Cisco Meeting Server

Cisco Meeting Server Release 2.1.12

Release Notes

September 03, 2018

Contents

What's changed

Version	Change
2.1.12	Added loadBalanceLyncCalls (previously omitted in error) (Sept 03, 2018)
2.1.12	Added section “Resolved in 2.1.12”
2.1.11	Added section “Resolved in 2.1.11”
2.1.10	Added section “Resolved in 2.1.10”
2.1.9	Added section “Resolved in 2.1.9”.
2.1.8	Added section “Resolved in 2.1.8”.
2.1.7, May 12th	Changed heading from “Call Bridge Groups” to” Load Balancing Calls” and Included information on participant limit to a space on a single Call Bridge.
2.1.7	Added section “Resolved in 2.1.7”.
2.1.6	Added section “Resolved in 2.1.6”.
2.1.5	Added section “Resolved in 2.1.5”. API addition to section 2.8.9 **`/system/status`**: **`cdrCorrelatorIndex`**
2.1.4	Added section “Resolved in 2.1.4”. Added bug SERVER-5928 to the “Resolved in 2.1.0” section.
2.1.3	Added section “Resolved in 2.1.3”.
2.1.2	Reverted from Web Bridge 2.0 to Web Bridge 1.9, see *Reverting to Web Bridge 1.9*. Added section “Resolved in 2.1.2”.
2.1.1	Added section “Resolved in 2.1.1”. Release no longer available.
2.1.0	New release, incorporating redesigned Web Bridge: Web Bridge 2.0. Release no longer available.

1 Introduction

This release note describes the new features, improvements and changes in release 2.1.12 of the Cisco Meeting Server software for: specified servers based on Cisco UCS technology, Acano X-Series Servers, and virtualized deployments.

The Cisco Meeting Server was formerly called the Acano Server. The Cisco Meeting Server can be hosted on:

- 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.

The Cisco Meeting Server software is referred to as the Meeting Server throughout the remainder of this guide.

If you are upgrading from 2.1.x, 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 2.1, 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: 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 about rebranding the background image to the login page for the WebRTC app: From Meeting Server 2.1.2 the Meeting Server no longer supports the redesigned Web Bridge 2.0. Instead it supports Web Bridge 1.9 which does support rebranding the background image for the login page to the WebRTC app.

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, see Section 2.6.7.

Note about chat message board: For existing deployments that use chat message boards, chat will remain enabled when you upgrade to 2.1. 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.

2 New Features/Changes in 2.1

Release 2.1 of the Meeting Server software comprises:

- Call Bridge Groups and load balancing calls
- ActiveControl
- streaming meetings
- improved join options for meetings
- support for Cisco Expressway X8.9
- a few miscellaneous new features
- additional MMP commands
- additional API objects and parameters to support these new features
- additional CDR support for new features.
- Cisco endpoints no longer supported

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

2.1 Load Balancing Calls

A typical large scale deployment consists of several Meeting Servers located at multiple offices/data centres. To minimise network load, reduce firewall configuration and to ensure efficient use of the Call Bridge resources, it is now possible to configure location information for components. A location could refer to a single datacentre, or a continent. The decision of how to group Call Bridges will depend on the specifics of your network configuration and the desired behavior.

Version 2.1 of the Cisco Meeting Server software introduces the API object **`/callBridgeGroups`** to specify a group. It also introduces API fields to limit the usage of other components to either a specific Call Bridge or Call Bridge Group.

In addition, version 2.1 introduces a limit of 450 participants to a conference in a space on a single Call Bridge. By introducing this limit we have standardized the experience of participants joining a call, no longer will there be a risk of participants not having audio on spaces with a large number of participants (more than 500 participants in a space on a single Call Bridge). To have more than 450 participants in a conference you will need to setup either clustered Call Bridges in conjunction with Cisco Unified Communications Manager, or preferably Call Bridge Groups so that calls are load balanced on Call Bridges within the Call Bridge group.

Note: Unless Call Bridge Groups have been set up, calls coming in via IVR will always by joined to the conference irrespective of whether the 450 limit has been reached. This may result in participants joining via IVR not receiving audio if more than 500 participants have connected to a space on a single Call Bridge.

2.1.1 Load balancing calls across Call Bridges

Ideally all of the media for calls to a conference should reside on the same Call Bridge if users are in the same location and if the required call capacity exists. When users are in multiple locations then ideally one Call Bridge per location should be used.

Creating a Call Bridge Group with Call Bridges that are configured as a cluster, will result in intelligent load balancing of calls across the Call Bridges in the cluster. For the load balancing feature to work correctly, a Round Trip Time (RTT) of less than 100 ms is required for the servers in a Call Bridge Group. The maximum RTT between any two nodes in the same cluster remains as 300 ms.

If the Call Bridges in a group are heavily loaded, then calls can be moved to Call Bridges in a different group using a call control device such as the Cisco Unified Communications Manager. The intelligent decision making behind where calls end up, is handled by the Meeting Servers. The call control system needs to be able to handle SIP messages from the Meeting Servers and move calls to the correct location. This functionality has been tested using Cisco Unified Communications Manager, which is the only Cisco supported call control system for this functionality. The Cisco VCS is not currently supported since it doesn't include support for INVITE with Replaces.

By default, a Call Bridge in a Call Bridge Group will reject all calls from new participants at 80% load , and only distribution calls will be allowed. The white paper entitled "Loading Balancing Across Cisco Meeting Servers" explains how load balancing is implemented across Call Bridges which are in a Call Bridge Group. It provides examples of how Call Bridge Groups can be used to redirect calls if particular Call Bridges are heavily loaded. It also explains what is required in a dial plan to implement call redirection.

Note: Call Bridge Groups only supports standard inbound SIP calls, it currently does not support outbound SIP calls or Cisco Meeting Apps.

2.1.1.1 How to enable load balancing of calls across a Call Bridge Group?

Perform a PUT on the new API object **`/callBridgeGroups`** with the **`loadBalancingEnabled`** parameter set to true.

2.1.1.2 How to enable load balancing of calls across a Call Bridge Group from Lync?

Perform a PUT on the new API object **`/callBridgeGroups`** with the **`loadBalanceLyncCalls`** parameter set to true.

2.1.1.3 How to determine the media loading on a Meeting Server?

Perform a GET on the new API object **`/system/load`**. A numeric value for parameter **`mediaProcessingLoad`** will be returned, this represents the load on the Meeting Server

If you have Call Bridge Groups configured, and you have load balancing activated, then calls from new participants are rejected at 80% load.

If you are not using load balancing with Call Bridge Groups, then calls will not be rejected, but the quality of all calls will be reduced when the load limit is reached. If this happens often, we recommend that you buy additional hardware.

Tip: If you have only one Call Bridge, and you want to reject calls rather than reducing quality, you can create a Call Bridge Group with a single Call Bridge and enable load balancing.

2.1.1.4 How to specify the load limits on a cluster of Meeting Servers?

Perform a PUT on the API object **`/system/configuration/cluster`** with the following parameters set:

- **`loadLimit`** with a numeric value for the maximum load on the Meeting Server
- **`newConferenceLoadLimitBasisPoints`** with a numeric value for the basis points of the load limit at which incoming calls to non-active conferences will be rejected, ranges from 0 to 10000, defaults to 5000.
- **`existingConferenceLoadLimitBasisPoint`** with a numeric value for the basis points of the load limit at which incoming calls to this Call Bridge will be rejected, ranges from 0 to 10000, defaults to 8000.

Suggested Load limits.

System	Load Limit
CMS1000	96000
X3	250000
X2	125000
X1	25000
VM	1250 per vCPU

Note: These load limits are currently being evaluated and may change.

2.1.2 Associating Web Bridges, Recorders, Streamers, and TURN servers to Call Bridges and Call Bridge Groups

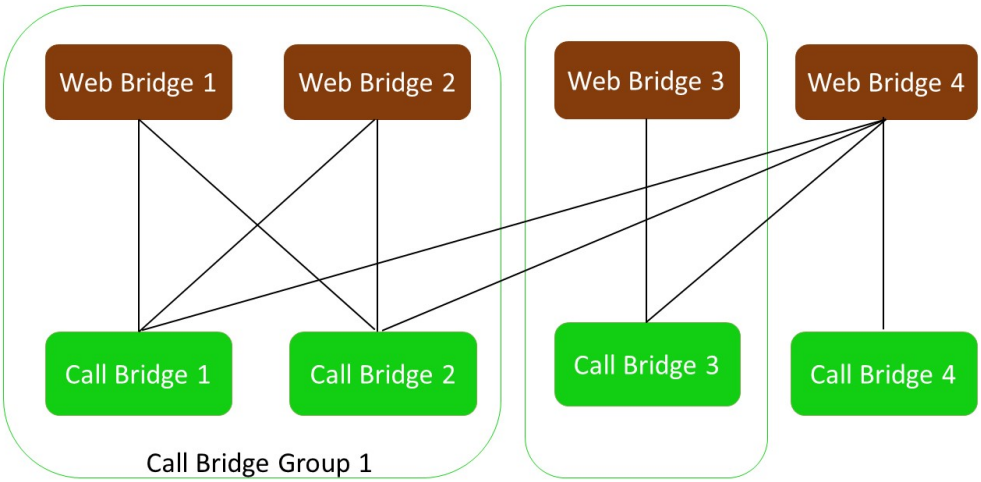
From version 2.1, Web Bridges, Recorders, Streamers, and TURN servers can be associated with individual Call Bridges and Call Bridge Groups. If a component is configured with either a

Call Bridge Group or a Call Bridge, then only the Call Bridges in the group or the specific Call Bridge will attempt to connect to the component.

For instance:

- a Web Bridge with a callBridgeGroup set: only the Call Bridges in the Call Bridge Group that was set for the Web Bridge, will attempt to connect to the Web Bridge.
- a Web Bridge with a specific callBridge set (but no group): only the Call Bridge that was set for the Web Bridge, will attempt to connect to the Web Bridge.
- a Web Bridge with neither a callBridgeGroup nor a callBridge set: any Call Bridge may attempt to connect to the Web Bridge.

Figure 1: Associating Web Bridges with Call Bridges and Call Bridge Groups



In Figure 1 above:

- Call Bridge 1 and Call Bridge 2 form Call Bridge Group 1, and Web Bridge 1 and Web Bridge 2 are associated with Call Bridge Group 1.
- Web Bridge 3 has Call Bridge 3 set.
- Web Bridge 4 has no Call Bridge Group or Call Bridge set, and therefore any Call Bridge (Call Bridge 1, Call Bridge 2, Call Bridge 3 or Call Bridge 4) may attempt to connect to Web Bridge 4.

2.1.2.1 How to set which Call Bridge Groups or specific Call Bridges connect to the components?

Perform a PUT on the API objects **`/webBridges`**, **`/recorders`**, and **`/turnServers`** with the following parameters set: ID of the **`callBridgeGroup`** and **`callBridge`** associated with the component.

2.2 Support for ActiveControl

From version 2.1, the Meeting Server supports ActiveControl for hosted calls. For participants using a Cisco SX, MX or DX endpoint with CE 8.3+ software installed, ActiveControl allows the meeting participant to receive details of the meeting and perform a few administrative tasks during the meeting, using the endpoint interface.

2.2.1 ActiveControl on the Meeting Server

The Meeting Server supports sending the following meeting information to ActiveControl enabled endpoints:

- Participant list (also known as the roster list) so that you can see the names of the other people in the call and the total number of participants,
- indicator of audio activity for the currently speaking participant,
- indicator of which participant is currently presenting,
- Indicators telling whether the meeting is being recorded or streamed, and if there are any non-secure endpoints in the call,
- on screen message which will be displayed to all participants, see Section 2.6.2.

In addition, the Meeting Server can control the following features on ActiveControl enabled endpoints:

- select the layout to be used for the endpoint,
- disconnect other participants in the meeting, see Section 2.2.4

Note: These features are configured using the API of the Meeting Server, see defaultLayout parameter on the API objects: /calls, /callLegProfile and /coSpace.

2.2.2 Limitations

- If an ActiveControl enabled call traverses a Unified CM trunk with a Unified CM version lower than 9.1(2), the call may fail. ActiveControl should not be enabled on older Unified CM trunks (Unified CM 8.x or earlier).
- ActiveControl is a SIP only feature. H.323 interworking scenarios are not supported.

Note: ActiveControl uses UDT transport for certain features, for example sending roster lists to endpoints and allowing users to disconnect other participants while in a call. See Section 2.2.4 for the steps to follow on the Meeting Server.

2.2.3 Overview on ActiveControl and the iX protocol

ActiveControl uses the iX protocol, which is advertised as an application line in the SIP Session Description Protocol (SDP). The Meeting Server automatically supports ActiveControl, and the feature cannot be disabled. In situations where the far end network is not known or is known to have devices that do not support iX, it may be safest to disable iX on SIP trunks between the Meeting Server and the other call control or Video Conferencing devices. For instance:

- for connections to Unified CM 8.x or earlier systems the older Unified CM systems will reject calls from ActiveControl-enabled devices. To avoid these calls failing, leave iX disabled on any trunk towards the Unified CM 8.x device in the network. In cases where the 8.x device is reached via a SIP proxy, ensure that iX is disabled on the trunk towards that proxy.
- for connections to third-party networks. In these cases there is no way to know how the third-party network will handle calls from ActiveControl-enabled devices, the handling mechanism may reject them. To avoid such calls failing, leave iX disabled on all trunks to third-party networks.
- for Cisco VCS-centric deployments which connect to external networks or connect internally to older Unified CM versions. From Cisco VCS X8.1, you can turn on a zone filter to disable iX for INVITE requests sent to external networks or older Unified CM systems. (By default, the filter is off.)

2.2.4 Disable UDT within SIP calls

ActiveControl uses the UDT transport protocol for certain features, for example sending roster lists to endpoints, allowing users to disconnect other participants while in a call, and inter-deployment participation lists. UDT is enabled by default. You can disable UDT for diagnostic purposes, for example if your call control does not use UDT, and you believe this is the reason the call control does not receive calls from the Meeting Server.

Using the Meeting Server API:

1. Create a compatibility profile with the sipUdt parameter set to “false”. Either POST sipUdt=false to the **`/compatibilityProfiles`** object or PUT to **`/compatibilityProfiles/<compatibility profile id>`** object
2. Disable the use of UDT at the system level, by adding the compatibilityProfile parameter and id (from step 1) to the system profile. PUT compatibityProfile=<compatibility profile id> to the **`/system/profiles/`** object.

2.2.5 Enabling iX support in Cisco Unified Communications Manager

Support for the iX protocol is disabled by default in Cisco Unified Communications Manager. To enable iX support, you must first configure support in the SIP profile and then apply that SIP profile to the SIP trunk.

Configuring iX support in a SIP profile

1. Choose **Device > Device Settings > SIP Profile**. The Find and List SIP Profiles window displays.
2. Do one of the following:
   a. To add a new SIP profile, click **Add New**.
   b. To modify an existing SIP profile, enter the search criteria and click **Find**. Click the name of the SIP profile that you want to update.

   The SIP Profile Configuration window displays.
3. Check the box for **Allow iX Application Media**
4. Make any additional configuration changes.
5. Click **Save**

Applying the SIP profile to a SIP trunk

1. Choose **Device > Trunk**.

   The Find and List Trunks window displays.
2. Do one of the following:
   a. To add a new trunk, click **Add New**.
   b. To modify a trunk, enter the search criteria and click **Find**. Click the name of the trunk that you want to update.

   The Trunk Configuration window displays.
3. From the SIP Profile drop-down list, choose the appropriate SIP profile.
4. Click **Save**.
5. To update an existing trunk, click **Apply Config** to apply the new settings.

2.2.6 Filtering iX in Cisco VCS

To configure the Cisco VCS to filter out the iX application line for a neighbor zone that does not support the protocol, the zone must be configured with a custom zone profile that has the SIP UDP/IX filter mode advanced configuration option set to On.

To update advanced zone profile option settings:

1. Create a new neighbor zone or select an existing zone (**Configuration > Zones > Zones**).
2. In the Advanced parameters section, for **Zone profile**, choose *Custom* if it is not already selected. The zone profile advanced configuration options display.
3. From the **SIP UDP/IX filter mode** drop-down list, choose **On**.
4. Click **Save**.

2.2.7 iX troubleshooting

Table 1: Call handling summary for calls that contain an iX header

Scenario	Outcome
Unified CM 8.x or earlier	Calls fail
Unified CM 9.x earlier than 9.1(2)	Calls handled normally but no ActiveControl
Unified CM 9.1(2)	Calls handled normally plus ActiveControl
Endpoint - no support for iX and no SDP implementation	Endpoint may reboot or calls may fail

2.3 Streaming meetings

Version 2.1 adds a new component: Streamer, to the Meeting Server. The Streamer component adds the capability of streaming meetings held in a space to the URI configured on the space.

An external streaming server needs to be configured to be listening on this URI. The external streaming server can then offer live streaming to users, or it can record the live stream for later playback.

Note: Several standards based streaming servers are known to work with the Streamer, but Cisco only offers support for VBrick as external streaming server.

The Streamer connects to an external server using RTMP with an overall bitrate of 2Mbps. The video is encoded using H.264 at 720p30, while the audio is 64kbps AAC-LC. All traffic between the Streamer and the external streaming server is unencrypted.

The Streamer should be hosted on another Meeting Server instance than the server hosting the Call Bridge, see Figure 2. If the Streamer is hosted on the same server as the Call Bridge (local), then it should only be used for testing purposes .

The recommended deployment for production usage of the Streamer is to run it on a separate VM. This VM should be sized with 1 vCPU and 1GB of memory per 6 concurrent streams, with a minimum of 4vCPUs and a maximum of 32vCPUs.

Note: These VM specifications are currently being evaluated, and the sizes are likely to be reduced.

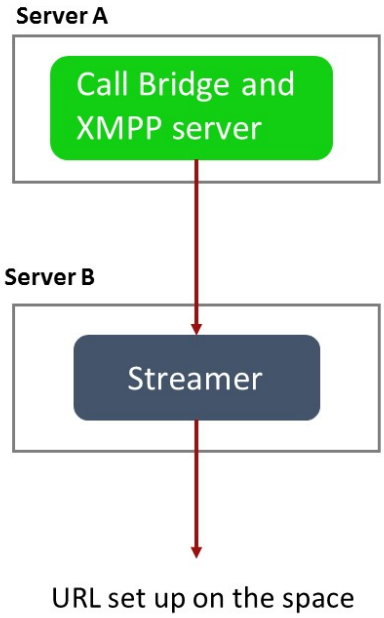
For more details on VM specification see Unified Communications in a Virtualized Environment - Cisco (www.cisco.com/go/uc-virtualized).

Where possible, it is recommended that the Streamer is deployed in the same physical locality as the Call Bridge to ensure low latency and high network bandwidth. If there are network

connection issues between the Call Bridge and the Streamer, then the resultant stream could be affected.

Note: you may need to open firewall ports if the streaming destination URIs are on the external side of a firewall.

Figure 2: Permitted deployment for streaming: remote mode



The Streamer also supports redundant configurations, see Figure 3, Figure 4, Figure 5 and Figure 6. If you use multiple streamers then the solution load balances between available streaming devices. To restrict the use of specific Streamers to specific Call Bridges use the Call Bridge Group functionality introduced in version 2.1.

Figure 3: Permitted deployments for streaming: multiple streamers

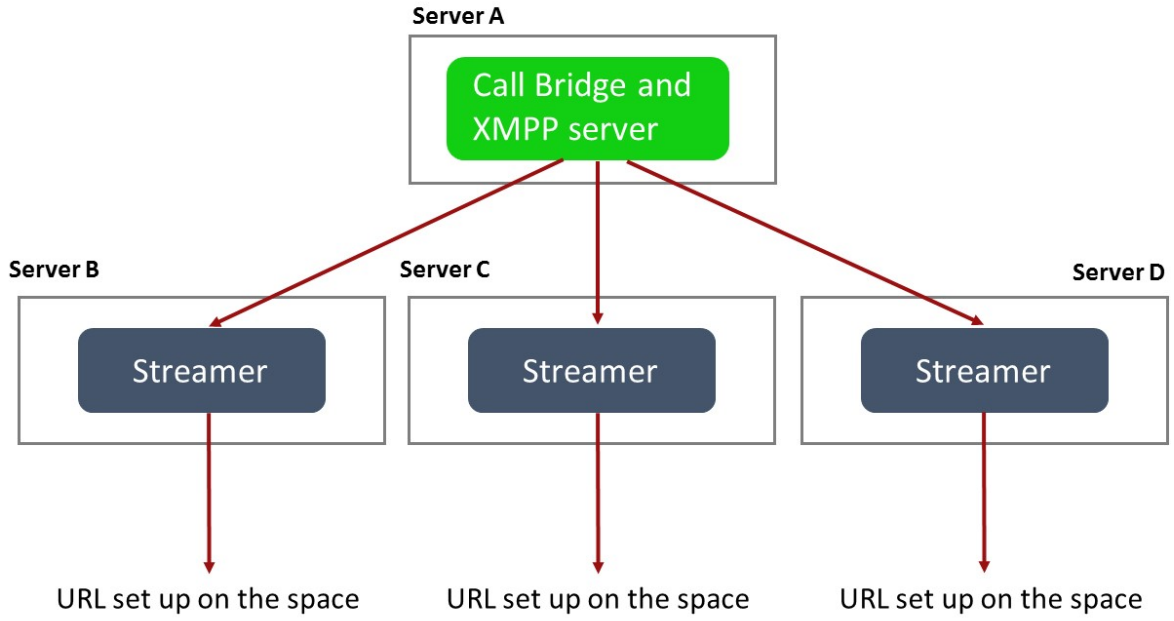
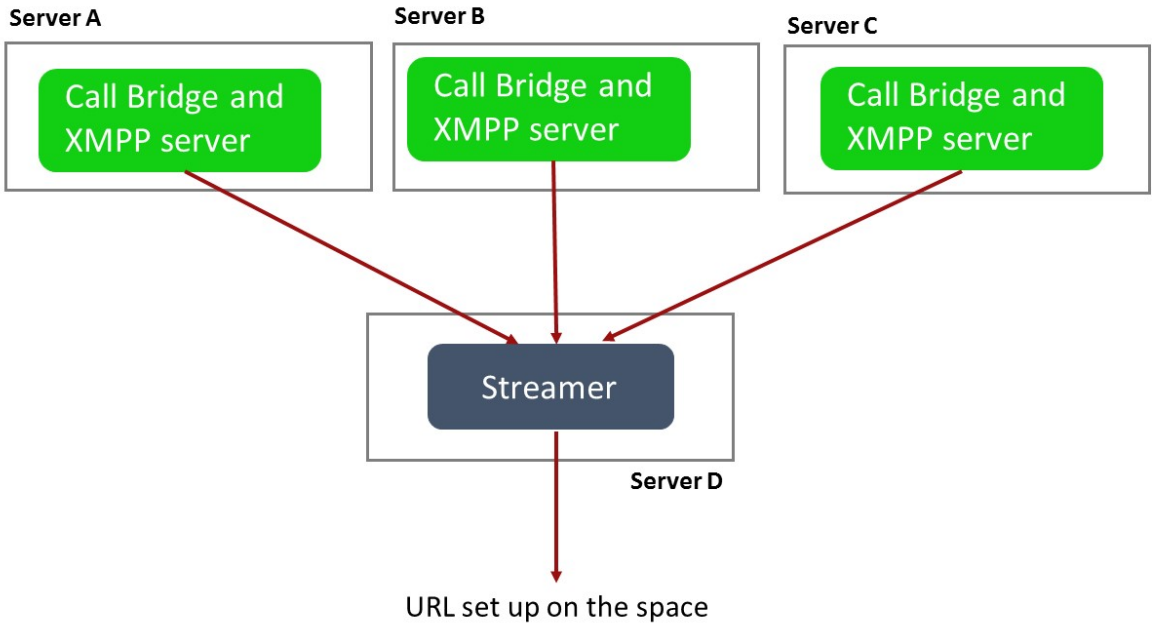


Figure 4: Permitted deployments for streaming: Call Bridge cluster



If your deployment has multiple Call Bridges and multiple Streamers then every Call Bridge will use every Streamer (see Figure 5), unless the callBridgeGroup and callBridge parameters have been set for each Streamer using the API to PUT to `/streamers/<streamer id>` (see Figure 6).

Figure 5: Permitted deployments for streaming: Call Bridge cluster with multiple Streamers and no Call Bridge Groups set up

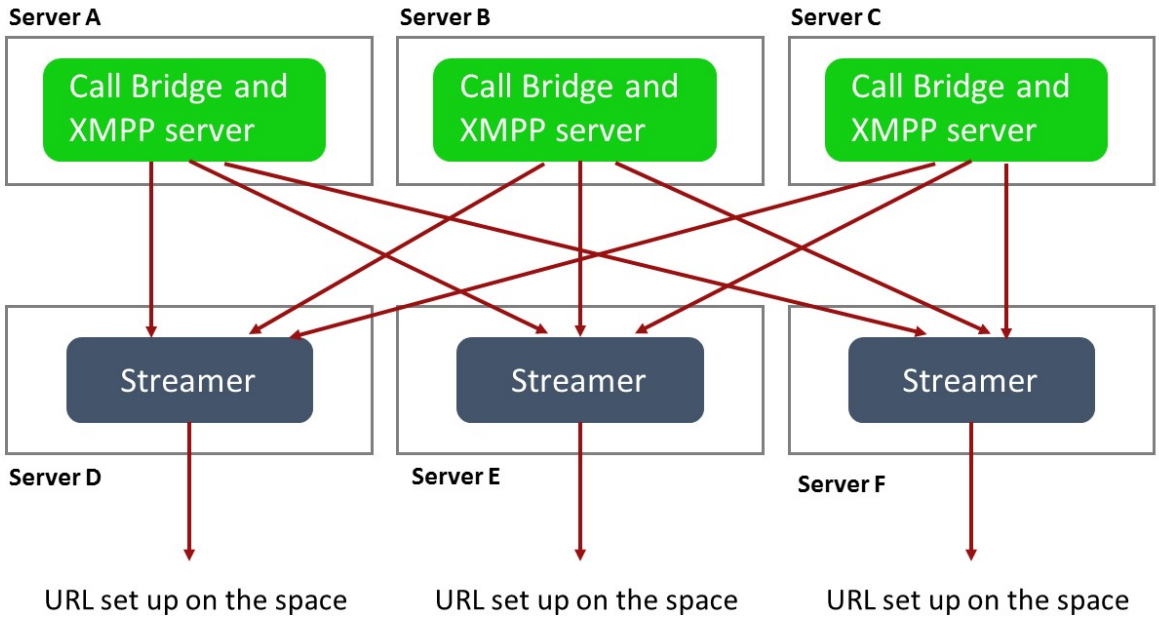
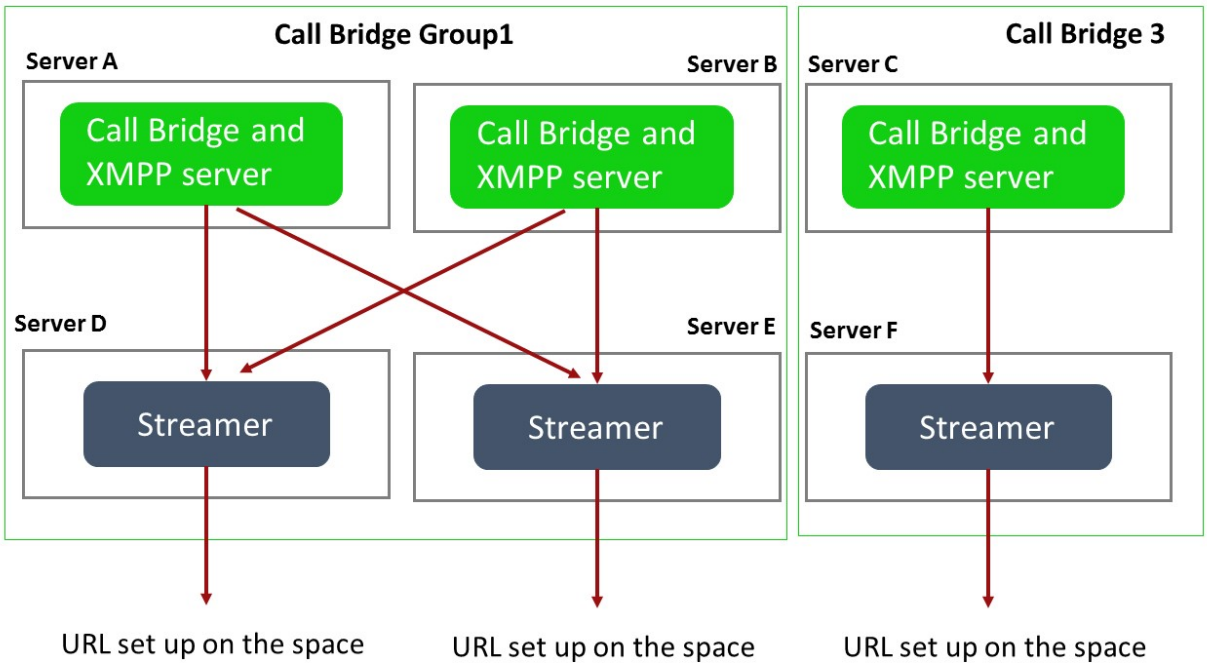


Figure 6: Permitted deployments for streaming: Call Bridge cluster with multiple Streamers and a Call Bridge Group and Call Bridge set up



For testing purposes, the Streamer can be co-located on the same server as the Call Bridge. This may support between 1 to 2 simultaneous streamings.

Note: Acano X series servers used in the single combined deployment mode should only be used for testing the Streamer, they should not be used in production networks to host the Streamer.

2.3.1 Overview of steps to configuring the Streamer

- Use MMP commands to configure and enable the Streamer on a Meeting Server and to add certificates.
- Use the API of the Meeting Server hosting the Call Bridge to configure the settings through which the Call Bridge will communicate with the Streamer, and where to save the streamings.
- Use the new **`streamingMode`** parameter on the API object **`/callProfiles`** or **`/callProfiles/<call profile id>`** to select whether a meeting can be streamed or not.

2.3.2 Example of deploying streaming

Note: The Streamer behaves as an XMPP client, so the XMPP server needs to be enabled on the Meeting Server hosting the Call Bridge.

This example gives the steps to deploy a streamer remote to the Call Bridge. It assumes that you already have a working Call Bridge and XMPP server.

1. Create a certificate and private key for the Streamer, following the steps described in the Certificates guidelines for an internal CA signed certificate.

2. SSH into the MMP of the Meeting Server hosting the Streamer.

3. Configure the Streamer to listen on the interface(s) of your choice with the following command:
   ```
   streamer listen <interface[:port] whitelist>
   ```
   The Streamer can listen on multiple interfaces, e.g. one on public IP and one on the internal network. (However, it cannot listen on more than one port on the same interface.)

   The following is an example where interfaces are set to interface A and B, both using port 8443.
   ```
   streamer listen a:8443 b:8443
   ```
   To use a local Streamer, the Streamer must listen on the loopback interface lo:8443, for example
   ```
   streamer  listen lo:8443 b:8443
   ```

4. Upload the certificate file, key file and certificate bundle to the MMP via SFTP.
   ```
   streamer certs <keyfile> <certificatefile> [<crt-bundle>]
   ```
5. Add the Call Bridge certificate to the Streamer trust store using the command:
   ```
   streamer trust <crt-bundle>
   ```
6. Use the streamer command to list the details for the streamer, for example:
   ```
   cms1> streamer
   Enabled                 : true
   Interface whitelist     : a:8445 b:8445
   Key file                : streamer0.key
   Certificate file        : streamer0.cer
   CA Bundle file          : streamer.crt
   Trust bundle            : callbridge.crt
   ```
7. Enable the Streamer:
   ```
   streamer enable
   ```
8. Create DNS A record for the Streamer and set it to resolve to the IP Address of the Ethernet interface you want the Streamer to listen on.

9. Use the API of the Meeting Server hosting the Call Bridge to configure the settings through which the Call Bridge will communicate with the Streamer.

a. Specify the HTTPS URL address that the Call Bridge will use to reach this streamer. Either POST the URL to the **/streamers** object or PUT to the **/streamers/<streamer id>** object

---

Note: If using a local Streamer, the URL must be the loopback interface, for example **https://127.0.0.1:8443**

---

b. POST to **/coSpaces** or PUT to **/coSpaces/<coSpace id>** the **streamUrl** which determines where streaming is streamed to, if streaming is initiated

c. Select whether a meeting can be streamed or not and whether the streaming will start without any user intervention. Use the **streamingMode** parameter on the API object **/callProfiles** or **/callProfiles/<call profile id>**

   Options for this are:

   automatic - streaming occurs without any user intervention, if streaming cannot occur the meeting still occurs.

   manual - users can manually start and stop the streaming using DTMF.

   disabled - no users can stream.

d. Control which users have permission to start and stop streaming. Use the **streamingControlAllowed** parameter on **/callLegProfiles**

e. For each space that a user would like to stream, POSTor PUT to **/coSpaces** the **streamURL** parameter specifying the destination URL to stream to.

Note: some streaming services require username and password, others provide a unique stream key. For example, for vBrick:
streamUrl=rtmp://<username>:<password>@<vbrick IP/FQDN>/live/PullStream1

and for YouTube:
streamUrl=rtmp://a.rtmp.youtube.com/live2/<stream key>

---

f. Use the **startStreaming** and **stopStreaming** parameters for **/dtmfProfiles** and **/dtmfProfiles/<dtmf profile id>** to map the DTMF tones for starting and stopping streaming. For example: **7 to start and **8 to stop streaming.

2.3.3 Streamer licensing

You will need one or more licenses for streaming which is loaded on the Meeting Server hosting the Call Bridge, not the server hosting the Streamer. One 'recording' license supports 1 concurrent streaming or 1 recording, existing recording licences will allow streaming. From version 2.1, a starter kit is available which includes one recording/streaming license or additional

ports. Contact your Cisco sales representative or partner to discuss your licensing requirements.

2.4 Improvements to the join meeting experience for participants using SIP endpoints

In releases prior to 2.1, it was possible to have multiple access methods that shared a URI, but each had to have a unique non-empty PIN. In 2.1, it is possible to mix PIN and no-PIN with the same URI. For instance, from version 2.1 it is possible to have separate host and guest PINs, with the host having a non-empty PIN and guests having an empty PIN. Guests have to press "#" (pound) to join the meeting or, if configured, guests can wait a specified amount of time to join the meeting.

To select the option to require guests to press '#' (pound) to join a meeting, set the **`passcodeMode`** parameter to **`required`** on **`/callProfiles/<call Profile id>`**

To select the option to automatically connect guests after a specified waiting time, set the **`passcodeMode`** parameter to **`timeout`** on **`/callProfiles/<call Profile id>`** and configure the value of the timeout via the **`passcodeTimeout`** parameter on **`/callProfiles/<call Profile id>`**.

To support these new combinations of URIs and PINs, and alter the join meeting experience for participants using SIP endpoints, two additional voice prompts and two additional background images are available for customization, see Table 2. If these additional files are not included in the branding archives, then the voice prompts and images used for passcode_entry will be used instead.

Table 2: Join Options for Meetings

Scenario	passcodeMode	Behavior	Background used	Voice prompt	Notes
All access methods have passcodes	NA	User prompted for passcode, must enter '#'	passcode_background.jpg	passcode_entry.wav	Used when below files not present. If not in archive then black background and no voice prompt.
Some access methods have passcodes	required	User prompted for passcode, must enter '#'	passcode_or_blank_required_background.jpg	passcode_or_blank_required_entry.wav	If not in customization archive then top case used.
Some access methods have passcodes	timeout	If user enters nothing, will join as if entered just '#'	passcode_or_blank_timeout_background.jpg	passcode_or_blank_timeout_entry.wav	If not in customization archive then top case used.
No passcode	NA	User joins without any additional input	NA	NA	

2.5 Support for Cisco Expressway X8.9

The Cisco Expressway X8.9 supports traversal of SIP traffic at the edge of the network, to and from the Cisco Meeting Server. This allows collaboration using Cisco Meeting spaces between on-premise Cisco Meeting App or SIP endpoint users, and users external to the network who are using standards-based SIP endpoints, Microsoft Skype for Business or Microsoft Office 365. Cisco Expressway does not currently support traversal for external Cisco Meeting App users. Cisco Expressway X8.9 is also previewing a Cisco Meeting Server web proxy to enable off-premise users to join meetings held in spaces using a web browser supporting WebRTC.

To use the Cisco Expressway X8.9 for TURN, rather than the TURN Server in the Meeting Server:

- ignore the TURN configuration section in the chapter on Configuring the MMP in the Meeting Server deployment guide. If you have already configured the TURN server, then disable it via the MMP command **`turn disable`**

  then either:

- use the Web Admin interface of the Cisco Meeting Server. Go to **Configuration>General** and type the Expressway IP address in the TURN Server address (server) field. The Cisco Meeting Server will use port 3478 to communicate with the Cisco Expressway.

or:

- use the Cisco Meeting Server API object **/turnServers** and set **type**=**expressway**.

For more information, see the Cisco Expressway X8.9 release notes.

2.6 Miscellaneous changes and improvements

Release 2.1 supports the following changes and new features:

- support for up to four CDR receivers,
- support for on-screen messaging,
- disconnect inactive calls,
- improvement to media handling on VMs,
- support for Oracle Internet Directory (LDAP version 3)
- support for Web Bridge 1.9,
- incoming calls to the Cisco Meeting App can be disabled,
- additional voice prompts and background images to allow new combinations of URI's and passcodes,
- Ad Hoc conferences might consume one PMP+ license rather than an SMP+ license.

2.6.1 Support for multiple CDR receivers

From version 2.1, the Meeting Server supports up to four CDR receivers, enabling you to deploy up to four different management tools, or duplicate instances of the same management tool for resiliency.

Note: The list of CDR receivers is held locally to an individual Call Bridge, it is not stored in the database shared between clustered Call Bridges.

To configure the multiple CDR receivers, POST each URI to the API object:

```
/system/cdrReceivers/<CDR receiver id>
```

or alternatively, configure the multiple CDR receivers through the Web Admin Interface, navigate to **Configure> CDR settings**, enter each receiver's HTTP or HTTPS URI.

2.6.2 On screen messaging

From version 2.1, the Meeting Server provides the ability to display an on-screen text message to participants in a meeting hosted on the Meeting Server; only one message can be shown at a time. The duration that the message is displayed can be set, or made permanent until a new message is configured.

For users of SIP endpoints and Lync/Skype for Business clients, the on-screen text message is displayed in the video pane. The position of the message in the video pane can be selected from top, middle or bottom.

On screen messaging is also sent to other devices that are using ActiveControl in the deployment, for instance CE8.3 endpoints, and individual Meeting Servers not in a cluster but with the in-call message feature enabled. Meeting Servers in a cluster also support on screen messaging through a proprietary mechanism.

Use the **`messageText`**, **`messagePosition`** and **`messageDuration`** parameters for API object **`/calls`**.

2.6.3 Disconnect inactive calls

SIP sessions between the Meeting Server and a call control device, for example Cisco Unified Communications Manager, can remain in place even if there is no longer any activity in the call. This situation can arise from a laptop battery dying while in the call, or from network problems.

From version 2.1, the Meeting Server will disconnect and end SIP calls when the Meeting Server detects no media activity in the call over a period of 60 seconds. This includes Lync and Skype for Business (S4B) calls with no media activity. For SIP, TIP, Lync and S4B calls that go on hold , if the call stops sending RTP/RTCP traffic, then after 60 minutes the call is disconnected, this is to prevent calls hanging around indefinitely.

2.6.4 Improvement to media handling on VMs

In version 2.1 of the VM software release, the media code is isolated from the rest of the Call Bridge code. This means that the media code can be restarted without dropping ongoing calls or loss of any other functionality. There will simply be a brief pause in media during a restart.

2.6.5 Support for Oracle Internet Directory

From version 2.1, the Meeting Server supports Oracle Internet Directory (LDAP version 3). This must be configured through the API, not the Web Admin interface.

To configure the Meeting Server to support Oracle Internet Directory, the Meeting Server should not use the LDAP paged results control in search operations during LDAP sync. POST to **`/ldapServers`** or PUT to **`/ldapServers/<ldap server id>`** the request parameter **`usePagedResults`** set to false .

2.6.6 Reverting to Web Bridge 1.9

From version 2.1.2, the Meeting Server no longer supports Web Bridge 2.0, instead it supports Web Bridge 1.9 and :

- the original look and feel for the Web RTC app.
- the background image for login to the WebRTC app can be customized. For more information, refer to the Customization guidelines.

Note about browser to use with WebRTC App: We strongly recommend only using the most recent version of Chrome, see this FAQ.

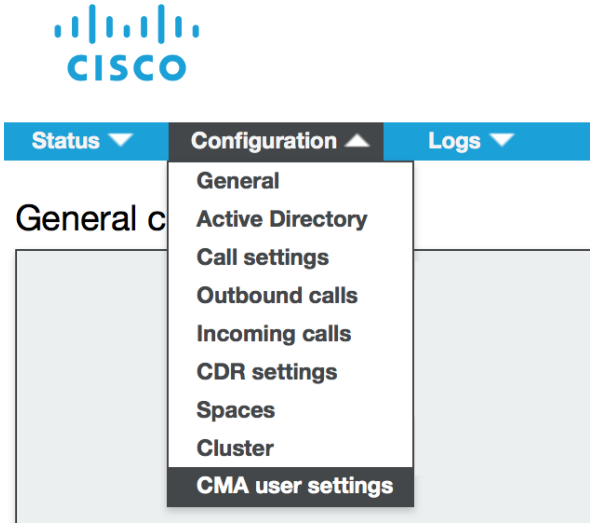
2.6.7 Incoming calls to Cisco Meeting Apps

From Meeting Server version 2.1, incoming calls to the Cisco Meeting App can be disabled.

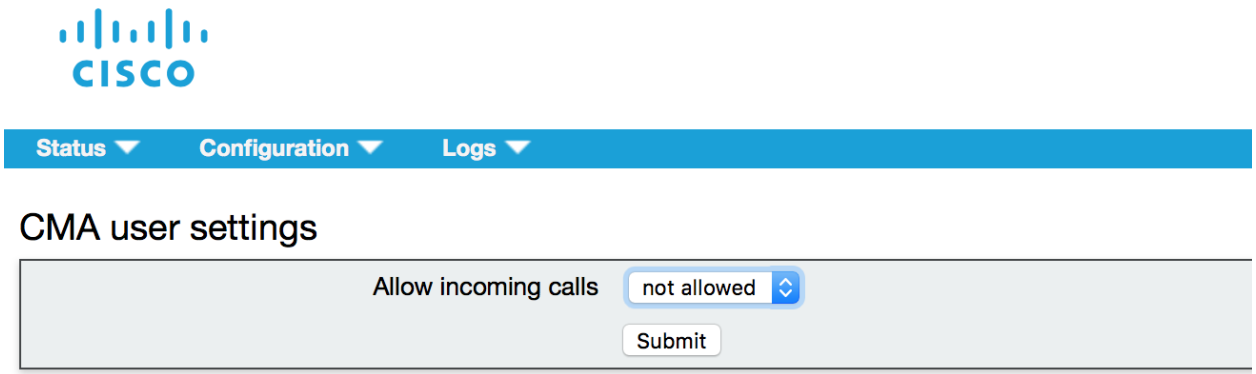
By default incoming calls to Cisco Meeting Apps are allowed, however this behavior can be changed so that incoming calls are not allowed to users of the Cisco Meeting App. Follow these steps:

Either:

1. Login to the Web Admin interface of the Meeting Server, go to **Configuration**>**CMA user settings**.



2. Set **Allow incoming calls** to **not allowed** and select **Submit**.



or use the API object to either POST to /userProfiles or PUT to /userProfiles/<user profile id> the request parameter canReceiveCalls = “false”.

2.6.8 Additional voice prompts and background images

Version 2.1 supports additional voice prompts and background images to allow new combinations of URI’s and passcodes. These alter the join meeting experience for participants using SIP endpoints.

The new voice prompts are:

Filename	Text of message	Repeating?	Played when ...
passcode_or_ blank_required_ entry.wav	Please enter the PIN, followed by the '#' (pound) key.	No	a PIN is required for the host to enter the space as host, but guests only need to use the # (pound) key.
passcode_or_ blank_timeout_ entry.wav	Please enter the PIN, followed by the '#'(pound) key.	No	a PIN is required for the host to enter the space as host, but guests join after a short timeout.

The new background images are:

Filename to use	Image used when ....
passcode_or_blank_ required_background.jpg	Screen can be shown when a PIN is required for the host to enter the space as host, but guests only need to use the # (pound) key.
passcode_or_blank_ timeout_background.jpg	Screen can be shown when a PIN is required to enter the coSpace as host, but guests join after a short timeout.

New API parameters of **`passcodeMode`** and **`passcodeTimeout`** for **`/callProfiles`** and **`/callProfiles/<call profile id>`** are provided to select the join meeting experience. See Section 2.8.8.

2.6.9 Ad Hoc conference license consumption

Before release 2.1, Ad Hoc conferences never consumed PMP+ licenses. With this 2.1 release, the initiator of the Ad Hoc conference can be identified and if they have been assigned a PMP+ license then that is used for the conference.

2.7 Summary of MMP changes

Version 2.1 supports these additional MMP commands.

2.7.1 MMP commands for the Streamer

Command	Description
`streamer restart`	Restarts the Streamer
`streamer`	Displays the current configuration of the Streamer
`streamer listen <a|b|c|d|lo|none [:<port>] whitelist>` `streamer listen a b`	Sets up the interface(s) and port(s) for the Streamer to listen on. You must enable the service to start listening with the command recorder enable. The default for the optional port argument is 443.
`streamer listen none`	Stops the Streamer listening.
`streamer (enable|disable)`	Enables or disables the Streamer. You need to disable the Streamer before configuring it. After configuration, you need to enable the Streamer.

`streamer certs <keyfile-name> <crt filename> [<crt-bundle>]`
 	
`streamer certs none`
	Provides the name of the key file and .crt file for the Streamer and, optionally, a CA certificate bundle as provided by your CA
	
	Removes certificate configuration

`streamer trust <crt-bundle|crt-file>`
 	
`streamer trust none`
	Controls which Call Bridge instances are allowed to connect to the Streamer.
	If the trusted Call Bridge is running on the same server as the Streamer, then issuing the streamer trust command with the name of the Call Bridge public certificate/certificate bundle is sufficient. If the Call Bridge is running on another server, the public certificate/certificate bundle of the Call Bridge must first be copied to the server with the enabled Streamer using SFTP.
	
	Deconfigures any trust settings

2.8 Summary of API Additions & Changes

New API functionality for the Meeting Server 2.1 includes support for:

- grouping Call Bridges
- load balancing of calls across Call Bridges
- streaming calls
- ActiveControl
- on screen messaging
- Oracle Internet Directory
- disable incoming calls to users of Cisco Meeting App
- altering the join meeting experience for participants using SIP endpoints

there are also some other minor additions.

2.8.1 Support for grouping Call Bridges

- New API object to enable the grouping of Call Bridges : **`/callBridgeGroups`**

  Note: Load balancing calls across Call Bridges in a group is disabled by default.

- New request parameter to **`/callBridges`** : **`callBridgeGroup`**
- New request parameters to **`/recorders`** : **`callBridge`**, **`callBridgeGroup`**
- New request parameters to **`/turnServers`** : **`callBridge`**, **`callBridgeGroup`**
- New request parameters to **`/webBridges`** : **`callBridge`**, **`callBridgeGroup`**
- New failure reason : **`callBridgeGroupDoesNotExist`**

2.8.2 Support for load balancing across Call Bridges

- New request parameter to **`/callBridgeGroups`**: **`loadBalancingEnabled`**
- New request parameter to **`/callBridgeGroups`**: **`loadBalanceLyncCalls`**
- New request parameters to **`/system/configuration/cluster`**: **`loadLimit`**, **`newConferenceLoadLimitBasisPoints`**, **`existingConferenceLoadLimitBasisPoints`**
- New API object: **`/system/load`** that returns a numeric value for **`mediaProcessingLoad`**

2.8.3 Support for streaming meetings

- New API object to enable the streaming of meetings hosted on the Meeting Server : **`/streamers`**

- New request parameter to **/coSpaces** : **streamUrl**
- New request parameter to **/calls** : **streaming**
- New request parameter to **/callProfiles** : **streamingMode**
- New request parameter to **/callLegProfiles** : **streamingControlAllowed**
- New request parameters to **/dtmfProfiles** : **startStreaming**, **stopStreaming**
- New response value for **/calls/<call id>** : **streaming**
- New status value returned on **/callLegs/<call leg id>** : **streaming**
- New alarm type for **/system/alarms**: **streamer unavailable**
- New response value for features field of **/system/licensing** : **streaming**
- New failure reasons : callStreamingCannotBeModified, streamerDoesNotExist, streamingLimitReached

2.8.4 Support for ActiveControl

- New request parameter to /**callLegProfiles** : **disconnectOthersAllowed**. POST to **/callLegProfiles** to create a new call or PUT to **/callLegProfiles/<call leg profiles id>** if modifying an existing call.

  The setting determines whether participants can drop others from a call when they are using an endpoint that can support ActiveControl.

  The default setting is *true*.
- New status section returned on **/callLegs/<call leg id>** : **activeControl**

  Note: If ActiveControl has been negotiated with the remote party, the callLeg information returned will include an **activeControl** section. Within that section, you can see whether the ActiveControl connection is encrypted.
  encrypted: *true* - an encrypted ActiveControl has been negotiated with the remote party.
  encrypted: *false* - ActiveControl has been negotiated with the remote party, but it is not encrypted.

- New request parameter to **/compatibilityProfiles** and **/compatibilityProfiles<compatibility profile id>**: **sipUdt**

2.8.5 Support for on screen text

- New request parameters to **/calls** : **messageText**, messagePosition, messageDuration. POST to **/calls** to create a new call or PUT to **/calls/<call id>** if modifying an existing call.

- New response value for **/calls/<call id>** : **messageText**, **messagePosition**, **messageDuration**, **messageTimeRemaining**

Note: a message can be permanently displayed.

2.8.6 Support for Oracle Internet Directory

New request parameter to **/ldapServers**: **usePagedResults**

2.8.7 Disable incoming calls to users of Cisco Meeting App

- New request parameter to **/userProfiles/<user profile id>**: **canReceiveCalls**

2.8.8 Selecting the join meeting experience for participants using SIP endpoints

New request parameters to **/callProfiles** and **/callProfiles/<call profile id>**: **passcodeMode**, **passcodeTimeout**

2.8.9 Other minor additions

To support a user (imported through AD) being added as owner of a space:

- added new request parameter to **/coSpaces** : **ownerADGuid**

To support retrieval of meeting entry details for a specific space:

- added “meetingEntryDetail” node. Perform a GET on **/coSpaces/<coSpace id>/meeting EntryDetail** to obtain the uri and CallId.

To improve filtering on **/users**:

- added **emailFilter**, which if supplied, will restrict results returned to those users whose email value exactly matches the specified email address.
- added **cdrTagFilter**, which if supplied, will restrict results returned to those users whose cdrTag value exactly matches the specified cdrTag.

Additional TURN server types provided for **/turnServers**:

- **expressway** indicates the Cisco Expressway X8.9 TURN server is used.
- **cms** is equivalent to **acano** which is retained for legacy deployments.

To support external tools to the Meeting Server determining whether they have received all CDR records that have been sent. (From version 2.1.5)

- New request parameter added to **/system/status**: **cdrCorrelatorIndex**

2.9 Summary of CDR Additions & Changes

Version 2.1 introduces the following changes to the Call Detail Records of the Meeting Server:

- support for up to 4 CDR receivers,
- new **`subType`** of **`distributionLink`** in the **`callLegStart record`**, indicates when the call leg is a conference distribution link to another Call Bridge in the cluster,
- new parameter **`replacesSipCallId`** in the **`callLegStart record`**, and new reason for call ending of **`callMoved`** in **`callLegEnd`** record.

2.10 Cisco endpoints no longer supported

From version 2.1, the Meeting Server is no longer tested for interoperabililty with these endpoints:

- Cisco TelePresence System 3200 Series
- Cisco TelePresence System 3000 Series
- Cisco TelePresence System 1300 Series
- Cisco TelePresence System 1000
- Cisco TelePresence System 500-37 (only with 37 inch display)

As a consequence Meeting Server 2.1 does not support the endpoints listed above, nor will related bugs be fixed in version 2.1.

Note: Version 2.0 of the Meeting Server will continue to support the endpoints listed above.

3 Notes on Installing and Upgrading to Cisco Meeting Server 2.1

This section assumes that you are upgrading from Cisco Meeting Server software version 2.0. If you are upgrading from an earlier version, then Cisco recommends that you upgrade to 2.0 first following the instructions in the 2.0.x release notes, before following any instructions in these Cisco Meeting Server 2.1 Release Notes.

Note: Cisco has not tested upgrading from a software release earlier than 2.0.

To check which version of Cisco Meeting Server software is installed on a 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 2.1

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 2.1.12 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.

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_1_12_vm-upgrade.zip

   This file requires unzipping to a single upgrade.img file. Use this file to upgrade vm deployments, follow the instructions below.

   Cisco_Meeting_Server_2_1_12.vhd

Use this file to upgrade Microsoft Hyper-V deployments

Cisco_Meeting_Server_2_1_12_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_1_12.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 2.1.12 release are shown in a pop up box that appears when you hover over the description for the download.
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:
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 apply the upgrade, issue the upgrade command.

   a. Establish a SSH connection to the MMP and log in.

   b. Initiate the upgrade by executing the upgrade command.
   `upgrade`
   The Server/ virtualized server restarts automatically: allow 10 minutes for the process to complete.

6. Verify that the Meeting Server is running the upgraded image by re-establishing the SSH connection to the MMP and typing:
   `version`
7. Check the **Configuration > Outbound Calls** rules updating the Local Contact Domain field and completing the new Local From Domain field if necessary.

8. Update the customization archive file when available.
9. 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.
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 & Resilience Deployment Guide.
11. 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 2.1 Deployments

To simplify explaining how to deploy the Meeting Server, deployments are described in term 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 installing the Meeting Server for the first time on 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 (installation guide for 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.

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

If you are installing the Meeting Server for the first time 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 Resolved Issues

Resolved in Meeting Server 2.1.12

Cisco identifier	Summary
CSCvh31022	Using Cisco Meeting App 1.10 for desktop or WebRTC and selecting the option “Use my phone” to call a number, results in a dial transform not being applied to the outbound call.
CSCvh24431	A cache issue prevents the Meeting Server WebRTC from working with Cisco Expressway.
CSCvg49776	Using the WebRTC 1.9 app in Finnish, username is incorrectly spelt as " Käyttääjnimi" .
CSCvg42618	Under rare circumstances, the Meeting Server can unexpectedly restart after a SIP participant has joined a conference.
CSCvg41087	A media module on the Meeting Server, crashed with 'mf_remote_media!mf_pipe_source_run' message. Note: that this restart will not be observed by any users, as media module restarts do not affect users.
CSCvf87952	After many hundreds of thousands of calls, the Meeting Server can get into a state where it will stop sending RTCP packets to SIP participants. This can sometimes result in video not being decoded from these participants.
CSCvf84935	Occasionally, the Meeting Server may restart after some calls are put on hold.
CSCvf78852	In some virtual dual NIC environments, reducing the MTU of any non-default interface to 1280 or lower results in a loss of network connectivity.
CSCve14298	Using the WebRTC 1.9 app in Finnish, the “ Sign in” button was incorrectly labelled as " Liity" .

Resolved in Meeting Server 2.1.11

Reference	Issue	Summary
SERVER-6643/ CSCvf42693	Attempting to resolve a blank call ID for a Lync conference could cause the Meeting Server to restart.	Fixed in 2.1.11.
SERVER-6613/ CSCvf36654	In some call flows through a Cisco Unified Communications Manager, calls placed on hold to a Meeting Server may be disconnected after a period of time.	Fixed in 2.1.11.

Reference	Issue	Summary
SERVER-6612/ CSCvf36154	During some database to Call Bridge syncs, an unnecessarily large number of records may be updated, possibly reducing performance on heavily loaded systems or preventing some data from being updated.	Fixed in 2.1.11.
SERVER-6302/ CSCvf51295	Some error messages in WebRTC calls may be incorrectly displayed in English when using the Japanese language pack.	Fixed in 2.1.11.
SERVER-5868/ CSCvf31494	In AVMCU meetings, SIP endpoints could have an avatar displayed rather than their main video.	In an AVMCU meeting where media is encrypted between the AVMCU and the Meeting Server, if the spotlight is locked on any participant for 15 minutes or longer, then on unlocking it, a SIP endpoint could be displayed as an avatar. Fixed in 2.1.11.
SERVER-5825/ CSCve08594	After a period of time, an H.323 GW can stop accepting new calls. A restart of the H.323 GW fixes this problem.	This problem could occur if the TCP channel for the H.245 connection for a particular H.323 call had closed while the call was still connected. Fixed in 2.1.11.

Resolved in Meeting Server 2.1.10

Reference	Issue	Summary
SERVER-6475/ CSCvf14323	If a customized background image is in use, the background image is repeatedly loaded when lots of participants in a space need to be activated or deactivated en masse (for instance because a host joins a space with lots of guest users). If this background image file is fairly large, it causes an extra load on the system, which can eventually lead to a restart of the Meeting Server.	Fixed in 2.1.10.
SERVER-6464/ CSCve95813	A rare thread synchronization error can result in a media process crash. Users might experience a brief interruption in media while objects are moved to another media framework.	Fixed in 2.1.10.
SERVER-6449/ CSCve87518	Participant name labels are missing in layouts with PIPs, for example stacked layout.	Fixed in 2.1.10.
SERVER-6444/ CSCve83819	Content sharing in dual-home call to Lync/SfB Client shows black screen when Lync proxy connection is used.	Fixed in 2.1.10.

Reference	Issue	Summary
SERVER-6424/ CSCve72610	Chat messages do not appear in the chat window for a non-member user connected to a space.	This occurs when the /callProfile has parameter “messageBoardEnabled” initially set to false, but is subsequently changed to true. Fixed in 2.1.10.
SERVER-6391/ CSCve62662	A resource leak could lead to the H.323 Gateway component crashing.	Fixed in 2.1.10.
SERVER-6343/ CSCve49642	If a new distributed peer link is established 'after' a permanent messageText has been sent for a particular call, participants over the distributed link are not shown this message.	Fixed in 2.1.10.
SERVER-6342/ CSCve49637	TX9000/IX5000 does not receive video after Hold/Resume if a Session Border Controller (SBC) is within the call path.	Fixed in 2.1.10.
SERVER-6286/ CSCve35060	H.323 Gateway calls through an IVR will be disconnected if the overall server setting for encryption is “Allowed”, but encryption is “Required” for the space.	Fixed in 2.1.10.
SERVER-6179/ CSCve18588	The H.323 Gateway crashes, causing all calls to be dropped.	This issue is a result of a resource leak caused by a race conditiun between a new media stream being set up, and the call that the media stream belongs to being ended. Fixed in 2.1.10.
SERVER-4824/ CSCve08092	When making an outgoing call to a Lync client with videoMode set to disabled, the call rings on the Lync client but then drops shortly afterwards.	Fixed in 2.1.10.
SERVER-4555/ CSCvf21193	If custom branding resources (call branding or IVR branding) should be used for a call leg and the web server hosting these resources is unavailable, then the Meeting Server will wait for up to two minutes for a TCP response on every call leg in the conference before giving up and joining the endpoint to the conference.	Fixed in 2.1.10. After this bug fix, the Meeting Server will delay the first call that needs custom branding resources for a short time before determining that they are not available, and proceeding without them. Subsequent calls will not be delayed.
CLIENT-5610/ CSCve35856	If a logged in user calls into a space that they aren’t a member of using the WebRTC app, the log in box displays “Type passcode”, even if the passcode is optional.	Message has changed to “Type passcode if required”. Fixed in 2.1.10.

Resolved in Meeting Server 2.1.9

Reference	Issue	Summary
SERVER-6401 CSCve70685	Occasionally, the Cisco Meeting Server restarts when a participant is put on hold and then activated.	Fixed in 2.1.9.
SERVER-6362/ CSCve65931	Multiple Call Bridges configured as a group may cause the Cisco Meeting Server to restart during PIN entry.	Fixed in 2.1.9.
SERVER-6267/ CSCve70201	Audio quality significantly degrades during very high load. This may happen during peak hours when hundreds/thousands of audio and video calls as well as hundreds of distributed links are being hosted on a Meeting Server.	Fixed in 2.1.9.

Resolved in Meeting Server 2.1.8

Reference	Issue	Summary
SERVER-6274/ CSCve31915	If a Lync participant locks the spotlight on itself, participants on a remote Call Bridge will then see only participants on that Call Bridge, rather than the Lync participant as expected.	This issue occurred in dual homed meetings involving a cluster of Call Bridges. Fixed in 2.1.8.
SERVER-6255/ CSCve22901	If a member is logged into the Cisco Meeting App and observing their space when a participant calls into the space, sometimes the member sees the name of the new participant appear in green under the space name, but not always.	Fixed in 2.1.8.
SERVER-6206/ CSCve21895	Frozen video from Skype for Business clients in a dual-homed conference is sent to SIP endpoints.	Fixed in 2.1.8.
SERVER-6204/ CSCve22765	Incoming callers to a Cisco Meeting Server space may hear inconsistent voice prompts when Call Bridge Groups are in use.	If a conference is hosted on the Call Bridge that the first participant connects to, the expected voice prompts are heard. If, however, the Call Bridge moves this first participant to a different Call Bridge for load balancing, then participants in this meeting will not hear the " Welcome to a Cisco meeting. You are entering the meeting now" voice prompt when they connect. Fixed in 2.1.8.
SERVER-6197/ CSCve18884	In some rare circumstances, dropped video frames and throttling can occur in video sent from a Cisco Meeting Server, even when the unit is not heavily loaded.	Fixed in 2.1.8.

Reference	Issue	Summary
SERVER-6164/ CSCve28532	Presentation is not seen on XMPP participants connected to a different core server in a clustered deployment to the one that has the call to the AVMCU conference.	This affected Cisco Meeting App users, including WebRTC app users. Fixed in 2.1.8.
SERVER-6160/ CSCve20873	Guests can join via a hyperlink even when guest access via hyperlink is set to disabled.	Fixed in 2.1.8.
SERVER-5997/ CSCve07146	If the firewall is configured for default deny, and to allow TCP traffic on port 514, syslog messages cannot be sent from the Cisco Meeting Server to a syslog server.	Fixed in 2.1.8.
SERVER-5847/ CSCve08787	Calls to Cisco Spark drop after 30 minutes due to a timeout. Call is ended by the Spark side due to “Media inactivity timer disconnect”.	This occurred when the Call Bridge is on a public IP, without any proxy in the SIP signalling path (e.g. Cisco Unified Communications Manager, Cisco VCS). Fixed in 2.1.8.
SERVER-4824/ CSCve08092	When making an outgoing call to a Lync client with videomode=disabled set in the API request, the call rings on the Lync client then drops shortly afterwards.	Fixed in 2.1.8.

Resolved in Meeting Server 2.1.7

Reference	Issue	Summary
SERVER-6184	A Call Bridge can restart when a Lync conference is ended at the same time as the Lync inter-cluster distribution call leg arrives at that Call Bridge	Fixed in 2.1.7.
SERVER-6136	If a full database sync between nodes fails, for example following an LDAP sync, then any video calls to a space could be torn down by the Meeting Server, and new calls through IVRs are no longer possible, until a database sync has succeeded.	Fixed in 2.1.7.
SERVER-5931	In a large scale clustered deployment, changing the URIs of a large number of spaces at once, for example by adding a new highest priority dial plan rule, can cause a service outage.	Fixed in 2.1.7.
SERVER-5779	If video from a Meeting Server is ended on a Lync client then restarted, there could be a delay of several minutes before video from the Meeting Server is seen again by the Lync client.	Fixed in 2.1.7.

Reference	Issue	Summary
CLIENT-5731	The French language translations for the following text prompts have been improved: “Your browser does not support video calls, or support has been disabled by an administrator. To join the call, copy this text into the address bar of a supported browser:” and “Join call in app”	Fixed in 2.1.7.

Resolved in Meeting Server 2.1.6

Reference	Issue	Summary
SERVER-6165	On a single Call Bridge deployment, if a Web RTC app guest user is the first participant to join a conference in a space, and a permanent user who's a member of the space is instantiated on the Call Bridge, the conference will be permanently locked for the duration of the conference.	Restarting the Server will cause the guest access to the space to unlock as expected. Fixed in 2.1.6.
SERVER-6074	Cisco Meeting App guest users can join spaces even when nonMemberAccess is set to False, and can send and receive audio and video to and from other Cisco Meeting App guest users in the space.	Fixed in 2.1.6.
SERVER-6027	If the connection from a Call Bridge to a Web Bridge is lost while a request for a WebRTC guest login is processed it may result in a Call Bridge crash.	The lost connection could be caused by a number of things, for example a network problem, or if theWeb Bridge was removed using the Call Bridge API. Fixed in 2.1.6.
SERVER-6001	An H.323 Gateway crash can occur as a result of a race condition between tearing a call down and responding to a BFCP message from the Call Bridge.	Fixed in 2.1.6.
SERVER-5956	On some rare occasions, a Call Bridge could restart after tearing down the peer link for a conference distributed between two clustered Call Bridges.	Fixed in 2.1.6.
SERVER-5925	If a call's SIP TCP or TLS connection is torn down, the Meeting Server could try to re-establish a connection to the remote address that the original SIP connection came from, rather than using the remote address specified in the appropriate Via header. This would result in the call itself being torn down.	Fixed in 2.1.6.

Reference	Issue	Summary
SERVER-5880	If no Lync participants are present in an AVMCU call, and several clustered Call Bridges are connected to the AVMCU call, then disconnecting all participants from one of the Call Bridges will cause all participants on the other Call Bridges to be disconnected too.	Fixed in 2.1.6.
SERVER-4848	An incoming SIP call to the H.323 Gateway can crash the gateway.	This crash of the H.323 Gateway can happen a) during REINVITE, where a bug in the SIP stack can cause the Meeting Server to end up in a state without any transactions, or b) during an H.323 Gateway call, a certain call-back pointer can be null before use, causing the gateway to crash. Fixed in 2.1.6.
SERVER-4332	Outbound calls to an Avaya Session Manager fail after 32 seconds	The Meeting Server incorrectly treated URIs in SIP Record-Route headers as case sensitive, which could result in SIP ACKs being sent to the wrong address, causing the call to be torn down. Fixed in 2.1.6.

Resolved in Meeting Server 2.1.5

Reference		Issue	Summary
-	SERVER-5899	Cisco Meeting Server database stops syncing with database cluster after becoming slave from being master.	When the master database fails, a slave database takes over as the master database. Once the previous master database comes back online, it is now a slave but stays out of sync with the new master database and other slave databases, even if rebooted. Fixed in 2.1.5.
-	SERVER-5873	Occasionally, a Lync 2010 client stops receiving incoming video after the active speaker switches between other participants.	Fixed in 2.1.5.
-	SERVER-5788	The CDR receiver field has a 100 character limit which can cause issues for longer hostnames.	Fixed in 2.1.5 by increasing the limit.

Reference		Issue	Summary
-	SERVER-5706	A participant leaving a clustered Call Bridge connected to a Lync conference, may result in the Call Bridge crashing when further cluster look ups are received.	This is caused by the local conference being destroyed when the participant leaves, causing the local conference to be torn down and further cluster lookups failing. Fixed in 2.1.5.
11363	SERVER-4790	Lync 2013 and S4B 2016 clients crash when receiving content from a Cisco Meeting Server deployment.	Pressing the 'actual size' button on Lync/S4B clients when receiving content from a Meeting Server deployment causes the Lync/S4B clients to crash. Experienced after upgrading to patch KB3115268 for S4B and patch KB3114944 for Lync 2013. This has been fixed by Microsoft, install the KB3141501 update for Skype for Business 2016. This updated Microsoft client will work with any 2.1 release of the Cisco Meeting Server software.
10717	SERVER-4467	Content sharing from Meeting Server to Lync client fails.	When the Meeting Server starts content sharing to a Lync client, the Call Bridge becomes the ICE controlling agent, but does not send the USE-CANDIDATE attribute in the Binding Request. This causes content sharing to the Lync client to fail. Fixed in 2.1.5.

Resolved in Meeting Server 2.1.4

Reference		Issue	Summary
-	SERVER-5927	The Meeting Server crashes when transferring a call from one endpoint to another before entering the call ID.	After dialing into an IVR and then transferring the call to a different endpoint before the call ID has been entered, the Meeting Server crashes when the ID is entered from the second endpoint. Fixed in 2.1.4.
-	SERVER-5863	Chat within a space from Cisco Meeting App or WebRTC app users not received by Lync client.	Lync client users in a space with Cisco Meeting App or WebRTC App users can send chat to the space, the Cisco Meeting App and WebRTC App users see the chat, but when they reply the Lync client user does not see the reply. Fixed in 2.1.4.
-	SERVER-5826	Web Bridge crashes if set in legacy mode and guest dials into a space with an incorrect passcode.	Fixed in 2.1.4.

Reference		Issue	Summary
-	SERVER-5805	Redirection of calls fail for Call Bridge Groups if port other than 5060 used on SIP trunk to Cisco Unified Communications Manager.	If the SIP trunk to Cisco Unified Communications Manager is set to use a port other than 5060, for example 5062, the redirection of calls for Call Bridge Groups fails as the Call Bridge sends the SIP Replace message to TCP port 5060, and the Cisco Unified Communications Manager rejects it with 503/Service Unavailable message. Fixed in 2.1.4, by using the port from the contact header from the initial INVITE, in this case, port 5062.
-	SERVER-5522	Encrypted outgoing call from a Call Bridge Group failed to connect to the Cisco Unified Communications Manager.	If there is no outbound rule pointing back to CUCM, an encrypted outbound call would always be used when a call is Replaced, resulting in the call failing if the trunk to CUCM is set as TCP. Fixed in 2.1.4 by ensuring the SIP encryption setting of the REPLACE Invite is the same as the incoming call.
-	SERVER-5516	Participant limit on a call is ignored when a participant joins the call via a SIP Replace.	Fixed in 2.1.4.
-	CLIENT-5574	WebRTC App user unable to join as a guest using an Access Method with no passcode, if the host Access Method has a passcode and using the same call ID.	Fixed in 2.1.4.

Resolved in Meeting Server 2.1.3

Reference		Issue	Summary
-	SERVER-5758	Unable to disable load balancing for Lync calls	Fixed in 2.1.3.
-	SERVER-5753/ SERVER-4686	Under sustained heavy loading of Ad Hoc and Rendezvous calls, the Meeting Server occasionally drops calls due to a media module crashing	Fixed in 2.1.3

Reference		Issue	Summary
-	SERVER-5712	Sometimes the Cisco Meeting App failed to successfully launch for guest participants joining a call using Microsoft Internet Explorer.	Fixed in 2.1.3 by increasing the guest timeout duration.
-	CLIENT-5541	WebRTC app could not proxy through Expressway	Fixed in 2.1.3. Participants using the WebRTC app can now login or join calls via the web proxy in Cisco Expressway.
12037	SERVER-5138	No indication that a user was the active speaker on the participant list for a Lync client	Fixed in 2.1.3.
11642	SERVER-4967	Occasionally, Rendezvous calls failed due to Midcall Invites not being answered by the Meeting Server	Fixed in 2.1.3.
11588	SERVER-4935	The Meeting Server only supported DTLS 1.0, this caused cipher compatibility issues for FIPS enabled servers	Guest participants were unable to join conferences on FIPS enabled servers. Fixed in 2.1.3, by enabling DTLS 1.2 to be negotiated if supported by the browser being used by the guest.
11150	SERVER-4686	Occasionally, under a sustained heavy load, a VM Meeting Server will crash	Fixed in 2.1.3.

Resolved in Meeting Server 2.1.2

Reference		Issue	Summary
-	SERVER-5533	In some situations when placing SIP calls through a Cisco Expressway, an incorrect SIP message from the Meeting Server could cause unnecessary retransmission of many messages, which fills the log rapidly with messages.	Fixed in 2.1.2.

Reference		Issue	Summary
-	SERVER-5531	The Meeting Server Syslog was being filled with " unmatched video RTCP feedback received"	The " unmatched video RTCP feedback received" message was filling the log, impacting the server operation and making troubleshooting difficult. This volume of these messages has been reduced in 2.1.2.
10611	SERVER-4411	One Recorder can only handle up to 5 simultaneous recordings	The maximum of 5 simultaneous recordings only applies to Acano X-Series servers. From 2.1.2, other Meeting Servers for example the Cisco Meeting Server 1000 and VM deployments, can handle up to 32 simultaneous recordings per Recorder.
-	SERVER-4161	Sometimes, SIP calls to a Meeting Server using UDP as a signaling transport mechanism would not connect properly	During call setup, the Meeting Server could sometimes erroneously send two different 200 OK SIP messages, preventing the call from connecting properly. Fixed in 2.1.2.
-	CLIENT-5530	Cannot join a call via the Web RTC app using Firefox	Fixed in 2.1.2, by replacing Web Bridge 2.0 with Web Bridge 1.9.
-	CLIENT-5525	Unable to change passcode on spaces created using Web Admin interface	Fixed in 2.1.2, by replacing Web Bridge 2.0 with Web Bridge 1.9.
-	CLIENT-5351	Launching the Web RTC app in guest mode is not possible using Web Bridge 2.0	Fixed in 2.1.2, by replacing Web Bridge 2.0 with Web Bridge 1.9.
-	CLIENT-5333	Using the Web RTC app to join a space with no passcode is not possible using Web Bridge 2.0	Fixed in 2.1.2, by replacing Web Bridge 2.0 with Web Bridge 1.9.

Resolved in Meeting Server 2.1.1

Reference		Issue	Summary
-	SERVER-5720	Meeting Server ignores licenses with any invalid fields.	Fixed in 2.1.1 by relaxing restrictions on licenses with invalid fields.

Reference		Issue	Summary
-	SERVER-5711	Active calls on Meeting Server not shown on **Status**>**Calls** page of Web Admin	Fixed in 2.1.1 by increasing page buffer size.
-	SERVER-5524	Meeting Server unable to receive (encrypted) RFC2833 DTMF packets from certain Lync deployments	Fixed in 2.1.1, now supports encrypted DTMF input from Lync deployments that previously it was unable to receive from.
11997	SERVER-5126	Echo is heard in Lync meeting when a SIP endpoint joins meeting	This happens on Lync clients who joined via the IVR. Fixed in 2.1.1
-	SERVER-5082	Calls from some TIP endpoints drop and the BYE from those endpoints result in the error “481 call leg doesn’t exit”	Fixed in 2.1.1
11785	SERVER-5045	Meeting Server unable to receive (encrypted) RFC2833 DTMF packets from Cisco Spark	Fixed in 2.1.1, now supports encrypted DTMF input from Cisco Spark.

Resolved in Meeting Server 2.1.0

Reference		Issue	Summary
-	SERVER-5928	In some cases, the Meeting Server sends too high a video resolution in calls to devices offering low bit rates.	The Meeting Server can fail to take account of the bit rate offered by a device when deciding the resolution to send it, for instance it can send 720p at a low frame rate when the device offers a low bit rate. Fixed in 2.1.0. The Meeting Server should now prefer a higher frame rate and lower resolution.
12005	SERVER-5131	Under heavy load, occasionally dynamic spaces are not created.	Under heavy, sustained ad-hoc conference load, occasionally dynamic spaces are not handled properly, leading to a failure of the ad-hoc conference escalation. Fixed in 2.1.0.

Reference		Issue	Summary
11943	CLIENT-5322	In some situations the login page for the Web Bridge may fail to load in your browser.	If the web browser attempts to supply a cookie of 512 bytes or more to the Web Bridge, the login page will fail to load. A web browser may supply cookies belonging to other websites in the same domain as the Web Bridge. Clearing your cookies will resolve this issue. Fixed in 2.1.0.
11602	SERVER-4946	The Call Bridge can crash in some rare circumstances when the connection to the XMPP server is lost.	Fixed in 2.1.0.
11312	SERVER-4766	Three Screen TIP Endpoints lose Content after a Hold and Resume.	If a 3-screen endpoint is receiving content, in a CMS conference, and then goes on Hold and then resumes, the presentation is lost. Fixed in 2.1.0.

5 Known Limitations

The following are known issues in this release. If you require more details on any of these please contact Support, https://www.cisco.com/support.

Reference		Issue	Summary
CSCve08594	SERVER-5825	H.323 Gateway component stops accepting new calls	In some circumstances, the H.323 Gateway component can stop accepting new calls. Restarting the H.323 Gateway component will temporarily resolve this problem.
-	SERVER-5519	Load balancing only applies to incoming calls	Limit parameters on API node /system/configuration/cluster only apply to incoming calls
-	SERVER-5142	Heavy conference load can cause VM to crash	Meeting Server on VM can crash if under very heavy, sustained load involving small ad-hoc and small Rendezvous conferences.
CSCvg36523	SERVER-4784	syslog may not work for some components	Enabling syslog for a Recorder, Streamer or Web Bridge will not work (syslogs will not be written to the remote location) until the component in question has been restarted.
-	SERVER-4411	One Recorder can only handle up to 5 simultaneous recordings.	We recommend that each Recorder is used for a maximum of 5 simultaneous recordings.
-	SERVER-3670	Endpoint presence incorrect when already in a Lync meeting	When an endpoint is dragged and dropped into a Lync meeting its presence is not correctly updated as busy.
-	SERVER-3365	No conference control possible by Acano Client of Lync Clients, although controls appear	When adding a space into a Lync conference with multiple Lync users, an Acano app user can select a Lync users name and conference control options appear (mute audio/video, remove) but these options don't do anything.

Reference		Issue	Summary
-	SERVER-3238	Syscall errors in logs	If a WAN optimizer is deployed between clustered database nodes, it may prevent keep-alive checks from completing, causing SYSCALL errors to appear in logs. In cases where a WAN optimizer is being used between cluster nodes, it is important to ensure that all keep alive traffic is sent in a timely manner. Consult your WAN optimizer documentation on how to either disable this functionality between specific IP addresses, or for options that control which optimizations are applied.

Cisco Legal Information

Cisco Trademark