expressway between remote Lync deployments and the Meeting Server, see the Cisco Expressway with Cisco Meeting Server and Microsoft Federation deployment guide.

The SIP and Lync Call Traversal feature first introduced in Acano Server release 1.8, is still a beta feature in Cisco Meeting Server 2.3, it is not intended for a production environment. This SIP edge feature will be withdrawn in a future version of the Cisco Meeting Server software.

Note about WebRTC proxying via Expressway: If proxying WebRTC traffic to the Meeting Server via Expressway, then when upgrading to Meeting Server release 2.3 it may be necessary to run 2.2.10 software versions or later for at least seven days before upgrading to the 2.3 release. Failure to do so will lead to an inability to connect to the Web Bridge. This is due to a very long cache header provided by previous versions of Meeting Server. For more information, please read CSCvh24431.

Note about incoming calls: From Meeting Server version 2.1, there is a change to the way the Cisco Meeting App handles 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 2.3. Otherwise, you will need to use the API to create a callProfile with parameter **`messageBoardEnabled`** set to true.

Note about a single Edge solution for Cisco collaboration products: 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 Cisco Meeting Server H.323 Gateway component. From version 2.3 of the Meeting Server software, there will be no further development or feature releases related to the H.323 Gateway component, and in version 2.5 the component will be removed from the Meeting Server software. 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.

Note about Cisco TelePresence System (CTS) endpoints: From version 2.1 of the Meeting Server, CTS endpoints are no longer supported, this includes the 3200 Series, 3000 Series, 1300 Series, the 1000 and the 500-37. In version 2.3.0 of the Meeting Server, CTS endpoints were not able to decode video from the Meeting Server.

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
- Cisco Multiparty Media 400v, 410v and 410vb
- specification-based VM platforms.

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 End Of Software Maintenance

On release of Cisco Meeting Server software version 2.3, Cisco announces the timeline for the end of software maintenance for versions 2.0 and 2.1.

Table 1: Timeline for End Of Software Maintenance for versions 2.0 and 2.1

Cisco Meeting Server software version	End of Software Maintenance notice period
2.0	3 months after first release of version 2.3
2.0 for federal customers	3 months after JITC acceptance of version 2.3
2.1	3 months after first release of version 2.3

At the end of the notice period, shown in Table 1, Cisco will remove the software and release notes from the download center and support pages. For more information on Cisco's End of Software Maintenance policy for Cisco Meeting Server click here.

2 New Features/Changes in version 2.3

Release 2.3 of the Meeting Server software adds the following:

- an improved meeting experience for Lync and Skype for Business participants. The Meeting Server sends a high resolution and a low resolution H.264 video stream per video participant to the AVMCU. These dual streams overcome the poor video quality experienced by participants when a Lync client that can only receive a lower resolution joins the call.
- you can choose the behavior of the Call Bridge when connecting SIP participants to Lync conferences.
- support for the new Cisco Meeting Apps, version 1.10, which have an improved, more intuitive user interface, including the facility to lock and unlock conferences through the user interface, rather than use a DTMF keypad. For more information, see the Cisco Meeting App version 1.10 release notes.
- a new WebRTC app with an improved, more intuitive, user interface in keeping with the new Cisco Meeting Apps, version 1.10. There are also changes to customizing the WebRTC sign in.
- support for load balancing Cisco Meeting App calls to spaces using Call Bridge Goups.
- you can prevent incoming audio-only calls from creating video streams for outgoing calls to a new destination when the Meeting Server acts as a gateway.
- support for ESXi 6.5 and also ESX 6.0 Update 3 on the Cisco Meeting Server 1000 and on generic Cisco Meeting Server VM deployments.
- support for dual screen endpoints now enabled by default.
- support for TLS 1.2.
- support for more video streams over distribution links creating a more consistent video experience from remote single, dual and three screen end point systems. This is a preview feature.
- an Uploader tool to simplify the work flow for uploading Meeting Server recordings to the video content manager, Vbrick, from a configured NFS. This is a preview feature.
- additional MMP commands.
- new API functionality

and a few miscellaneous improvements.

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.

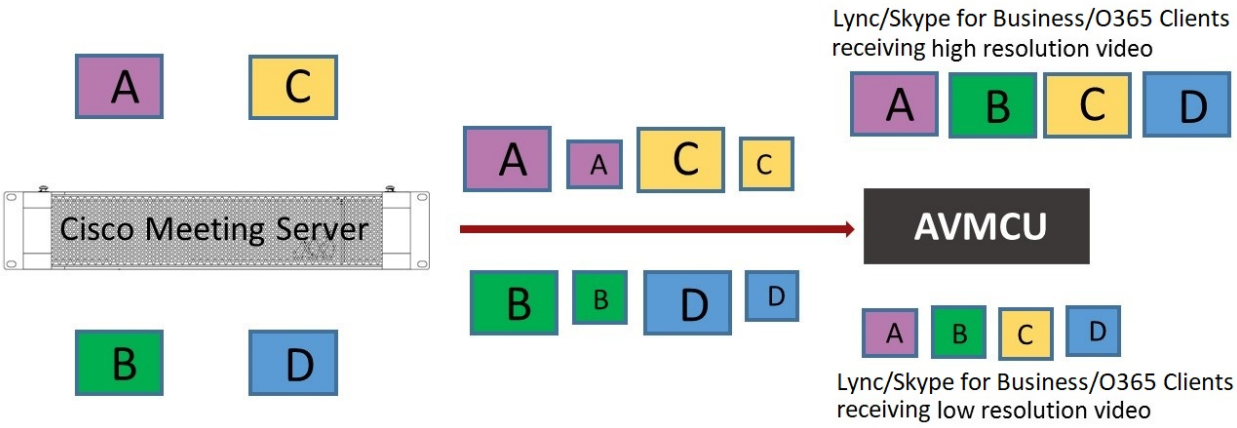
2.1 Improved dual homed meeting experience

Prior to version 2.3, the Meeting Server only sent one H.264 video stream per video participant to the AVMCU. The video resolution received by Lync, Skype for Business and O365 client users was degraded if another client that could only receive a lower resolution joined the dual homed call, all Lync, Skype for Business and O365 clients in the call received the lower resolution.

From version 2.3, the Meeting Server sends two H.264 video streams stream per video participant to the AVMCU, a high resolution video stream and a low resolution video stream, see Figure 1. Clients that can support the high resolution, subscribe to and receive the high quality video stream. Clients that select a lower quality, because of bandwidth restrictions, window size, layout, cpu power or being on a mobile device, subscribe to and receive the lower quality stream, instead of reducing the video experience for all participants.

Note: Ensure that the bandwidth of the SIP trunk is set sufficiently high to accommodate the two video streams. We recommend 8MB for LANs and 2.5MB for WANs.

Figure 1: Dual media streams to AVMCU



Note: Any devices using Microsoft RTVideo will not benefit from this feature.

2.2 Choosing Call Bridge mode to connect participants to Lync conferences

Version 2.3 allows you to choose the behavior of the Call Bridge when connecting participants to Lync conferences. A request parameter **`lyncConferenceMode`** has been added when POSTing to **`/callProfiles`** or PUTing to **`/callProfile/<call profile id>`**.

Set **`lyncConferenceMode`** to **`dualHomeCluster`** if you want the calls to be distributed between clustered Call Bridges, with one of the Call Bridges calling out to the AVMCU meeting. This is the same behavior as version 2.2 and earlier.

Set to **`dualHomeCallBridge`** if you do not want the calls to be distributed between clustered Call Bridges, but calls on the same Call Bridge need to be combined into one conference. This will result in a single conference on each Call Bridge, each Call Bridge will call out to the AVMCU meeting.

Set to **`gateway`** if you do not want the calls to be distributed between Call Bridges or calls on the same Call Bridge combined into one conference. Each SIP participant will be in their own conference with an associated call out to the AVMCU meeting.

Note: Set **`lyncConferenceMode`** to **`gateway`** to disable dual home conferencing.

For example, in a deployment with three SIP participants connecting to an AVMCU conference via two Meeting Servers, with two of the SIP participants on the same Meeting Server, the following behaviors will be seen by selecting the different modes:

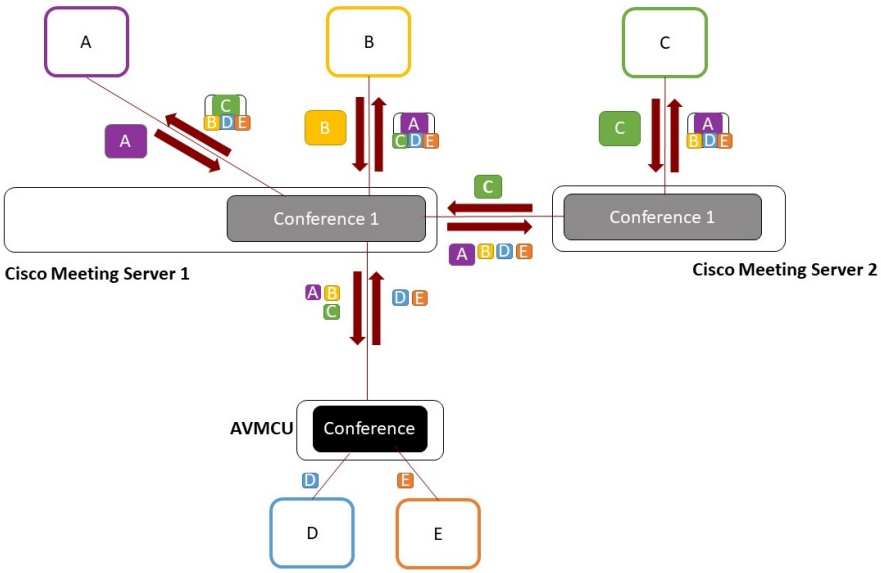
- **`dualHomeCluster`**: media streams are sent between the clustered Meeting Servers, see Figure 2. All calls from the SIP participants will be combined into one conference spanning both Call Bridges; one Call Bridge will call out to the AVMCU. **`dualHomeCluster`** uses one Multiparty Plus license for the single conference.

  Note: In the **`dualHomeCluster`** mode, video streams for participants directly connected to the AVMCU, come from the AVMCU. If using Lync2013 or Skype for Business and four or more participants join the meeting, then the resolution of these streams may limited to a maximum of 360p.

  This mode typically allows more video streams to be available, often at high resolution. This comes from two factors: firstly, if fewer media streams are requested from Lync, these streams may be at higher resolution, secondly the streams sourced from SIP devices are typically available at a higher resolution. However, since all audio streams need to be sent, then even without video, this can be a substantial overhead leading to increase bandwidth requirements. Since video streams traverse multiple hops, then even more bandwidth is required. And the multiple hops can add latency.

  Note: This mode leads to less predictability, since the order that people join the conference changes the connections made, and hence the available streams. In addition, the first Call Bridge to connect to Lync may not be the best choice, and in some cases can mean that fewer participants are seen.

Figure 2: Lync AVMCU/Meeting Server deployment using dualHomeCluster mode



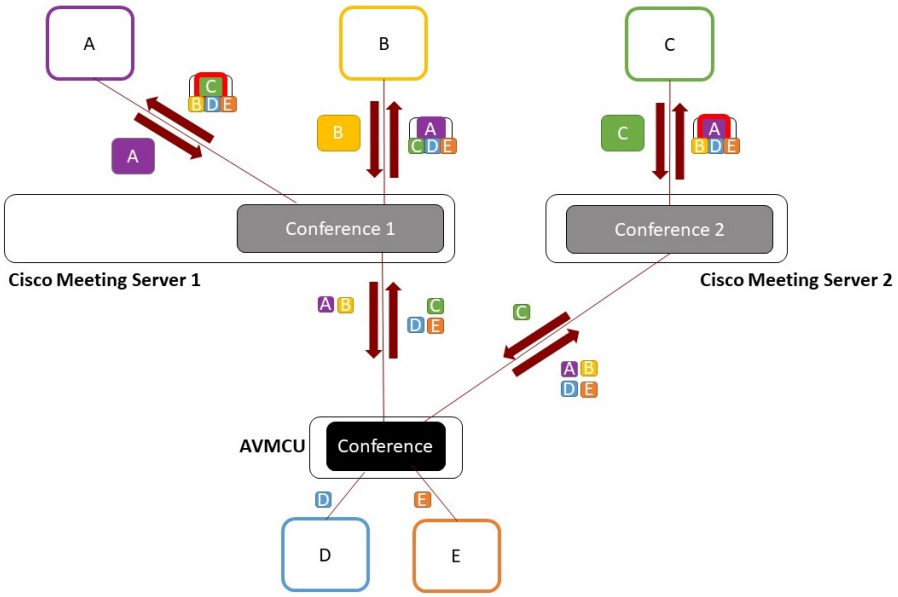
- **`dualHomeCallBridge`**: will result in the two SIP participants on the same Call Bridge being combined into one conference, see Figure 3. Streams seen by endpoint C come via the AVMCU, the stream of endpoint A seen by endpoint B does not come via the AVMCU. **`dualHomeCallBridge`** mode involves multiple conferences on the Meeting Servers and will consume multiple Multiparty Plus licenses; two Multiparty Plus licenses are consumed in the example given in Figure 3.

  Note: In the dualhomeCallBridge mode, video streams for participants on another Call Bridge and directly connected to the AVMCU, come from the AVMCU. If using Lync2013 or Skype for Business and four or more participants join the meeting, then the resolution of these streams may limited to a maximum of 360p.

  This mode cuts down on the bandwidth usage, as media streams going towards the AVMCU do not need to be sent to a single Meeting Server node. However, video coming from the AVMCU can potentially be at lower resolution (indicated in Figure 3 by a red outline around the main panes potentially affected).

  Note: This mode is more predictable since the order of people joining the meeting is not relevant.

Figure 3: Lync AVMCU/Meeting Server deployment using dualHomeCallBridge mode



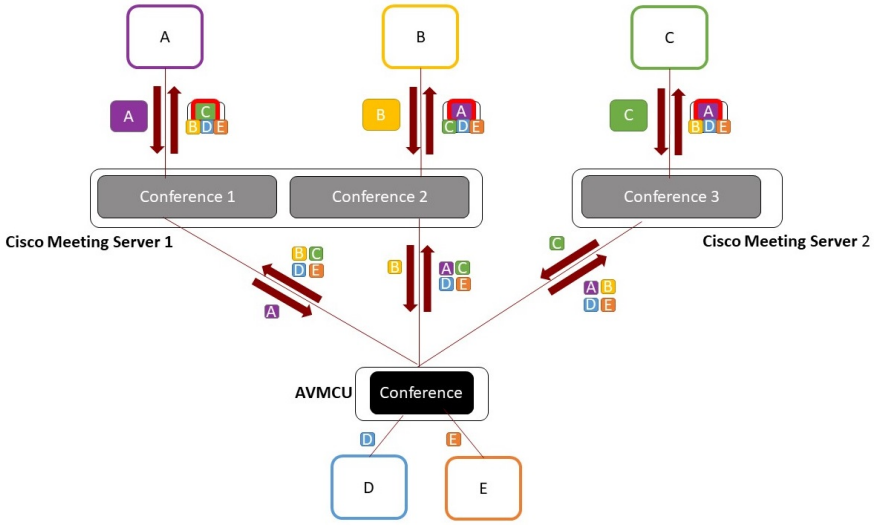
- **gateway** this will result in all three Meeting Server conferences calling out to the AVMCU meeting. Video streams seen by endpoints A, B and C all come via the AVMCU, see Figure 4, and can potentially be at lower resolution, indicated by a red outline around the main panes potentially affected.

  Since each call leg is handled separately, then a single Call Bridge may be requesting multiple copies of the same video stream, consuming more bandwidth.

  From version 2.3, a Shared Multiparty Plus license entitles you to six **gateway** calls. Each participant dialing through CMS to another user, or to a Microsoft Lync AVMCU meeting using the gateway mode consumes one sixth (1/6) of an SMP plus license. In the example given in Figure 4, one half (3/6) of a Shared Multiparty Plus license is consumed. Note that reporting license usage via the API does not reflect this yet—every gateway call will currently report 1 full license consumed rather than the one sixth (1/6) that is actually consumed.

  Note: In **gateway** mode, all video streams come from the AVMCU. If using Lync 2013 or Skype for Business and four or more participants join the meeting, then the resolution of each stream may be limited to a maximum of 360p.

Figure 4: Lync AVMCU/Meeting Server deployment using gateway mode



2.3 New WebRTC App and Web Bridge

Version 2.3 of the Meeting Server introduces the new WebRTC app which receives and transmits higher quality video using H.264, and has an improved user interface, similar to the new Cisco Meeting App version 1.10 for Windows, Mac and iOS. Chrome is the only browser currently supported for this version of the WebRTC app.

Note: There are differences between the new WebRTC app and the new Cisco Meeting App version 1.10 for Windows and Mac. Refer to the Feature Comparison Matrix that accompanies the user documentation for these differences.

Behind the WebRTC app is a new Web Bridge, there is a minor change to the functionality and configuration of the new Web Bridge. This change is:

- the legacy mode for guest access on the Web Admin interface (**Configuration** > **General** > **Guest access via ID and passcode**) has no effect. From version 2.3, if passcodes are required for guest, then the passcode needs to be supplied at the same time as the guest id.

Note: If you have a single combined Meeting Server deployment then the Web Bridge will be upgraded to the new version when you upgrade the Meeting Server software to version 2.3. For deployments involving multiple Meeting Servers, we recommend that you upgrade all Meeting Servers to the same version to avoid the risk of any incompatibilities between versions.

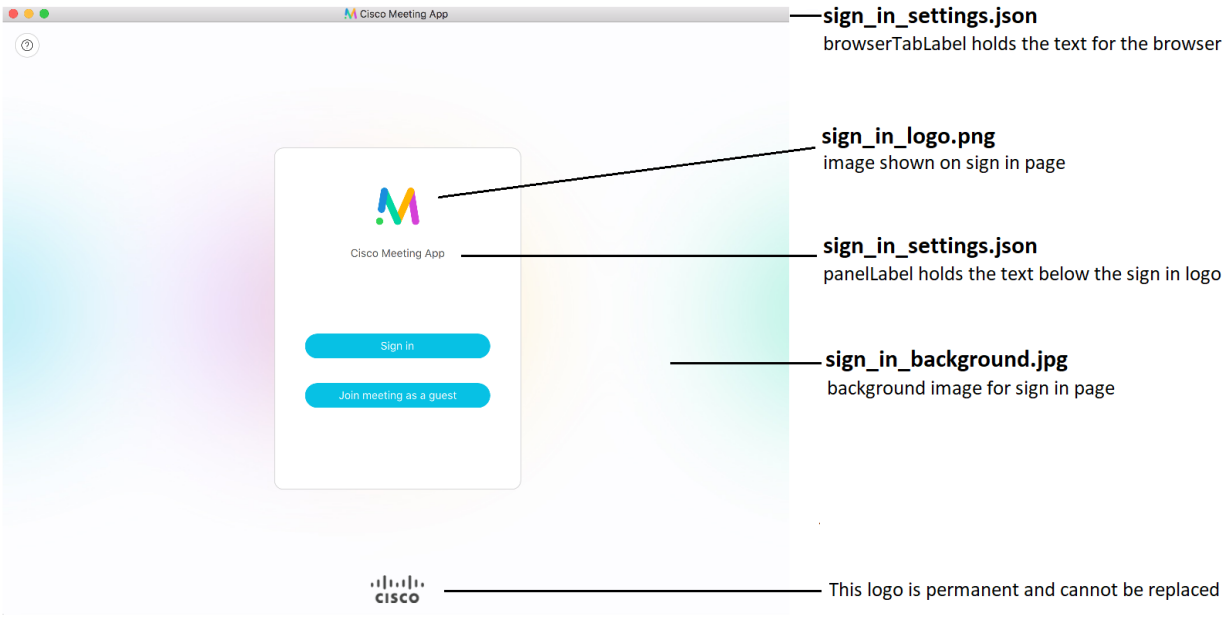
2.3.1 Customizing the WebRTC sign in page

From version 2.3, the redesigned Web Bridge can only be customized through the API; it is no longer possible to upload a new background image and logo for the WebRTC app using the Web Admin interface.

The new look and feel for the WebRTC app, has resulted in changes to the design elements that can be rebranded. From 2.3, only these elements can be rebranded via the API:

- sign in background image for WebRTC app,
- sign in logo,
- text below sign in logo,
- text on browser tab.

Figure 5: WebRTC app assets



See the Cisco Meeting Server 2.3 Customization Guidelines for examples on using the API to undertake this level of customization.

2.4 Load balancing Cisco Meeting App calls

Since version 2.2, inbound and oubound SIP calls through Cisco Unified Communications Manager can be load balanced using Call Bridge Groups. However, calls using the Cisco Meeting App in the same deployment could not be load balanced; the media to and from the Cisco Meeting App always flowed through the Call Bridge that it first connected to.

In version 2.3, the existing load balancing algorithm has been extended to include Cisco Meeting App participants (including the WebRTC app users). This applies to:

- a Cisco Meeting App user joining as a member of the space,
- a Cisco Meeting App user joining as a non-member of the space, with and without a

passcode

- a guest user joining the space.

By default, Cisco Meeting App participants are also load balanced if the **`loadBalancingEnabled`** parameter is set to true on the **`/callBridgeGroups`** API object (by default it is set to false). The decision on where to place the call is no longer restricted to the first Call Bridge which the Cisco Meeting App connects to.

The load balancing algorithm has been extended to include:

- Cisco Meeting App participants added via the API with a Call Bridge Group specified. The media will come from a Call Bridge in the specified Call Bridge Group, the Call Bridge chosen will be based on the existing algorithms
- Cisco Meeting App participants added via the API with a Call Bridge specified. The media will come from that Call Bridge.
- Cisco Meeting App participants simply joining a space without having been added to the space via the API. If this occurs, the Call Bridge that the Cisco Meeting App first connects to is determined, if that Call Bridge is part of a Call Bridge Group then the call is load balanced.

To load balance Cisco Meeting App calls, ensure that each Call Bridge in the Call Bridge Group has a connection to the XMPP cluster or single XMPP server, see the appropriate deployment guide for details on how to configure the connection.

For more information on load balancing, see the Loading Balancing Calls Across Cisco Meeting Servers white paper.

2.4.1 Disabling load balancing Cisco Meeting App participants

To disable load balancing Cisco Meeting App participants while continuing to load balance SIP calls, use the API to set the **`loadBalanceUserCalls`** request parameter on **`/callBridgeGroups`** to **`false`**.

2.5 Reducing wasted video streams on audio-only gateway calls

Version 2.3 introduces a new request parameter **`audioGatewayCallOptimization`** to the **`/callProfile`** object to set outgoing calls as audio-only if they are as a result of audio-only incoming calls. Setting **`audioGatewayCallOptimization`** to **`true`** affects:

- incoming SIP or Lync calls resulting in outgoing SIP calls
- incoming SIP or Lync calls resulting in outgoing Lync calls
- incoming SIP or Lync calls to an IVR that trigger participation in a Lync conference

Using this feature prevents the Meeting Server from generating audio and video streams on outgoing call legs when the received incoming call has audio-only call legs. The reduction in unused video streams will potentially reduce the loading on the Meeting Server and AVMCU.

Note: The outgoing call leg will remain audio-only, even if the incoming call leg later changes to audio and video.

Note: This feature requires 'early offer' enabled on Cisco Unified Communications Manager deployments. Deployments using 'delayed offer' will still send video on the Lync leg of the call, as a result of the Meeting Server not knowing that the call is audio only until after the call is established.

2.6 Support for TLS 1.2

Since the standardization of TLS 1.2 in 2008, continued analysis of older versions of TLS has shown significant weaknesses. This led to NIST advising in 2014 to move from TLS 1.0 to later versions of the protocol. Since then the deprecation of TLS 1.0 in products has started, with the PCI deadline for complete removal currently standing at June 2018.

Due to this, from version 2.3, the Meeting Server will by default use TLS 1.2 and DTLS 1.2 for all services: SIP, LDAP, HTTPS (inbound connections: API, Web Admin and Web Bridge, outbound connections: CDRs) and XMPP. If needed for interop with older software that has not implemented TLS 1.2, a lower version of the protocol can be set as the minimum TLS version for the SIP, LDAP and HTTPS services using the MMP command **`tls <service> min-tls-version <minimum version string>`**. See Section 2.12.

However, note that a future version of Meeting Server may completely remove TLS 1.0.

Note: Ad hoc escalation from Cisco Unified Communications Manager uses the HTTPS interface of the Meeting Server. Versions of Cisco Unified Communications Manager prior to 11.5(1)SU3 only support TLS 1.0 for this communication path. If using ad hoc escalation, either upgrade Cisco Unified Communications Manager to a version that supports later versions of TLS, or lower the minimum version of TLS supported for the HTTPS interface on the Meeting Server.

2.7 ESXi 6.5 and ESX 6.0 Update 3 support

Meeting Server version 2.3 adds support for ESXi 6.5 and also ESX 6.0 Update 3 on the Cisco Meeting Server 1000 and on generic Cisco Meeting Server VM deployments. Both ESXi 6.5 and ESX 6.0 Update 3 provide a tool to enable you to disable TLS 1.0 and TLS 1.1 from communicating with ESXi.

2.8 Support for dual screen endpoints enabled by default

Support for dual screen endpoints was first introduced in Meeting Server version 2.2, allowing video to be shown across both screens of a dual screen endpoint running CE9.1.4 (or later) that

are in local calls within your network or for calls over Cisco Expressway (X8.9). In version 2.2 the feature was disabled by default, but from version 2.3, the feature is enabled by default.

When content is being shared with a dual screen endpoint, either one video and one content stream is sent, or in the case of a dual screen endpoint with a 3rd monitor connected, two video streams and one content stream are sent. For more information on this feature see this FAQ.

2.8.1 Disabling dual screen endpoint support

To disable dual screen endpoint support:

1. Identify the compatibilityProfile that is applied to **`/system/profiles`** with **`sipMultistream`** set to true.
2. PUT to **`/compatibilityProfiles/<compatibility profile id>`** the parameter **`sipMultistream`** set to false, where **`<compatibility profile id>`** is the ID of the compatibilityProfile identified in step 1.

2.9 More video streams over distribution links between clustered Call Bridges (preview feature)

Note: This remains a beta feature.

Prior to version 2.3, video from a maximum of four remote participants could be sent over each distribution link between clustered Call Bridges. From version 2.3, the Meeting Server supports more video streams over the distribution links. Participants using single, dual and three screen endpoint systems can now have a more consistent conference experience between conferences hosted on clustered Call Bridges as those hosted on only a single Call Bridge.

To support more than four video streams across a distribution link, the bandwidth of the link must be set to greater than 2Mbps. Use the API or the Web Admin Interface to set the bandwidth. If using the API, PUT a value for the **`peerLinkBitRate`** parameter to the API object **`/system/configuration/`**; the value will be the maximum media bit rate to use on distribution links between Call Bridges in the cluster. Alternatively, using the Web Admin Interface, go to **Configuration>Cluster>Call Bridge identity** and enter the **Peer link bit rate**.

If the Peer link bit rate is set to be above 2Mbps, and there are more than 4 remote participants across a distribution link, then the Meeting Server will send up to 9 participants across the distribution link.

2.10 Recording with Vbrick (preview feature)

Note: This remains a beta feature.

Version 2.3 simplifies the work flow for uploading Meeting Server recordings to the video content manager, Vbrick, from a configured NFS connected to a Meeting Server. No manual importing of recordings is required.

Once the Uploader component is configured and enabled, recordings are pushed from the NFS to Vbrick, and an owner is assigned to the recording. The Rev portal applies security configured by your administrator to your video content, only allowing a user to access the content that they are permitted to access. Vbrick emails the owner when the recording is available in the owner's Rev portal. Owners of a recording access video content through their Rev portal, and can edit and distribute as necessary.

Note: If a file is added to the NFS share within a space directory, the file will be uploaded to Vbrick as though it were a valid recording. Take care to apply permissions to your NFS share so that only the Recorder can write to it.

2.10.1 Prerequisites for the Meeting Server

Uploader installation. The Uploader component can be installed on the same server as the Recorder component, or on a separate server. If installed on the same server as the Recorder, then add a couple of vCPUs for it to use. If run on a different server, then use the same server specification as for the Recorder: dedicated VM with a minimum of 4 physical cores and 4GB.

CAUTION: The Uploader must run on a different Meeting Server to the Call Bridge hosting the conferences.

Read and Write access to the NFS share. The Meeting Server running the Uploader will require Read and Write permissions for the NFS. Write permission is required to allow the Uploader to re-write the name of the mp4 file when upload is completed.

Note: 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.

API Access to Vbrick Rev. Configure API access for a user on Vbrick Rev.

API Access to Call Bridge. Configure API access for a user on the Meeting Server running the Call Bridge.

Trust Store Storing the certificate chains from the Vbrick Rev server, and the Meeting Server running the Web Admin interface for the Call Bridge. The Uploader needs to trust both the Vbrick Rev and the Call Bridge.

Decide who has access to the video recordings. Access to uploaded video recordings can be set to: All Users, Private, and for only space owners and members.

Default state of video recordings. Decide whether the video recordings are immediately available after upload (Active), or that the owner of the video recording needs to publish it to make the recording available (Inactive).

Table 2: Port Requirements

Component	Connecting to	Destination port to open
Call Bridge	NFS (version 3)	2049
Uploader	Web Admin of Call Bridge	443 or port specified in Uploader configuration
Uploader	Vbrick Rev server	443 for video uploads and API access to Vbrick Rev server

2.10.2 Configuring the Meeting Server to work with Vbrick

These steps assume that you have already setup the NFS to store recordings.

1. Establish an SSH connection to the MMP of the Meeting Server where you want to run the Uploader. Log in.
2. For new Vbrick installations, ignore this step. If you are reconfiguring a Vbrick installation then first disable Vbrick access to the Meeting Server.
   `uploader disable`
3. Specify the NFS that the Uploader will monitor.
   `uploader nfs <hostname/IP>:<directory>`
4. Specify the Meeting Server that the Uploader will query for recording information, for example the name of the Meeting Server hosting the space associated with the recording.
   `uploader cms host <hostname>`
5. Specify the Web Admin port on the Meeting Server running the Call Bridge. If a port is not specified, it defaults to port 443.
   `uploader cms port <port>`
6. Specify the user with API access on the Meeting Server running the Call Bridge. The password is entered separately.
   `uploader cms user <username>`
7. Set the password for the user specified in step 6. Type
   `uploader cms password`
   you will be prompted for the password.
8. Create a certificate bundle (crt-bundle) holding a copy of the Root CA's certificate and all intermediate certificates in the chain for the Web Admin on the Meeting Server running the Call Bridge.
9. Add the certificate bundle created in step 8 to the Meeting Server trust store.
   `uploader cms trust <crt-bundle>`
10. Configure the Vbrick host and the port to which the Uploader will connect.
    `uploader rev host <hostname>`
    `uploader rev port <port>`

Note: The port defaults to 443 unless otherwise specified.

11. Add a Vbrick Rev user who has API permission to upload video recordings.
    uploader rev user <username>
12. Set the password for the user specified in step 11. Type
    uploader rev password
    you will be prompted for the password.
13. Create a certificate bundle (crt-bundle) holding a copy of the Root CA's certificate and all intermediate certificates in the chain for the Vbrick Rev server.
14. Add the certificate bundle created in step 13 to the Vbrick Rev trust store.
    uploader rev trust <crt-bundle>
15. Specify the name of the team permitted to edit the video recording.
    uploader edit <uploader-team name>

    Note: If the <uploader-team name> includes a space then use straight quotes around the team name, for example> **uploader edit "support team"**.

16. Specify the name of the team permitted to view the video recording.
    uploader view <uploader-team name>

    Note: If the <uploader-team name> includes a space then use straight quotes around the team name, for example **uploader view "sales team"**.

17. Set access to the video recording.
    uploader access <Private|Public|AllUsers>
18. Give members of the space the ability to view or edit the recordings.
    uploader cospace_member_access <view|edit|none>

    Note: This step requires that the JID of the members listed in the space MUST have accounts created in Vbrick Rev. The usernames of the members must be exactly the same in Vbrick as in the Meeting Server. For example **tenant10.user1@meetingserver10.example.com**

19. Decide whether the owner of the space is the single owner of the video recordings.
    uploader recording_owned_by_cospace_owner <true|false>
20. If the owner of the space is not listed in Vbrick Rev, then set the username of the fallback owner. If the fallback owner is not specified, then owner will default to the user configured on the MMP.
    uploader fallback_owner <vbrick-user>
21. Enable comments to the video recordings.
    uploader comments enable

22. Enable ratings for the video recordings.
    `uploader ratings enable`
23. Set the download permission for the video recordings.
    `uploader downloads enable`
24. Set the default state of the video recording when first uploaded to Vbrick Rev.
    `uploader initial_state <active|inactive>`
25. Decide whether to delete the video recording from the NFS after upload is complete
    `uploader delete_after_upload <true|false>`
26. Enable the Uploader to access the Meeting Server
    `uploader enable`

Note: Set **`messageBoardEnabled`** to **`true`** to see the messages being posted in the space indicating that the recording is available.

2.11 Miscellaneous changes and improvements

Release 2.3 supports the following changes and new features:

- if the parameter **`participantLabels`** is set to true on **`/callLegProfile`**, then participant name labels are shown on the smaller panes of multi-pane screen layouts in addition to the main pane.
- the response value **`name`** can now be returned on **`/calls/<call id>`**, this was missing in previous versions.
- for outbound or transferred calls, the Meeting Server now uses the display names configured on the end points as the display name labels. Prior to version 2.3, the Meeting Server ignored the “Remote-Party-ID” SIP header.
- the font pack has been replaced with the Cisco Sans Regular font, the Cisco pack has a wider language support, but will look slightly different from the font used in previous releases.

2.12 Summary of MMP changes

Version 2.3.0 has the following changes to the MMP commands:

- ability to change the minimum version of TLS used by the Meeting Server for SIP, LDAP, HTTPS (inbound connections: API, Web Admin and Web Bridge, outbound connections: CDRs) and DTLS services. This may be required for interop with older software that has not implemented TLS 1.2. See table below.

Command/Examples	Description
tls <service> min-tls-version <minimum version string> **tls sip min-tls-version 1.1** **tls ldap min-tls-version 1.1**	Configures the minimum TLS version that the system will use for the specified service. Use TLS version 1.1 or later for SIP Use TLS version 1.1 or later for LDAP
tls min-dtls-version <minimum version string **tls min-dtls-version 1.1**	Configures the minimum DTLS version that the system will use.

Note: When you change the minimum version of TLS or DTLS, you need to restart the Call bridge service using the command **callbridge restart** from SSH.

- removal of 3DES from the list of ciphers supported for TLS certificate verification. 3DES is considered a weak cipher and new tighter security requirements require it's removal.

  The default cipher support for TLS certificate verification is now:
  " ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES"

  You can configure the default cipher string to allow 3DES ciphers, if really necessary. Use the MMP command: **tls <service> ciphers <cipher string>**.

- new commands to support using Vbrick Rev for video content.

Commands	Description
uploader (enable|disable)	Enables or disables the uploader component. Before configuring the Uploader, ensure the component is disabled.
uploader nfs <host-name/IP>:<directory>	Specify the NFS that the Uploader will monitor.
uploader (cms|rev) host <hostname>	Configure the Uploader with the name of the host for the Meeting Server (cms) and the host for the Vbrick Rev server.Default port is 443.
uploader (cms|rev) port <port>	Configure the Uploader with the port to use to connect to the Meeting Server (cms) and the port for the Vbrick Rev server. Default port is 443.
uploader (cms|rev) user <username>	Configure the Uploader with the user that has access to the API of the Meeting Server and the user with access to the Vbrick Rev server.
uploader (cms|rev) password	Configure the Uploader with the password for the specified Meeting Server user and the Vbrick Rev user.

Commands	Description
uploader (cms|rev) trust (<crt-bundle>|none)	Upload the specified certificate bundle to the trust store on the Meeting Server or the Vbrick Rev server. **none** removes the certificate bundle from the specified trust store. Note: the Uploader will not work without a certificate bundle in the Meeting Server trust store and the Vbrick Rev trust store.
uploader edit (<uploader-team name>|none)	Allow the named team to edit the video recordings on Vbrick Rev. If the **<uploader-team name>** includes a space then use straight quotes around the team name. **none** removes the named team, members of the team can no longer edit the video recordings.
uploader view (<uploader-team name>|none)	Allow the named team to view the video recordings on Vbrick Rev. If the **<uploader-team name>** includes a space then use straight quotes around the team name. **none** removes the named team, members of the team can no longer view the video recordings.
uploader access <Private|Public|AllUsers>	Set access permission to the video recordings
uploader cospace_member_access <view|edit|none>	Allows members of the space to view or edit the video recordings. **none** removes view or edit permissions for members of the space.
uploader recording_owned_by_cospace_owner <true|-false>	**true** selects the owner of the space as the single owner of these video recordings.
uploader fallback_owner (<username>|none)	Use the named user as the fallback owner of the video recordings, if the owner of the space is not listed in VbrickRev. **none** removes the fallback owner.
uploader comments (enable|disable)	Enables or disables commenting on video recordings. Default is disabled.
uploader ratings (enable|disable)	Enables or disables video recording ratings. Default is disabled.
uploader downloads (enable|disable)	Sets the download permission, enables or disables downloading the video recordings.
uploader initial_state (<active|inactive>)	Set the initial state of the video recording when first uploaded to Vbrick Rev. Default is active.
uploader delete_after_upload (<true|false>)	Selects whether to delete the video recording from the NFS after upload is complete. Default is false.

2.13 Summary of API Additions & Changes

New API functionality for the Meeting Server 2.3 includes the ability to:

- control whether call legs using a specific call leg profile can add other participants, this is typically used through ActiveControl.
- control whether call legs using a specific call leg profile can change the importance of participants in the call.
- control whether a Cisco Meeting App user can send email invites to space meetings.
- control whether a Cisco Meeting App user is allowed to change non-member access to spaces.
- set outgoing gateway call legs as audio-only, if the incoming call leg is audio-only.
- define the behavior of the Call Bridge when connecting participants to Lync conferences.
- identify the call type of an individual active call.
- display the associated human-readable name for a call.
- load balance Cisco Meeting App calls to spaces using Call Bridge Groups.
- find whether a conversation with a specified ID has been found.
- find the coSpace, user and/or IVR using a specified URI within a specified tenant.
- find whether a call leg is a distributed Lync connection.
- find the original destination address for outbound call legs or the remote address first signalled to the Call Bridge for inbound call legs.
- find the remote address first used by or signaled to the Call Bridge.

API changes for Meeting Server 2.3:

- support for dual video endpoints enabled by default.

2.13.1 Control whether call legs can add other participants

New request parameter **`addParticipantAllowed`** added to: **`/calls/<call id>`**, **`/calls/<call id>/callLegs`**, **`/calls/<call id>/participants`**, **`/callLegProfiles`**, **`/callLegProfiles/<call leg profile id>`**

New response value **`addParticipantAllowed`** added to **`/callLegs/<call leg id>/callLegProfileTrace`**

`addParticipantAllowed` can have the value of **`true`** or **`false`**

2.13.2 Control whether call legs using a specific call leg profile can change the importance of participants in the call

New request parameter **`setImportanceAllowed`** added to: **`/callLegProfiles`**, **`/callLegProfiles/<call leg profile id>`**

`setImportanceAllowed` can have the value of **`true`** or **`false`**

2.13.3 Control whether a Cisco Meeting App user can send email invites

New request parameter **canSendEmailInvite** added to: **/userProfiles**, **/userProfiles/<user profile id>**

canSendEmailInvite can have the value of **true** or **false**

2.13.4 Control whether a Cisco Meeting App user is allowed to change non-member access

New request parameter **canChangeNonMemberAccessAllowed** added to: **/coSpaces/<coSpace id>/coSpaceUsers/<coSpace user id>**

2.13.5 Set outgoing gateway call legs as audio-only if the incoming call leg is audio-only

New request parameter**gatewayAudioCallOptimization** added to: **/callProfiles**, **/callProfiles/<call profile id>**

gatewayAudioCallOptimization can have the value of **true** or **false**

2.13.6 Choose the behavior of the Call Bridge when connecting participants to Lync conferences

New request parameter **lyncConferenceMode** added to: **/callProfiles**, **/callProfiles/<call profile id>**

lyncConferenceMode can have a value of **dualHomeCluster**, **dualHomeCallBridge** or **gateway**

2.13.7 Identify the call type of an individual active call

New response **callType** for: **/calls/<call id>**

callType can have a value of: **coSpace**, **forwarding**, **adHoc**,or **lyncConferencing**

2.13.8 Display the associated human-readable name for a call

New response **name** for: **/calls/<call id>**

name is a string

2.13.9 Load balance Cisco Meeting App calls to spaces using Call Bridge Groups

New request parameter**loadBalanceUserCalls** added to: **/callBridgeGroups**, **/callBridgeGroups/<call bridge group id>**

loadBalanceUserCalls can have the value of **true** or **false**. Default is **true**.

2.13.10 Find whether a conversation with a specified ID has been found

New API object **`/conversationIdQuery`**, with request parameter **`conversationId`**, returns **`found`** with value of **`true`** or **`false`**

2.13.11 Find the coSpace, user and/or IVR using a specified URI within a specified tenant

New API object **`/uriUsageQuery`**, with request parameters **`uri`** and **`tenant`**, returns **`coSpaceId`**, **`userId`**, **`ivrID`** .

2.13.12 Find whether a call leg is a distributed Lync connection

New parameter returned on GET **`/callLegs/<call leg id>:lyncDistribution`**

2.13.13 Find the original destination address for outbound call legs or the remote address first signaled to the Call Bridge for inbound call legs

New parameter returned on GET **`/callLegs/<call leg id>:originalRemoteParty`**

2.13.14 Find the remote address first used by or signaled to the Call Bridge

New parameter returned on GET **`/participants/<participant id>:originalUri`**

2.14 Summary of CDR Changes

Version 2.3.0 has no additions or changes to the Call Detail Records of the Meeting Server.

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 2.3

This section assumes that you are upgrading from Cisco Meeting Server software version 2.2. If you are upgrading from an earlier version, then Cisco recommends that you upgrade to 2.2 first following the instructions in the 2.2.x release notes, before following any instructions in these Cisco Meeting Server 2.3 Release Notes.

Note: Cisco has not tested upgrading from a software release earlier than 2.2.

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 2.3

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 to release 2.3 you must 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. Do NOT use the automatic backup file that is created during the upgrade process.

CAUTION: If you have a Cisco Expressway connected to the Meeting Server, check that you have run version 2.2.10 or later on your Meeting Server for at least seven days before upgrading to release 2.3. This is required to resolve a cache issue which prevents the Meeting Server WebRTC from working with Cisco Expressway.

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 support section of the Cisco website. There will be four files:

   Cisco_Meeting_Server_2_3_0_CMS2000.zip

   This file requires unzipping to a single upgrade.img file. Use this file to upgrade Cisco Meeting Server 2000 servers, follow the instructions below. Note: this file may be released after the other upgrade files.

   Cisco_Meeting_Server_2_3_0.vhd

   Use this file to upgrade Microsoft Hyper-V deployments

   Cisco_Meeting_Server_2_3_0_x-series.zip

   This file requires unzipping to a single upgrade.img file. Use this file to upgrade Acano X-series servers, follow the instructions below.

   Cisco_Meeting_Server_2_3_0.ova

   Use this file for new vm deployments, follow the steps in the Installation Guide for Virtualized Deployments.

   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.

2. Validate the download; the checksums for the 2.3.0 release are 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-256 hash values in the table below.

Type	File	Hash
Server	upgrade.img	d8b4d7d3a8d8a519a7721eccc4eff6b518b58ed5fe7c783279ee7160c77a4286
VM	/acanoserverovf/acanoserverdisk1. vmdk	6694afad8f81b887d8a2e43e4f8cb6914e20a8390b32a9f7d089608c152342bb
VM	/acanoserverovf/acanoserver. mf	b3daf1fd9f0e69fd65a2b171b7a23be7869b86347e8734d1aa2b807cb0640f6e
VM	/acanoserverovf/acanoserver. ovf	cf7f9bf2f8b89e87650025ec4df8c044d595b0269e46487b61750fd993b59c18
VM	/acanoservervhd/acanoserver. vhd	33bad94d556953ed2e555e2d89e410ad1119b548871570b61ff2160138be5f9a
VM	upgrade.img	531ecf401b38ff0f9a7d307e0a26472a7dca14abd8e543821876cc358eec2290

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.
   c) After copying the upgrade.img file, you will not be able to see it listed as being in the file system; this is normal.

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 in the table 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. Check the **Configuration > Outbound Calls** rules updating the Local Contact Domain field and completing the new Local From Domain field if necessary.
9. Update the customization archive file when available.
10. If you are deploying a scaled or resilient deployment read the Scalability & Resilience Deployment Guide and plan the rest of your deployment order and configuration.

11. 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 & Resilience Deployment Guide.
12. You have completed the upgrade.

3.2 Downgrading

If anything unexpected occurs during the upgrade process you can return to the previous version of the server software.

Use the regular upgrade procedure to "upgrade" the Meeting Server to the appropriate version. Then restore the configuration backup for the older version, using the MMP command **backup rollback <name>** command. Do not rely on the backup generated automatically during upgrade. For deployments with clustered databases read the instructions in this FAQ, before "upgrading" clustered servers.

Note: In some rare cases with clustered deployments, it might be necessary to do the **factory_reset app** procedure on each server. For more information, see https://kb.acano.com/content/5/250/en/how-do-i-upgrade-a-resilient-deployment.html

---

Note: The **backup rollback <name>** 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.

3.3 Cisco Meeting Server 2.3 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 `2.2.0`.
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 2.3.0

Cisco identifier	Summary
CSCvh22934	In some rare circumstances, module 0 crashes on an Acano X2 server leading to lost video for participants in calls hosted on the Meeting Server.
CSCvh22828	If the Peer link bit rate is set, and it is set higher than the SIP bandwidth, then the lower SIP bandwidth setting is used for the distribution link and not the Peer link bit rate setting.
CSCvh21861	The Meeting Server may crash with error message " server-!ServerManagementCmgrClientInstance::PasscodeResolverUser_handlePasscodeResolutionFailure [server_management_cmgr_client_instance.cpp : 186 + 0x7]" .
CSCvg92785	The Call Bridge may restart when a SIP participant is disconnected from a meeting using ActiveControl.

Cisco identifier	Summary
CSCvg39964	For a scheduled meeting on TMS where TMS tells the Meeting Server to dial out to endpoints, the Meeting Server incorrectly reports to TMS that a participant is not connected, even though they are.
CSCvg16170	Some improvements have been made to the quality of the content received by the Chrome WebRTC app.
CSCvg01958	If a Cisco Meeting App user who is not a member of a space clicks on the space's weblink they are asked to enter a passcode for the space.
CSCve86564	Calls via the Meeting Server H.323 Gateway may fail if the maximum receiving resolution is set to SD on the Meeting Server.
CSCve14451	Audio on calls hosted on Acano X2 servers used for dual homed conferences become choppy as load approaches maximum capacity.
CSCve49740	The Meeting Server replies with a "486 Busy Here" message when it receives an invalid number for a gateway call rather than a "404 Not Found" call.

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
CSCvh47500	After upgrading to version 2.3, a WebRTC session will crash and return back to the landing page if the device being used does not have a working camera or microphone.
CSCvh23045	In a cluster of two Call Bridges, one of the Call Bridges may crash after a non-member has logged in and then logged out of a space that has no members.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.
CSCvh23036	DTLS1.2, which is the default DTLS setting for the Meeting Server 2.3, is not supported by Cisco endpoints running CE 9.1.x. Active Control will only be established between Meeting Server 2.3 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.
CSCvh22816	Logging in using the WebRTC app may fail even when correct credentials are supplied. This occurs when a particular cookie string is supplied by the web browser to the Web Bridge. To avoid this happening either open an incognito tab to use the WebRTC app or clear all cookies for the domain used by the Web Bridge, for example for the WebRTC app at https://join.example.com, clear all example.com cookies.

Cisco identifier	Summary
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.
CSCvg57974	The setting for **qualityMain** is lost when calling from one Call Bridge to another Call Bridge in the same cluster, with outbound load balancing enabled. **qualityMain** restricts the maximum negotiated main video call quality for a call leg.
CSCvf78579	In some deployments, Web Admin time stamps and cdrTime may be out of sync with time from the MMP. MMP **date** and **timezone** commands report the time correctly.
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 3.1(3a)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.
CSCve26287	TIP endpoint doesn't display video when quality is below 720p.

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.

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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this url: 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. (1110R)