Cisco Meeting Server

Cisco Meeting Server Release 2.9.1

Release Notes

April 30, 2020

Cisco Systems, Inc. www.cisco.com

Contents

What's changed

Version	Change
April 30, 2020	Resolved issues updated.
April 29, 2020	First maintenance release (2.9.1). Hashes updated. See resolved issues.
April 08, 2020	First release of version 2.9

1 Introduction

These release notes describe the new features, improvements and changes in release 2.9 of the Cisco Meeting Server software.

The Cisco Meeting Server software can be hosted on:

- Cisco Meeting Server 2000, a UCS 5108 chassis with 8 B200 blades and the Meeting Server software pre-installed as the sole application.
- Cisco Meeting Server 1000, a Cisco UCS server preconfigured with VMware and the Cisco Meeting Server installed as a VM deployment.
- Acano X-Series hardware.
- or on a specification-based VM server.

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

Note about Microsoft RTVideo: support for Microsoft RTVideo and consequently Lync 2010 on Windows and Lync 2011 on Mac OS, will be removed in a future version of the Meeting Server software. However, support for Skype for Business and Office 365 will continue.

1.1 Interoperability with other Cisco products

Interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco conferencing products.

1.2 Cisco Meeting Server platform maintenance

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

1.2.1 Cisco Meeting Server 1000 and other virtualized platforms

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

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

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.

1.2.3 Call capacities

Table 1 provides a comparison of the call capacities across the platforms hosting Cisco Meeting Server software version 2.8.

Table 1: Call capacities

Type of calls	Cisco Meeting Server 2000	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5
Full HD calls (1080p30)	350	48	48
HD calls (720p30)	700	96	96
SD calls (448p30)	1000	192	192
Audio calls	3000	1700	2200

Table 2 below compares the call capacities for a single or cluster of Meeting Servers compared to load balancing calls within a Call Bridge Group.

Table 2: Meeting Server call capacity for software version 2.8 and later

Cisco Meeting Server platform		Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 2000
Individual Meeting Servers or Meeting Servers in a cluster (notes 1,2 3 and 4)	1080p30 720p30 SD Audio calls	48 96 192 1700	48 96 192 2200	350 700 1000 3000
	HD participants per conference per server	96	96	450
	WebRTC connections per Web Bridge	100	100	100
Meeting Servers in a Call Bridge Group	Call type supported	Inbound SIP Outbound SIP Cisco Meeting App		
	1080p30 720p30 SD Audio calls Load limit	48 96 192 1700 96,000	48 96 192 2200 96,000	350 700 1000 3000 700,000
	Number of HD participants per conference per server	96	96	450
	WebRTC connections per Web Bridge	100	100	100

Note 1: Maximum of 24 Call Bridge nodes per cluster; cluster designs of 8 or more nodes need to be approved by Cisco, contact Cisco Support for more information.

Note 2: Clustered Cisco Meeting Server 2000's without Call Bridge Groups configured, support integer multiples of maximum calls, for example integer multiples of 700 HD calls.

Note 3: Up to 16,800 HD concurrent calls per cluster (24 nodes x 700 HD calls).

Note 4: A maximum of 2600 participants per conference per cluster depending on the Meeting Servers platforms within the cluster.

Note 5: Table 2 assumes call rates up to 2.5 Mbps-720p5 content for video calls and G.711 for audio calls. Other codecs and higher content resolution/framerate will reduce capacity. When meetings span multiple call bridges, distribution links are automatically created and also count against a server's call count and capacity. Load limit numbers are for H.264 only.

Note 6: VMware have made changes in their recent versions (6.0 update 3, 6.5 update 2 and 6.7) that has reduced the throughput of audio calls on Cisco Meeting Server version 2.8 and later (video capacity is unaffected).

1.3 Cisco Meeting App WebRTC and wep app Important information

For information on when features are released and issues resolved for the apps, refer to the appropriate Important Information guides as follows:

- If you are using Cisco Meeting Server WebRTC app (i.e. you have deployed Web Bridge 2), see Cisco Meeting App WebRTC Important information guide.
- If you are using Cisco Meeting Server web app (i.e. you have deployed Web Bridge 3), see Cisco Meeting Server web app Important Information guide.

All information relevant to the apps is contained in a separate document for each app, and is not included in the Meeting Server release notes.

The Important Information guides describe the following:

- Any new or changed feature in the app, and details of fixed issues and open issues associated with the app with an indication of the version of Meeting Server where this feature/fix is available.
- Any upcoming changes in browsers affecting the app, and the affected versions of the app with recommended workarounds.

WebRTC is an evolving technology and frequent changes are implemented by browser vendors. The Important Information guides will be updated when we need to inform you of upcoming changes.

1.4 End of Software Maintenance

On release of Cisco Meeting Server software version 2.9, Cisco announces the time line for the end of software maintenance for the software in Table 3.

Table 3: Time line for End of Software Maintenance for versions of Cisco Meeting Server

Cisco Meeting Server software version	End of Software Maintenance notice period
Cisco Meeting Server version 2.7.x	4 months after the first release of Cisco Meeting Server version 2.9.

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

2 New Features/Changes in version 2.9

Version 2.9 of the Meeting Server software, adds the following:

- Cisco Meeting Server web app (Web bridge 3.0)* is a new meeting join and user portal. Web app will eventually supersede Cisco Meeting App WebRTC.
- Custom email invites for use with the new Cisco Meeting Server web app.
- an additional lock mode that allows meetings to be locked so all participants are held in a lobby to prevent them joining a meeting until either they are admitted through the API or the meeting is unlocked by any one who has privileges to do so (not necessarily the host). (The existing lock mode allows certain participants to bypass the lock.)
- a method to admit participants from the lobby into a meeting using a new API command.
- support for configuration of a third party SIP recorder – when recording is started a SIP URI is called instead of using the Meeting Server recorder component.
- support for panoramic video layout experience in two participant meetings. This feature supports the new panorama endpoints. In version 2.9, this is beta support.
- support for 4K content* on any endpoint that supports 4K content.
- improved video/content quality for Chromium browsers*.
- increased security with support for stronger ciphers.
- support to allow far end camera control (FECC) on remote systems' cameras to be initiated using the Meeting Server API.
- simplified API user interface available on the Meeting Server web interface.
- Ability to enable Automatic Gain Control (AGC), introduced in 2.8 as a beta feature is now fully supported.
- support for creating and applying coSpace templates using the API.

Note: Features marked with an asterisk (*) are **not** supported on Acano X-Series in version 2.9.

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.

CAUTION: The additional lock mode feature introduces a change in default behavior. From version 2.9 `lockMode` set to `all` is the default. If you do not want this change in default behavior after upgrade you will need to change your cluster default. For more information, see Section 2.3

2.1 Cisco Meeting Server web app

In version 2.9, Meeting Server introduces the new Cisco Meeting Server web app which is a browser-based client for Cisco Meeting Server that lets users join meetings (audio and video). To use this feature you need to deploy the new Web Bridge 3. In addition, Meeting Server version 2.9 still offers the original Cisco Meeting App WebRTC (also referred to here as Web Bridge 2).

In this release Cisco Meeting Server web app is fully supported for internal calls, but not recommended for external calls (see Section 2.1.2), and it is not yet fully featured. It is intended that in due course it will support virtually the same feature set and supersede Cisco Meeting App WebRTC.

Note: For a full list of features that are not currently supported by web app in 2.9 and those features that we plan to support in the future, see Cisco Meeting Server web app Important Information for more details.

Note: Chat has been deprecated in web app – it is not intended to be supported in the future.

Note: The Web Bridge 3 component that supports web app cannot be run on the Acano X-series. However, the Acano X-Series can still run the Call Bridge and be part of the same cluster. Web Bridge 3 will need to be run on Cisco Meeting Server 1000 and 2000 platforms and other specification-based VM.

Note: Web app does not require XMPP. The XMPP component will be removed from a future version. Cisco Meeting App WebRTC still requires XMPP.

2.1.1 Useful information to help configure Web Bridge 3

The following is useful information to help you configure Web Bridge 3 so that you can use web app:

- "Call Bridge to Web Bridge" protocol (C2W) is the link between the callbridge and webbridge3.
- A port must be opened on an interface (using **`webbridge3 c2w listen`**) to allow the callbridge to connect to the webbridge3 (the webbridge listens on that port). This is why you have to give the address with this port when you do the API request to tell a callbridge about this webbridge. This connection must be secured with certificates.

- We recommend you protect that opened port from external access – it only needs to be reachable from callbridges.
- The callbridge uses the certificate set using **`callbridge certs`** and the webbridge uses the certificate set using **`webbridge3 c2w certs`**.
- The webbridge will trust certificates of callbridges that have been signed by one of those in its trust store, set by **`webbridge3 c2w trust`**.
- The callbridge will trust webbridges that have certificates signed by one of those in its trust store, set by **`callbridge trust c2w`**.
- The webbridge3 https certifcates and ports are the same as for webbridge2, it allows you to reach the web client using https and can be used in the same deployment at the same time.
- If the webbridge3 c2w certificate requires extended key usage, it should be "server authentication", and the callbridge certificate extended key usage should be "client authentication". However, these extensions are optional and if the certificate doesn't have them, the Web Bridge 3 will assume any usage is possible.
- You do not need a certificate signed by a public authority – you can use self-signed certificates created within the MMP.
- The SAN/CN must match the FQDN or IP address that is used in the c2w:// url used to register the Web Bridge 3 in the callbridge API. (If this does not match, the callbridge will fail the TLS negotiation, rejecting the certificate presented by the webbridge, and will fail to connect with the webbridge.)
- For general certificate information, see the Certificate Guidelines appropriate for your deployment.

The figures below show the flow of a typical Web Bridge 2 setup compared to that for Web Bridge 3.

Figure 1: Web Bridge 2 setup flow diagram

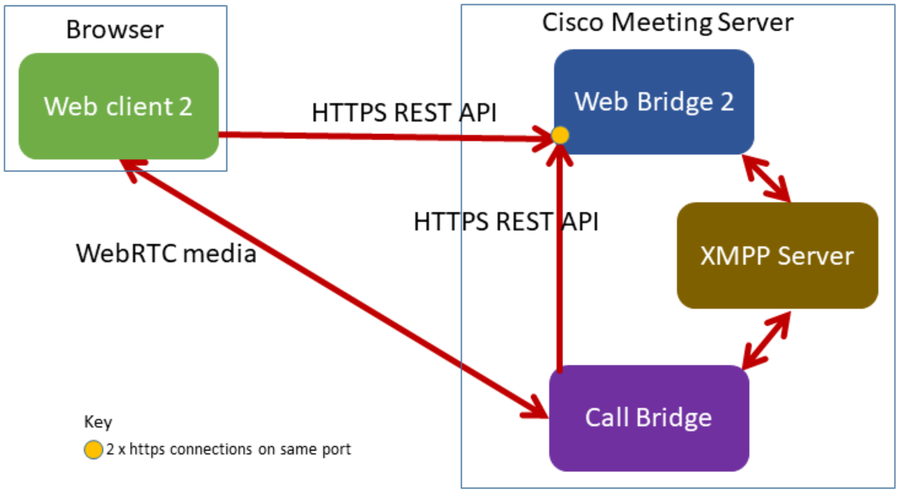
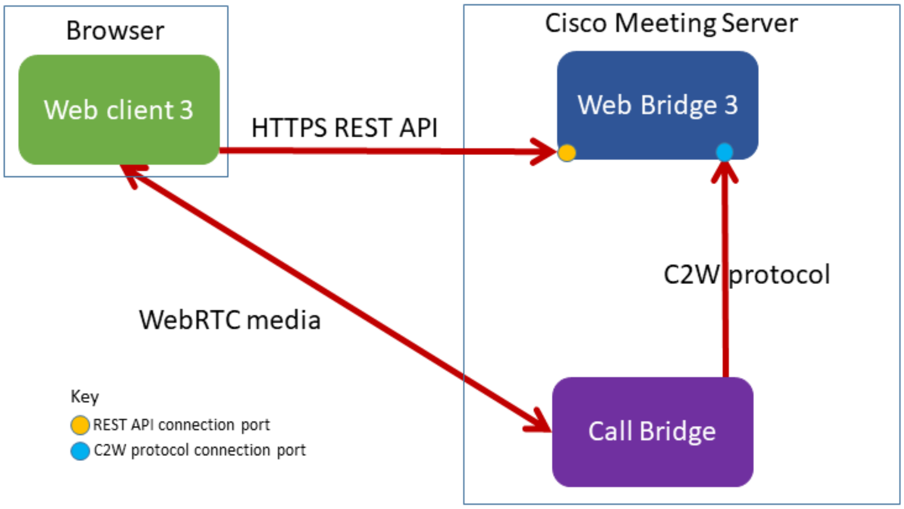


Figure 2: Web Bridge 3 setup flow diagram



2.1.2 Important notes for Expressway users

The web app can be deployed without any restrictions for internal calls or without going through Expressway, which means all calls within your corporate network or external calls to your network if done via the corporate VPN.

Web app calls via Expressway (or using its TURN server) is being released as a preview feature at the present time, pending scalability testing. Deploying the web app with an expressway in a production environment is not supported at this time, these release notes will be updated as soon as testing is completed.

To deploy the web app using an Expressway, the OAuth setting must be disabled in the Expressway configuration (this is enabled by default) – however, disabling OAuth impacts other clients such as Jabber in your deployment. Follow these steps based on your deployment:

Note: This is a temporary workaround and expected to be resolved in a future release of Expressway.

If you have Jabber deployed:

You will need to deploy an additional Expressway pair (with OAuth disabled) for the web app to work. Refer to Expressway documentation for instructions to deploy an Expressway pair. See steps below to disable the OAuth setting.

If you don't have Jabber deployed:

You need to disable OAuth in the MRA configuration as follows to use web app:

1. On the Expressway-C, go to **Configuration > Unified Communications > Configuration**.
2. Under **MRA Access Control**, set **Authorize by OAuth token with refresh** to **Off**.

Note: If you have a WebRTC deployment and you want to deploy the new web app in parallel, you'll also need a new Expressway pair to deploy the web app. Refer to Expressway documentation for more information.

2.1.3 Configuring Meeting Server to use Web Bridge 3

If upgrading your Meeting Server to 2.9, by default, this release will use your existing Web Bridge 2 configuration. However, you can configure Web Bridge 3 to operate at the same time as Web Bridge 2. Web Bridge 2 uses XMPP and Web Bridge 3 uses Call Bridge to Web Bridge (C2W) protocol connections so they can work in parallel, however, they will need to be configured to use different ports as shown in Figure 2.

Note: You don't need to configure an XMPP Server for Web Bridge 3.

Web Bridge 3 is similar to Web Bridge 2 for configuration and setup which is done using MMP commands via SSH. The main difference is that Web Bridge 2 requires configuring an HTTPs port, whereas Web Bridge 3 requires configuring an HTTPS port and a C2W port.

To configure Meeting Server to use Web Bridge3:

1. SSH into the MMP and log in.
2. Use the **webbridge3** command in the MMP to configure webbridge3. To display the webbridge 3 usage, enter: **help webbridge3**

```
> help webbridge3

     Usage:
     webbridge3
     webbridge3 restart
     webbridge3 enable
     webbridge3 disable
     webbridge3 https listen <interface:port whitelist>
     webbridge3 https certs  <key-file> <crt-fullchain-file>
     webbridge3 https certs none
     webbridge3 http-redirect (enable [port]|disable)
     webbridge3 c2w listen <interface:port whitelist>
     webbridge3 c2w certs  <key-file> <crt-fullchain-file>
     webbridge3 c2w certs none
     webbridge3 c2w trust <crt-bundle>
     webbridge3 c2w trust none
     webbridge3 options <space-separated options>
     webbridge3 options none
     webbridge3 status
```

   More detail can be found in the 2.9 MMP additions summary here.

3. (Optional) Set up a port for HTTP connections. This port will be opened for all Meeting Server interfaces on which the web app has been configured. Incoming HTTP connections will be automatically redirected to the matching HTTPS port for the interface they arrived on. The default port, if you don't specify one in **webbridge3 http-redirect enable [port]**, is 80.
4. Configure the port for the HTTPS service to listen to. To configure it to listen on port 443 of the a interface:

   ```
   webbridge3 https listen a:443
   ```

5. Set the HTTPS certificates. These are the certificates that will be presented to web browsers so they need to be signed by a certification authority and the hostname/purpose etc needs to match. (The certificate file is the full chain of certificates that starts with the end entity certificate and finishes with the root certificate.) Enter the command:

   ```
   webbridge3 https certs wb3-https.key wb3-https-fullchain.crt
   ```

6. Configure the C2W connection. We recommend that you make this address/port accessible from the Call Bridge(s) only. The following command sets it in port 9999 of

interface a:

```
webbridge3 c2w listen a:9999
```

Note that here we use the example of port 9999, however, it can be any available port on your network. It's not a fixed port, unlike 443.

7. Configure the C2W connection certificates. You need to configure the SSL Server certificates used for the C2W connection. (See "Configuring Call bridge to use C2W connections" below for certificate requirements, and more information can be found in this FAQ.)

   ```
   webbridge3 c2w certs wb3-c2w.key wb3-c2w-fullchain.crt
   ```

8. The Web Bridge 3 C2W server is expecting Call Bridges to present a client certificate – it will verify whether to trust them using the trust bundle provided by the following command:

   ```
   webbridge3 c2w trust wb3-c2w-trust-bundle.crt
   ```

9. Now enable Web Bridge 3:

   ```
   webbridge3 enable
   ```

2.1.4 Configuring Call bridge to use C2W connections

C2W certificates are used for the connection between Call Bridge and Web Bridge 3. For the Call Bridge to make a C2W connection to a Web Bridge 3, you need to specify a C2W trust store to verify certificates against, i.e. the ones presented by the Web Bridge 3 that were configured in step 7 above.

1. Use the **callbridge** command in the MMP to display the Call Bridge usage, enter: **help callbridge** to display:

   ```
   > help callbridge
   Configure CMS callbridge

   Usage:

       callbridge listen <interface whitelist>
       callbridge prefer <interface>
       callbridge certs <key-file> <crt-file> [<cert-bundle>]
       callbridge certs none
       callbridge trust xmpp <bundle>
       callbridge trust xmpp none
       callbridge trust c2w <bundle>
       callbridge trust c2w none
       callbridge add edge <ip address>:<port>
       callbridge del edge
       callbridge trust edge <trusted edge certificate bundle>
   ```

```
callbridge trust cluster none
callbridge trust cluster <trusted cluster certificate bundle>
callbridge restart
```

2. Set the certificates for the Call Bridge:

   ```
   callbridge certs cert.key cert.crt
   ```

3. Set the C2W trust store that will be used to validate the SSL Server certificate presented by the Web Bridge 3. (For more information, see this FAQ.)

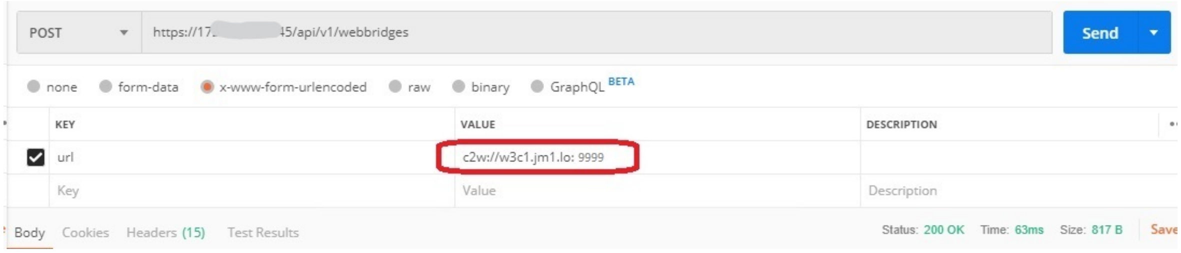
   ```
   callbridge trust c2w c2w-callbrige-trust-store.crt
   ```

4. Now restart Call Bridge:

   ```
   callbridge restart
   ```

5. Register the Web Bridge 3 URL to the running callbridge REST API in the same way as you would for Web Bridge 2, as shown below, i.e. POST to /api/v1/webbridges with the "url" parameter. The URL protocol indicates if it is webbridge2 or webbridge3. So, if the protocol is http:// or https:// then the webbridge is treated as webbridge2, and if you specify c2w:// protocol in the URL then it will be handled as a webbridge3 connection.

Figure 3: Registering Web Bridge 3 URL to the Call Bridge API



POST ▾ https://17[redacted]45/api/v1/webbridges

Send
○ none ○ form-data ● x-www-form-urlencoded ○ raw ○ binary ○ GraphQL BETA

	KEY	VALUE	DESCRIPTION
☑	url	c2w://w3c1.jm1.lo: 9999	
	Key	Value	Description

Body Cookies Headers (15) Test Results

Status: 200 OK Time: 63ms Size: 817 B

2.1.5 API methods presented by Web Bridge 3

Version 2.9 introduces new API methods to retrieve information specifically for the Web Bridge 3. These new API methods are not found on the usual Meeting Server API; they are supported on the API presented by Web Bridge 3. This API is used by the web app that runs in the browser to communicate with the Web Bridge 3. These methods are intended for use by administrators for diagnostic purposes.

For example, if Web Bridge 3 is running on: `join.meeting.space`, these API methods are on `https://join.meeting.space/api/bridge/info`

The new methods are:

- GET on `/api/bridge/info` returns an identifier for this Web Bridge 3.
- GET on `/api/v1/load` returns an identifier for this Web Bridge 3 (for legacy use).
- GET on `/api/bridge/callbridges` returns information on the current Call Bridge connections to this Web Bridge 3.

- GET on **`/api/bridge/connections`** returns information on current HTTP connections being served by this Web Bridge 3.*
- GET on **`/api/bridge/websockets`** returns information on current websockets being served by this Web Bridge 3.*
- GET on **`/api/configuration`** returns the languages available for custom email invites and other non-confidential configuration information.

* requires authentication (the same authentication that a web app user would use to log in).

2.2 Cisco Meeting Server web app custom email invites

In version 2.9, Meeting Server introduces custom email invites for use with the new Cisco Meeting Server web app.

This allows an administrator to create and upload different email invitation templates so that web app users can:

- send an email invite – in a language of their choice – to other people to join a future meeting.
- send email invites appropriate to different audiences, for example external and internal participants.

Note: We recommend using locally hosted branding for web app Custom Email invites. However, if you wish to use multiple languages on a more complex deployment (e.g. a multi-tenant deployment) then you will need to use a remote branding web server. For more information see the Customization Guidelines.

2.2.1 Default invitation templates

2.2.1.1 Invitation templates for different languages

There are two default language invitation email templates for web app on the Meeting Server, these are:

- invitation_template_es_ES.txt (Spanish – Spain)
- invitation_template_en_US.txt (English – US)

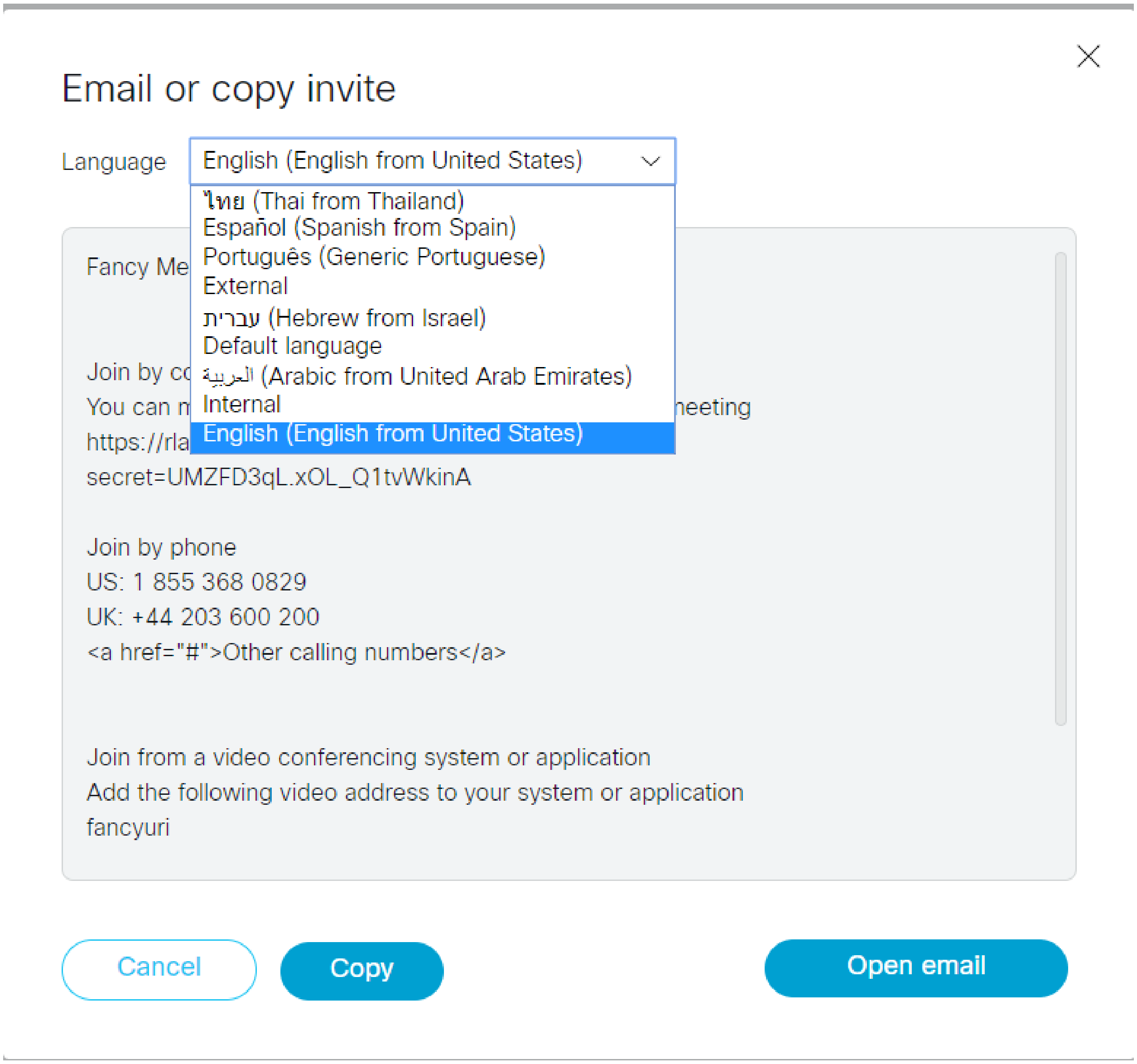
If you want to overwrite the default templates, you can create your own language tagged template file and upload to locally hosted branding. The Meeting Server interprets these language tags to return the appropriate template option in the web app.

A user can only select a language template that is uploaded – a language option is not shown in the drop-down list if it is not uploaded.

Note: You must upload the template files to all Meeting Servers in a cluster.

The figure below shows an example of some of the different email invites that have been created and uploaded on this particular Meeting Server:

Figure 4: Email invite options



Email or copy invite

Language English (English from United States)

ไทย (Thai from Thailand)
Español (Spanish from Spain)
Português (Generic Portuguese)
External
עברית (Hebrew from Israel)
Default language
العربية (Arabic from United Arab Emirates)
Internal
English (English from United States)

Fancy Me

Join by co
You can m neeting
https://rla
secret=UMZFD3qL.xOL_Q1tvWkinA

Join by phone
US: 1 855 368 0829
UK: +44 203 600 200
<a href="#">Other calling numbers</a>

Join from a video conferencing system or application
Add the following video address to your system or application
fancyuri

2.2.1.2 *Invitation templates for different audiences*

A user can generate different email invites appropriate for different audiences, for example, external and internal participants. To do this, you need to create an invitation template file with the following naming convention example: invitation_template_Internal.txt. This file will display in the email invite options as "Internal" as shown in Figure 4.

For more information on using the email invite option, see Cisco Meeting Server web app Important Information.

2.2.2 Creating the different language variant invitation template file

Create an invitation_template_xx_XX.txt file in UTF-8 using the information in Section 2.2.2.1.

2.2.2.1 Permitted conditional statements and placeholders

The template can contain both conditional statements and placeholders. This allows a single template to be used for multiple spaces and gives a consistent feel to the invitations.

The placeholders that are currently defined (each starts and ends with a % character) are listed in the table below:

Table 4: Placeholders in invitation template

Placeholder	Type
%name%	Conference name
%uri%	Dial-in URI of the conference
%numeric_id%	Numeric ID of the conference
%hyperlink%	Direct hyperlink to the conference on the web bridge
%passcode%	Numeric PIN for the conference
%%	Always replaced with % **Note:** that any % within the text will be interpreted as the start of a placeholder. To insert a single '%' in the text use the placeholder %%
%launch_link%	Direct hyperlink to launch the conference in desktop or iOS Cisco Meeting App. **Note:** If you are using Microsoft Outlook, add a "url:" prefix to the link so it can be recognised as hyperlink in Microsoft Outlook/email clients.

The following conditional statements are supported, see table below. They can be nested if required.

Table 5: Conditional statements in invitation template

Conditional statement	Meaning
#if condition	If the condition is true then include the lines until an else or endif statement. The condition section of this if statement takes the form of one of the placeholders. For example. “#if name”
#else	If the condition in the previous if statement was false then include the lines until an endif statement
#endif	

2.2.2.2 Example invitation template

Note:

- There is a 10000 byte limit* on the size of the invitation template .txt file.
- All invitation templates must be provided in UTF-8 format.
- Extended ASCII characters are not supported.
- UTF-8 format invitation template .txt files need to have Unix line endings, i.e. LF, not CRLF (as Windows uses). Omitting Unix line endings will result in the file not working.
- Language .txt files should have the appropriate language tags for its language variant (as defined by the IANA Language Subtag Registry) – where the two lower case characters indicate the language code and the two upper case characters the region code. For example, invitation_template_en_GB.txt, where "en" is the english language, and "GB" is the region (United Kingdom).
- The part of the file name between "invitation_template" and the .txt suffix can use alphanumerics and "_" (underscores) of up to 32 characters, i.e. any of the following regular expression: ^[a-zA-Z_]{1,32}$.

Note: *At the time of publication whilst using web app from Google Chrome on Windows, the **Open email** option fails if the file size of the invitation template exceeds 1491 bytes. This is a known issue with Google Chrome browsers, more information about this issue is available here: https://bugs.chromium.org/p/chromium/issues/detail?id=1034497

If this occurs, **Open email** will be greyed out, however, you can select **Copy** which will allow you to paste the meeting join information into your preferred email client.

Use the example below and customize with your specific values in the placeholders. Save it using the **invitation_template_xx_XX.txt** file name format for a language variant.

```
#if name
You're invited to %name%
#else
You're invited to my Cisco space
#endif


#if hyperlink
   Click to join: %hyperlink%
#else
#if numeric_id
   Click to join: https://join.example.com
   Call ID: %numeric_id%
#endif
#endif

#if hyperlink
Click to launch using web app: %launch_link%
#else
Launch link not available
#endif

#if uri
     Or call in:
     - Video system, Jabber or Lync: %uri%

#endif

#if numeric_id
       Phone Access: Call the regional access number, then enter %numeric_id%
       US Toll Free: (800)-555-1234
       UK Toll Free: 0800-800-8000
#endif


#if passcode
   Passcode: %passcode%
#endif
```

Note: `%launch_link%` placeholder should be included in the `#if_hyperlink` condition so it is included in the template if hyperlinks are enabled, and excluded if hyperlinks are disabled.

For information on uploading invitation template .txt files for locally hosted branding or remote web server hosted branding, see the Customization Guidelines.

Note: We recommend using locally hosted branding for web app Custom Email invites. However, if you wish to use multiple languages on a more complex deployment (e.g. a multi-tenant deployment) then you will need to use a remote branding web server. For more information see the Customization Guidelines.

2.3 Additional lock mode for meetings

From 2.9 the Meeting Server introduces an additional lock mode feature to lock a meeting.

CAUTION: This additional lock mode feature introduces a change in default behavior. From version 2.9 `lockMode` set to `all` is the default. If you do not want this change in default behavior after upgrade you will need to change your cluster default by setting your callProfile in `/system/profiles` to have `lockMode` set to `needsActivation`. Existing and new behavior is explained further below.

Existing functionality to "lock" a meeting behaves more as a "lock guest" feature and doesn't in effect lock the meeting itself as it allows certain members to bypass the lock. It uses the `needsActivation` parameter on the `callLeg` object – for guests this is set to `true` and for hosts this is set to `false`. Typically two different `accessMethods` with different `callLegProfiles` are used to configure this. Guests join using one `accessMethod` and hosts join using a different `accessMethod`.

The existing behavior when a meeting is "locked" means that hosts can still join the meeting but guests remain in the lobby even if a host has already joined. When the meeting is "unlocked", guests join the meeting or stay in the lobby depending upon whether a host is present in the meeting.

The new 2.9 functionality allows you to lock the meeting so all participants can be held in a lobby. It introduces the API parameter `lockMode` on callProfile objects with the possible values `all`, `needsActivation` or `<unset>`. This parameter supports the following operations:

- POST to `/callProfiles`
- PUT on `/callProfiles/<callProfile id>`
- GET on `/callProfiles/<callProfile id>`

When `lockMode` is set to `needsActivation` it provides the existing pre-version 2.9 behavior so only guests are locked.

When the meeting is locked with `lockMode` set to `all` no new participants can join the meeting, instead they will join the lobby, regardless of whether they are a guest, host, cospace member and so on. From version 2.9 `lockMode` set to `all` is the default.

When the meeting gets unlocked any participants in the lobby and any new participants trying to join the meeting are admitted into the meeting depending upon the activation configuration. The behavior is the same as an unlocked meeting with `lockMode` set to `needsActivation`. Hosts can join the meeting but guests can only join if a host is already present. The existing behavior rules about how guests are activated apply. The existing rules for behavior when the last host leaves the call are also respected (i.e. dependent upon the **deactivationMode** setting).

Note: Lock mode behavior (for both **all** and **needsActivation**) is disabled when the call type is 'forwarded' or 'lync conferencing'.

2.3.1 Default settings

The default for **/callLegs** is **needsActivation** set to **false**, i.e. everyone is a host. So unless that default is changed, **lockMode** set to **all** means everyone is locked out upon locking the meeting and everyone is admitted upon unlocking the meeting.

Similarly, when **needsActivation** is **<unset>** in **/callLegs** and the relevant **/callLegProfiles**, the behavior defaults to **needsActivation=false**, i.e. by default you are a host. (**<unset>** means behavior is inherited based upon the hierarchy of **/callLegProfiles**.)

When **lockMode** is set to **needsActivation** the meeting doesn't lock anyone out when all participants have **needsActivation** set to **false**.

The new **lockMode** set to **all** is appropriate for use for basic coSpace where you haven't configured different **accessMethods**.

2.3.2 Locking and unlocking the meeting

There are no changes in functionality. You can lock and unlock the meeting as before using DTMF, Active Control (Cisco Jabber only), or the API with the **locked** parameter set to a value of **true** or **false** applied to **/calls** or **/callProfiles**. For more information, see the Cisco Meeting Server API Guide.

2.3.3 Signaling when a call is locked / unlocked

The existing APIs and Active Control events already signal when a call is locked / unlocked. This will continue to work in both **lockMode** settings.

2.3.4 How to see who is in the lobby and who is in the meeting

Check the **status** section of the individual **/callLeg/<call leg id>** API node to see if the **deactivated** parameter shows. If a callLeg is not deactivated it does not show in the **status** section and indicates that the participant is in the meeting. The **deactivated** parameter will only show when set to **true** which indicates that the participant is in the lobby. This is existing behavior.

If the **deactivated** parameter is not shown in the **status** section, then the associated participant is in the meeting and if it is set to **true** it will be shown, the participant is in the lobby This is existing behavior.

2.3.5 Audio prompt behavior

A new audio prompt: "This meeting is locked, you are waiting to be allowed in" is implemented to support the new lock mode behavior. The file name for this new audio prompt is "locked_you_are_waiting.wav".

This new audio prompt is customizable as are the existing prompts. See Customization Guidelines for more information.

The prompts a deactivated participant may hear are as follows:

1. "Welcome to a Cisco Meeting"
2. "Waiting for host to join" / "This meeting is now locked, you are waiting to be allowed in"

Once the participant is activated they will hear "You are entering the meeting now" and they will then enter the meeting.

With regard to the two possible prompts in step 2, either prompt could play when a participant is in the deactivated state: the first one plays when a participant is a guest (**`needsActivation=true`**) and the host is not in the meeting, and the second one plays in all other cases where a participant is deactivated.

2.3.6 Changes to recorder/streamer behavior

Recorders/streamers are always able to go straight in to the meeting and bypass the lobby, regardless of whether the meeting is locked or what their **`needsActivation`** in the **`/callLegProfile`** is set to. This behavior is the same for both lock modes.

2.4 Admit participant from the lobby

When a participant joins a meeting they may be held temporarily in a lobby either because the meeting is locked or because they are waiting for the host to join (see "Additional lock mode for meetings " on page 23). From 2.9, Meeting Server introduces a method of admitting participants from the lobby into a meeting using a new API command. This feature lets you admit all participants, or individual participants.

When used on GET operations on **`/callLeg/<call leg id>`** API nodes, the existing **`deactivated`** parameter can take the values of **`true`** or **`false`**. The value **`true`** means the participant(s) are in the lobby; **`false`** means the participant(s) are in the meeting.

To support this new feature, usage of the API parameter **`deactivated`** is now extended to PUT and POST operations as detailed below. This parameter can only take the value of **`false`** for these operations.

To activate an individual participant to allow them into the meeting from the lobby, the **`deactivated`** parameter supports the following operation:

- PUT to **`/participants/<participant id>`**

To activate all participants to allow them into the meeting from the lobby, the **`deactivated`** parameter supports the following operation:

- POST to **`/calls/<call id>/participants/*`**

Depending upon which API operation is called, the individual participant or all participants currently in the lobby are then transitioned into the meeting as active participant(s). New participants joining after this will get a behavior determined by a combination of the lockMode in use, call lock status and needsActivation required status. Any guests (**`needsActivation=true`**) who are admitted into the meeting will subsequently obey the **`deactivationMode`** scenarios when the last activator leaves the call, i.e. they will go back to the lobby, be disconnected or allowed to remain in the call.

You can also create a new participant and put them straight into the meeting, bypassing the lobby, with the API parameter **`deactivated`** (value of **`false`**) using the following operation:

- POST to **`/calls/<call id>/participants`**

Note that if a participant is moved, they will still obey the same combination of settings, i.e. they are not treated differently. So even a moved participant will need to have **`deactivated=false`** to bypass the lobby.

2.5 SIP recorder support

From 2.9, the Meeting Server allows configuration of an external third-party SIP recorder so that when recording is started an administrator-configured SIP URI is called instead of using the Meeting Server internal recorder component.

Note: Support for an external third-party SIP recorder still requires Meeting Server recording licenses.

The new SIP recorder feature:

- allows recorders to negotiate BFCP in order to receive separate video and content streams. This gives more flexible options for how recordings are formatted.
- supports the same resolutions as we do for standard SIP calls
- supports the same audio and video codecs as standard SIP calls
- as with the existing Meeting Server internal recorder, any media content sent by the SIP recorder is discarded.

Note: The SIP recorder feature does not support TIP or Active Control.

2.5.1 Specifying the SIP recorder

A new API parameter for **`/callProfile`** objects is introduced to specify the SIP recorder. It supports GET, PUT and POST and is defined as follows:

- **`sipRecorderUri`** – If set, this URI is used to dial out to when recording is enabled. If unset, the Meeting Server recorder component (if configured in **`/recorders`**) is used.

2.5.2 Starting / stopping the recording

The same start / stop methods supported by the Meeting Server recorder component can be used to initiate a SIP recorder. Which recorder is used depends upon whether you have configured the API parameter **`sipRecorderUri`**. The methods currently supported are:

- With the callProfile **`recordingMode`** set to **`automatic`**, recording starts when users join. Users cannot start / stop the recording.
- When **`recordingMode`** is set to **`manual`**, users can start / stop recording using a dtmfProfile, Active Control, Meeting App or via an API PUT/POST on calls.

2.5.3 Finding out recording status

The same methods supported by the Meeting Server recorder component can be used to find out the SIP recorder status, for example, GET on **`callLegs/<call leg id>`** – the **`recording`** value in the **`status`** output found here indicates whether this callLeg is recording (**`true`**) or not (**`false`**).

2.6 Panoramic video layouts (Beta support)

From 2.9, the Meeting Server introduces support for the panoramic layout experience in two participant meetings. This feature supports the new panorama endpoints:

- Cisco Webex Room Panorama
- Cisco Webex Room 70 Panorama
- Cisco Webex Room 70D Panorama Upgrade

When both participants in the meeting are panorama endpoints the Meeting Server can request two camera streams from them so both participants get a wide panoramic view of the other room.

When other video participants join, Meeting Server will only request one camera stream from the panorama endpoint and it will transition from the panoramic layout to the existing dual screen layouts. If you have two panorama endpoints and an audio-only participant joins the meeting, the panoramic experience still applies.

Panoramic layout is fully supported across a Meeting Server cluster. Panoramic layout supports existing CE in-meeting controls (e.g. roster lists, mute, remove). Other features, such as changing the local layout or pane placement are only supported if the panorama endpoint transitions to the existing dual screen layouts, i.e. when there are more than two video participants.

Dual screen endpoints can receive a panoramic layout when in a meeting with a panoramic endpoint.

To support panoramic video, new response values are introduced to existing response elements as follows:

- GET on **`/callLegs/<callLeg ID>`** – the response element **`status`** has the element **`multistreamVideo`** which can return the following two new values:
  - **`numCameras`** which returns the number of multistream main video camera streams currently active for this call leg.
  - **`numCamerasAvailable`** which returns the number of multistream main video camera streams advertised by the far end as being available for this call leg.

2.6.1 Web interface change

From 2.9, the web interface "dual video" indication is changed to "dual screen" for clarity following the introduction of dual camera support.

2.7 Support for 4K7fps content

Version 2.9 introduces support for 4K7fps content on Cisco endpoints that offer 4K7fps.

Note: Support is for:

- content video only, not main video
- only supported for H.264
- only in SIP calls

Note: This feature is not supported on the Acano X-Series in version 2.9.

2.8 Improved video/content quality for Chromium browsers

Version 2.9 introduces improved video and content quality for Chromium browsers. In 2.9, the default behavior for H.264 for Chromium browsers is changed to allow 1080p main and content streams to be decoded using Chrome's software decoder; this improves the quality and user experience of the meeting.

We believe this offers the best experience for most users and if you previously forced VP8 we suggest you try this new H.264 implementation. In addition, VP8 implementation is improved to also support 1080p.

To achieve this change in default behavior, 2.9 introduces the new parameter `chromeWebRtcH264interopMode` which is set globally in the `compatibilityProfiles`.This new parameter has the following values: `auto` (new default behavior) and `none` (legacy behavior).

Note: This feature is not supported on the Acano X-Series in version 2.9.

2.9 Support for stronger ciphers

For increased security, version 2.9 introduces support for GCM ciphers in SRTP media encryption, in AES-128 and AES-256 variants.

The following ciphers are supported in SIP calls (in order of preference): "AEAD_AES_128_GCM", "AEAD_AES_256_GCM", "AES_CM_128_HMAC_SHA1_80" then "AES_CM_128_HMAC_SHA1_32".

The cipher that is used in calls may be determined by the call control infrastructure (for example, Cisco Unified CM) depending on how the trunks are configured (i.e. they can be configured to force certain ciphers, notably GCM (128 or 256 variants) or to allow only 256 bit GCM).

The new parameter `cipherSuite` has been added to the response to a GET on a `/callLegs/<call leg id>` object. If any of this call leg's media is encrypted, the returned value gives the SRTP encryption cipher suite in use; one of:

- `AEAD_AES_128_GCM` – AES encryption, 128 bit, GCM
- `AEAD_AES_256_GCM` – AES encryption, 256 bit, GCM
- `AES_CM_128_HMAC_SHA1_80` – AES encryption, 128 bit, 80 bit SHA1 authentication tag
- `AES_CM_128_HMAC_SHA1_32` – AES encryption, 128 bit, 32 bit SHA1 authentication tag

2.10 Support to allow Far End Camera Control using the API

The FECC support introduced in version 2.8, allows camera control commands sent by one endpoint in a Meeting Server conference to be passed through to another endpoint – the destination endpoint being the one currently in the controlling system's "main pane" in the layout.

Version 2.9 introduces API support to enable control of the remote systems' cameras using H.281 commands – there's no requirement for the system you want to control to be in your focused layout main pane.

To allow FECC on a remote system's camera the following new API object is introduced:

- PUT to `/callLegs/<call leg id>/cameraControl`

This object supports the new optional request parameters:

- `pan` – one of `left` or `right`. Pans the remote camera left or right.
- `tilt` – one of `up` or `down`. Tilts the remote camera up or down.
- `zoom` – one of `in` or `out`. Zooms the remote camera in or out.
- `focus` – one of `in` or `out`. Focuses the remote camera in or out.

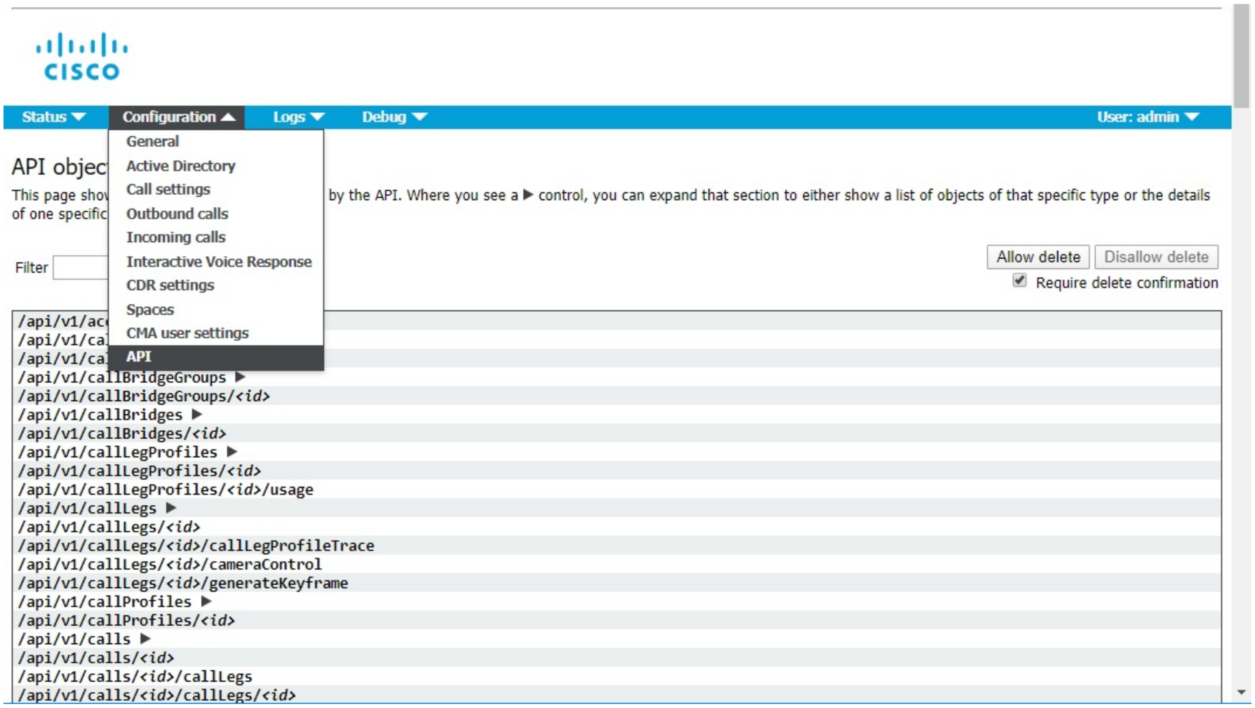
Not every call leg will support receiving H.281 commands for controlling its camera. To ensure you only send to call legs that have advertised FECC support, look at the `cameraControlAvailable` value in the status response for those call legs. Note that it's possible for call legs to change camera control availability during the course of a meeting.

2.11 API access on the web interface

To simplify using the API without the need for third-party applications, version 2.9 introduces a user interface for the API that can be accessed via the **Configuration** tab of the Meeting Server web interface, as shown in Figure 5.

Note: To access the API via the web interface you still need to do the initial Meeting Server configuration settings and authentication using the MMP as you would if you were using a third party application. See the [MMP Command reference guide]() for details.

Figure 5: Accessing the API via the Meeting Server web interface



API objec

This page shov by the API. Where you see a ▶ control, you can expand that section to either show a list of objects of that specific type or the details of one specific

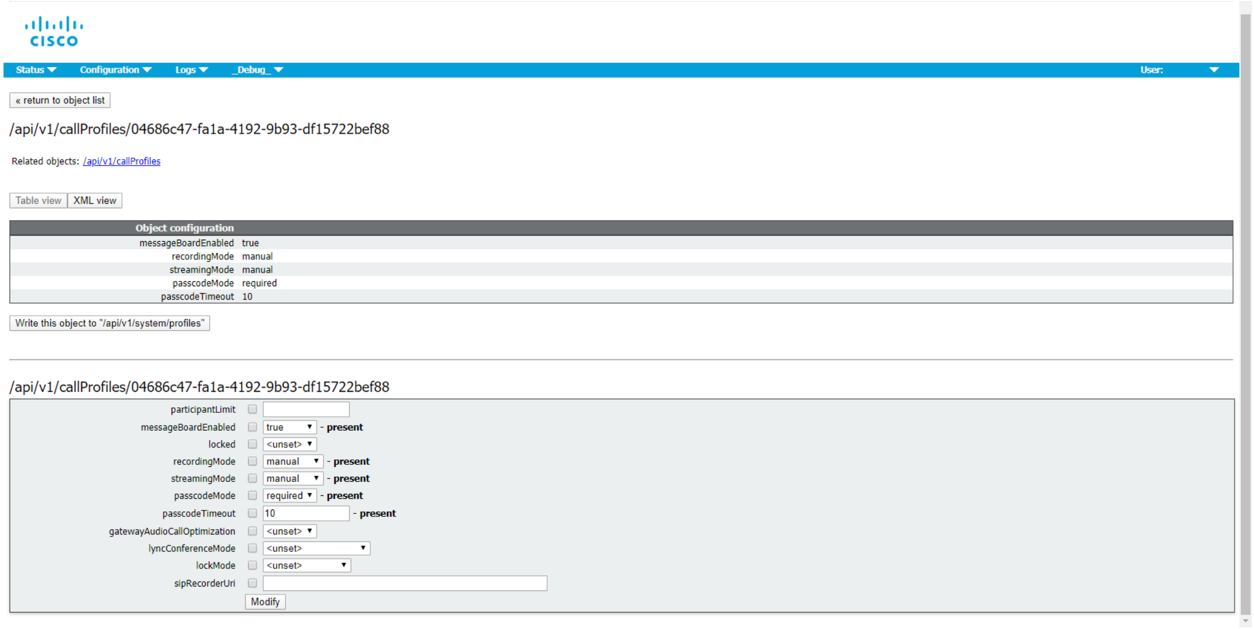
☑ Require delete confirmation

```
/api/v1/ac
/api/v1/ca
/api/v1/ca
/api/v1/callBridgeGroups ▶
/api/v1/callBridgeGroups/<id>
/api/v1/callBridges ▶
/api/v1/callBridges/<id>
/api/v1/callLegProfiles ▶
/api/v1/callLegProfiles/<id>
/api/v1/callLegProfiles/<id>/usage
/api/v1/callLegs ▶
/api/v1/callLegs/<id>
/api/v1/callLegs/<id>/callLegProfileTrace
/api/v1/callLegs/<id>/cameraControl
/api/v1/callLegs/<id>/generateKeyframe
/api/v1/callProfiles ▶
/api/v1/callProfiles/<id>
/api/v1/calls ▶
/api/v1/calls/<id>
/api/v1/calls/<id>/callLegs
/api/v1/calls/<id>/callLegs/<id>
```

Note: If you wish to delete any configured API objects, select **Allow delete** on the right-hand side of the screen. By default deletion is disallowed and **Require delete confirmation** is checked to help prevent unintentional deletions.

Using the API via the web interface offers a user-friendly way to work with the API as it gives a more visual approach to configuring your Meeting Server. For example, configuring callProfiles can be achieved using the check boxes and fields shown in Figure 6.

Figure 6: Configuring callProfiles using API access on the web interface



/api/v1/callProfiles/04686c47-fa1a-4192-9b93-df15722bef88

Related objects: /api/v1/callProfiles

Object configuration	
messageBoardEnabled	true
recordingMode	manual
streamingMode	manual
passcodeMode	required
passcodeTimeout	10

/api/v1/callProfiles/04686c47-fa1a-4192-9b93-df15722bef88

participantLimit	□		
messageBoardEnabled	□	true	- present
locked	□	<unset>	
recordingMode	□	manual	- present
streamingMode	□	manual	- present
passcodeMode	□	required	- present
passcodeTimeout	□	10	- present
gatewayAudioCallOptimization	□	<unset>	
lyncConferenceMode	□	<unset>	
lockMode	□	<unset>	
sipRecorderUri	□		

2.12 Ability to enable Automatic Gain Control (AGC)

Note: This feature was introduced in version 2.8 as a beta feature, however, it is now fully supported in version 2.9. It continues to be disabled by default.

Due to different audio levels being set by third party clients and the variation in audio levels from different headsets, conferences can often have participants that sound too loud or too quiet. Meeting Server uses Automatic Gain Control (AGC) to adjust audio level that it receives from individual participants in order to deliver as consistent an audio level across the conference as possible.

From 2.8, Meeting Server introduces Automatic Gain Control (AGC) on audio received by the Meeting Server. (It is not on audio transmitted by the Meeting Server.)

AGC will be applied to any endpoint (physical endpoints or soft clients) connected directly to the Meeting Server. It will not be applied to TIP calls or AVMCU (because this is a mixed audio stream).

Note:

- Skype participants connected to AVMCU will not be subject to any AGC as the AVMCU controls the audio.
- AGC is not applied to distribution links between Meeting Servers because this is a mixed audio stream.

AGC is disabled by default and can only be enabled via the new parameter **`audioGainMode`**, with possible options **`agc`** and **`disabled`**. This new parameter is supported on these APIs:

- GET and PUT operations on **`/callLegProfiles/<call leg profile id>`** and also POST on **`/callLegProfiles`**
- GET and PUT operations on **`/callLegs/<call leg id>`** and also POST on **`/callLegs`**
- GET and PUT operations on **`/calls/<call id>/callLegs`**

When AGC is enabled, the gain applied will be visible on the **Status > Calls** webadmin page. Also, there is a new API parameter **`gainApplied`** which is returned in response to a GET operation on **`/callLegs/<call leg id>`** under the **`rxAudio`** section.

2.13 Create and apply coSpace templates

From 2.9, Meeting Server introduces support for creating and applying coSpace templates. New APIs allow administrators to create templates with defined conference characteristics. These templates will be used by web app to simplify how end users create spaces and in the future could be used to apply spaces for end users. If no templates are assigned to an end user then they will not be able to create spaces in web app.

Previously, Meeting App clients/users could create spaces provided they had permission to do so. This permission was set using the API parameter canCreateCoSpaces in the userProfile assigned to that user. This setting does not apply to the new web app. Instead we give more detailed control to the administrator about not just who can create spaces but what type of spaces they can create. This is achieved by creating coSpace templates and specifying which templates a web app user has available to them.

Note: This feature can be configured via the API on Meeting Server. Cisco Meeting Management 2.9(RC1) and later versions provide a simpler web-based method to configure this feature. Please read the Cisco Meeting Management 2.9 Release Notes for further information.

This feature introduces the following new API objects in version 2.9:

- **`/coSpaceTemplates`**
- **`/coSpaceTemplates/<coSpace template id>`**
- **`/coSpaceTemplates/<coSpace template id>/accessMethodTemplates`**

- **`/coSpaceTemplates/<coSpace template id>/accessMethodTemplates/<access method template id>`**
- **`/ldapUserCoSpaceTemplateSources`**
- **`/ldapUserCoSpaceTemplateSources/<LDAP user coSpace template source id>`**
- **`/users/<user id>/userCoSpaceTemplates`**
- **`/users/<user id>/userCoSpaceTemplates/<user coSpace Template id>`**

For details of all API additions to support this feature, see the API additions summary.

2.13.1 How to create templates and assign to users

1. Create a coSpaceTemplates object using the API:
   - POST to **`/coSpaceTemplates`**
   - This operation can take the following request parameters:

Parameters	Type/Value	Description/Notes
name	String	the human-readable name associated with this coSpace template
description	String	a longer description of the coSpace template to give users an explanation of why they might want to use this template
callProfile	ID	if provided, associates the specified call profile with this coSpaceTemplate
callLegProfile	ID	if provided, associates the specified call leg profile with this coSpaceTemplate

2. Create 0, 1, or multiple access method template objects – this accessMethodTemplate object is specific to the coSpaceTemplate created in step 1 – using the API:
   - POST to **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates`**
   - This operation can take the following request parameters:

Parameters	Type/Value	Description/Notes
name	String	the human-readable name associated with this access method template
uriGenerator	String	the expression to be used to generate URI values for this access method template; the allowed set of characters are 'a' to 'z', 'A' to 'Z', '0' to '9', '.', '-', '_' and '$'; if non empty it must contain at least one '$' character
callLegProfile	ID	if provided, associates the specified call leg profile with this accessMethodTemplate

Parameters	Type/Value	Description/Notes
generateUniqueCallId	one of: true | false	

At this point, users can either be assigned templates using the API described below in step 3, or by creating a UserCoSpaceTemplateSource via the new /UserCoSpaceTemplateSources API and using that via the existing /ldapSources and /ldapSyncs APIs. See Applying userCoSpaceTemplates with LDAP.

3. Assign the coSpaceTemplate to a user with the API:
   - POST to **`/users/<user id>/userCoSpaceTemplates`**

Parameters	Type/Value	Description/Notes
coSpaceTemplate	ID	the id of a coSpace template that the user is allowed to use to instantiate a coSpace

2.13.2 Applying userCoSpaceTemplates with LDAP

1. Create, as you would for normal user provisioning, the following:
   - ldapServer – POST on /ldapServers node
   - ldapMapping – POST on /ldapMappings node
   - ldapSource – POST on /ldapSources node

   See the API reference Guide for more information.
2. For the ldapSource, create 0, 1, or multiple ldapUserCospaceTemplateSources – one for each coSpaceTemplate that you wish to apply to a set of users.
   - POST to **`/ldapUserCoSpaceTemplateSources`**
   - This operation can take the following request parameters:

Request Parameters	Type/Value	Description/Notes
coSpaceTemplate	ID	ID of the cospace template to be applied for these users
ldapSource	ID	ID of the LDAP source to be used to locate users
filter	String	Additional LDAP filter string to be applied when reading the source

The set of users that will be applied with the coSpaceTemplate is defined by the set produced by the ldapSource, filtered by the ldapUserCoSpaceTemplateSources 'filter' attribute.

Set the coSpaceTemplate attribute and the 'filter' attribute of the ldapUserCoSpaceTemplateSources accordingly.

3. Apply users and userCoSpaceTemplates using an LDAP sync via the API:
   - POST on /ldapSyncs node as for a normal LDAP synchronization.

Note: If the same user appears in more than one ldapSources/<id> filter, then that user's associated userProfile may change based upon the sync order that Meeting Server uses. (The userProfile contains permissions associated with that user, including hasLicense which associates a PMP license to that user.) This means that if a user is included in one ldapSources/<id> filter where the userProfile assigns PMP Plus licenses and is also included in an ldapSources/<id> filter where the userProfile doesn't assign licenses, then you cannot control whether that user is assigned a license.

2.14 Summary of 2.9 API Additions and Changes

New API functionality for the Meeting Server 2.9 includes:

- new API response value to support web app
- new API parameters to lock a meeting
- API parameter usage extended to admit participants from the lobby and to admit a participant into a meeting, bypassing the lobby.
- new API parameters to use a third party SIP recorder
- new API parameters to support panoramic video
- new API object and parameters to allow FECC on a remote system
- new API objects and parameters to support stronger ciphers
- new API parameter to control H.264 parameters used by Chromium browsers for WebRTC calls
- new API objects and parameters to support creating and applying cospace templates

The following new API objects are introduced in version 2.9:

- **`/callLegs/<call leg id>/cameraControl`**
- **`/coSpaceTemplates`**
- **`/coSpaceTemplates/<coSpace template id>`**
- **`/coSpaceTemplates/<coSpace template id>/accessMethodTemplates`**
- **`/coSpaceTemplates/<coSpace template id>/accessMethodTemplates/<access method template id>`**
- **`/users/<user id>/userCoSpaceTemplates`**
- **`/users/<user id>/userCoSpaceTemplates/<user coSpace Template id>`**
- **`/ldapUserCoSpaceTemplateSources`**

2.14.1 Retrieving web app information on a call leg

To find out if a call leg sub type is web app, when you do a GET on **`/callLegs/<call leg id>`**, the response value **`subType`** can return the new value of **`webApp`**.

2.14.2 Locking a meeting with the additional lock mode

To lock a meeting with the additional lock mode feature, a new API request parameter **`lockMode`** is added for:

- POST to **`/callProfiles`**
- PUT to **`/callProfiles/<call profile id>`**

For both the above operations, **`lockMode`** can be set to one of the following options:

- **`all`**: when the meeting is locked any new participants won't be admitted into the meeting and will be held in the lobby, this includes participants that don't need activation.
- **`needsActivation`**: when the meeting is locked, new participants that don't need activation will enter the meeting. However new participants that need activation will go into the lobby. Participants that are members of the cospace will bypass the lock and enter the meeting even if they require activation providing there is an activator already in the meeting.

2.14.3 Admitting participants from the lobby

When used on GET operations on **`/callLeg/<call leg id>`** API nodes, the existing **`deactivated`** parameter can take the values of **`true`** or **`false`**. The value **`true`** means the participant(s) are in the lobby; **`false`** means the participant(s) are in the meeting.

To support this new feature, usage of the API parameter **`deactivated`** is now extended to PUT and POST operations as detailed below. This parameter can only take the value of **`false`** for these operations.

To activate an individual participant to allow them into the meeting from the lobby, the **`deactivated`** parameter supports the following operation:

- PUT to **`/participants/<participant id>`**

To activate all participants to allow them into the meeting from the lobby, the **`deactivated`** parameter supports the following operation:

- POST to **`/calls/<call id>/participants/*`**

2.14.4 Creating a participant to go straight into a meeting, bypassing the lobby

To create a new participant and put them straight into the meeting, bypassing the lobby, the API parameter **`deactivated`** has been added for:

- POST to **`/calls/<call id>/participants`** the API parameter **`deactivated`**. This parameter can only take the value of **`false`**.

Note that to create a new participant for the specified meeting; the parameters are as per the callLeg create operation, but may result in the call leg instantiation ("owned" by the new participant object) to take place on a remote clustered call bridge.

2.14.5 Recording with a third-party SIP recorder

To record a meeting using a SIP recorder, a new request parameter **`sipRecorderUri`** is added for:

- POST to **`/callProfiles`**
- PUT to **`/callProfiles/<call profile id>`**

The **`sipRecorderUri`** parameter is the SIP recorder dial out URI string.

To find out the SIP recorder URI:

- GET on **`/callProfiles/<call profile id>`**. The response is structured as a top-level <callProfiles total="N"> tag with potentially multiple <callProfile> elements within it. Each <callProfile> tag may include **`sipRecorderUri`**.

2.14.6 Allowing Far End Camera Control (FECC) using the API

To allow FECC on a remote system's camera the following new API object is introduced:

- PUT to **`/callLegs/<call leg id>/cameraControl`**

This object supports the new optional request parameters:

`pan` – one of **`left`** or **`right`**. Pans the remote camera left or right.

`tilt` – one of **`up`** or **`down`**. Tilts the remote camera up or down.

`zoom` – one of **`in`** or **`out`**. Zooms the remote camera in or out.

`focus` – one of **`in`** or **`out`**. Focuses the remote camera in or out.

2.14.7 Using panoramic video

To support panoramic video, new response values are introduced to existing response elements as follows:

- GET on **`/callLegs/<callLeg ID>`** – the response element **`status`** has the element **`multistreamVideo`** which can return the following two new values:
  - **`numCameras`** which returns the number of multistream main video camera streams currently active for this call leg.

- **`numCamerasAvailable`** which returns the number of multistream main video camera streams advertised by the far end as being available for this call leg.

2.14.8 Determining the cipher suite used on a call leg

To find out the cipher suite used on a particular call leg:

- GET on **`/callLegs/<call leg id>`** response values support the new parameter **`cipherSuite`** which is returned under **`status`**. If any of this call leg's media is encrypted, the returned value gives the SRTP encryption cipher suite in use. One of:
  - **`AEAD_AES_256_GCM`** – AES encryption, 256 bit, GCM
  - **`AEAD_AES_128_GCM`** – AES encryption, 128 bit, GCM
  - **`AES_CM_128_HMAC_SHA1_80`** – AES encryption, 128 bit, 80 bit SHA1 authentication tag
  - **`AES_CM_128_HMAC_SHA1_32`** – AES encryption, 128 bit, 32 bit SHA1 authentication tag

2.14.9 Controlling H.264 parameters used by Chromium browsers for WebRTC calls

To control H.264 parameters used by Chromium browsers for WebRTC calls, a new request parameter **`chromeWebRtcH264interopMode`** is added for:

- POST to **`/compatibilityProfiles`**
- PUT to **`/compatibilityProfiles/<compatibility profile id>`**

The parameter **`chromeWebRtcH264interopMode`** is one of **`auto`** or **`none`**, where:

- **`auto`** – Default behavior. Allows 1080p main and content streams to be decoded using Chrome's software decoder.
- **`none`** – Legacy behavior.

From 2.9, Chromium browsers will now be using the software decoder by default, so there may be a CPU usage increase for WebRTC sessions – this is PC dependent.

Note: If this parameter is changed, the new setting is applied to any new WebRTC sessions; whilst active WebRTC sessions require a page refresh and will need to rejoin the call. Ongoing WebRTC calls are unaffected.

2.14.10 Using coSpace templates

2.14.10.1 Creating, modifying, retrieving, enumerating and deleting coSpace templates

The new API node **`/coSpaceTemplates`** is used to implement coSpace templates with the following request parameters:

Parameters	Type/Value	Description/Notes
name	String	the human-readable name associated with this coSpace template
description	String	a longer description of the coSpace template to give users an explanation of why they might want to use this template
callProfile	ID	if provided, associates the specified call profile with this coSpaceTemplate
callLegProfile	ID	if provided, associates the specified call leg profile with this coSpaceTemplate

This API node **`/coSpaceTemplates`** supports the following operations:

- POST to **`/coSpaceTemplates`**
- PUT to **`/coSpaceTemplates/<coSpace template id>`**
- DELETE on **`/coSpaceTemplates/<coSpace template id>`**
- GET on **`/coSpaceTemplates/<coSpace template id>`**, gives the following responses:

Response values	Type/Value	Description/Notes
name	String	the human-readable name associated with this coSpace template
description	String	a longer description of the coSpace template to give users an explanation of why they might want to use this template
callProfile	ID	if provided, associates the specified call profile with this coSpaceTemplate
callLegProfile	ID	if provided, associates the specified call leg profile with this coSpaceTemplate
numAccessMethodTemplates	Number	The number of access method templates associated with this coSpace template

- Enumerate GET on **`/coSpaceTemplates`**, gives the following responses:

URI parameters	Type/Value	Description/Notes
offset		an offset and limit can be supplied to retrieve coSpace templates other than the first page in the notional list
limit		
filter	String	supply filter=<string> to return just those coSpace templates that match the filter

The response is structured as a top-level <coSpaceTemplates total="N"> tag with potentially multiple <coSpaceTemplate> elements within it.

Each <coSpaceTemplate> tag may include the following elements:

Response elements	Type/Value	Description/Notes
name	String	the human-readable name associated with this coSpace template
callProfile	ID	if provided, associates the specified call profile with this coSpaceTemplate
callLegProfile	ID	if provided, associates the specified call leg profile with this coSpaceTemplate
numAccessMethodTemplates	Number	The number of access method templates associated with this coSpace template

2.14.11 Using Access Method templates

2.14.11.1 Creating, modifying, retrieving, enumerating and deleting coSpace template access method templates

2.9 introduces the new API node **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates`** with the following request parameters:

Parameters	Type/Value	Description/Notes
name	String	the human-readable name associated with this access method template
uriGenerator	String	the expression to be used to generate URI values for this access method template; the allowed set of characters are 'a' to 'z', 'A' to 'Z', '0' to '9', '.', '-', '_' and '$'; if non empty it must contain at least one '$' character
callLegProfile	ID	if provided, associates the specified call leg profile with this accessMethodTemplate
generateUniqueCallId	one of: true | false	whether to generate a unique numeric ID for this access method which overrides the global one for the cospace if this parameter is not supplied in a create (POST) operation, it defaults to "false"

The new API node **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates`** supports the following operations:

- POST to **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates`**
- PUT to **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates/<access method template ID>`**
- DELETE on **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates/<access method template ID>`**
- GET on **`/coSpaceTemplates/<coSpace template id>/accessMethodTemplates/<access method template id>`**, gives the following responses:

Response values	Type/Value	Description/Notes
name	String	the human-readable name associated with this access method template
uriGenerator	String	the expression to be used to generate URI values for this access method template; the allowed set of characters are 'a' to 'z', 'A' to 'Z', '0' to '9', '.', '-', '_' and '$'; if non empty it must contain at least one '$' character
callLegProfile	ID	if provided, associates the specified call leg profile with this accessMethodTemplate
generateUniqueCallId	one of: true | false	whether to generate a unique numeric ID for this access method which overrides the global one for the cospace if this parameter is not supplied in a create (POST) operation, it defaults to "false"

- Enumerate GET on **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates`**, gives the following responses:

URI parameters	Type/Value	Description/Notes
offset		an offset and limit can be supplied to retrieve coSpace access method templates other than the first page in the notional list
limit		
filter	String	supply filter=<string> to return just those coSpace access method templates whose name matches the filter
callLegProfileFilter	String	supply callLegProfileFilter=<string> to return just those coSpace access method templates that use the specified call leg profile

Response is structured as a top-level <accessMethodTemplates total="N"> tag with potentially multiple <accessMethodTemplate> elements within it.

Each <accessMethodTemplate> tag may include the following elements:

Response elements	Type/Value	Description/Notes
name	String	the human-readable name associated with this access method template
uriGenerator	String	the expression to be used to generate URI values for this access method template; the allowed set of characters are 'a' to 'z', 'A' to 'Z', '0' to '9', '.', '-', '_' and '$'; if non empty it must contain at least one '$' character
callLegProfile	ID	if provided, associates the specified call leg profile with this accessMethodTemplate
generateUniqueCallId	one of: true | false	whether to generate a unique numeric ID for this access method which overrides the global one for the cospace if this parameter is not supplied in a create (POST) operation, it defaults to "false"

2.14.11.2 Adding a name label to an access method (optional)

The new optional API parameter **`name`** allows you to add a name label to an access method to help identify the appropriate one to select to associate with your cospace template.

To add a name label to an access method, the parameter **`name`** takes the value of a string and is added for:

- POST to **`/coSpaces/<coSpace id>/accessMethods`**
- PUT to **`/coSpaces/<coSpace id>/accessMethods/<access method id>`**.

The **`name`** parameter is also returned for each access method in a GET response on **`/coSpaces/<cospaceId>/accessMethods`**

2.14.11.3 Adding a name label to an LDAP server (optional)

This API addition helps identify the LDAP server when shown in the user interface. To add a name label to an LDAP server, a new optional API request parameter **`name`** that takes the value of a string is added for:

- POST to **`/ldapServers`**
- PUT to **`/ldapServers/<ldap server id>`**.

The **`name`** parameter is also returned for each LDAP server in a GET response on **`/ldapServers`**

2.14.11.4 Applying coSpace templates to users

2.9 introduces the new API object **`/users/<user id>/userCoSpaceTemplates`** which supports the new request parameter **`coSpaceTemplate`**, where the value is the ID of a coSpace template that the user is allowed to use to instantiate a coSpace. The following operations are supported:

- POST to **`/users/<user id>/userCoSpaceTemplates`**

Parameters	Type/Value	Description/Notes
coSpaceTemplate	ID	the id of a coSpace template that the user is allowed to use to instantiate a coSpace

- DELETE on **`/users/<user ID>/userCoSpaceTemplates/<user coSpace template ID>`**
- GET on **`/users/<user ID>/userCoSpaceTemplates/<user coSpace template ID>`** will give the following response parameters:

Response parameters	Type/Value	Description/Notes
coSpaceTemplate	ID	The id of a coSpace template that the user is allowed to use to instantiate a coSpace.

Response parameters	Type/Value	Description/Notes
autoGenerated	one of true | false	Whether this coSpace template has been added automatically or manually: true - this template has been added automatically as part of an LDAP sync operation, therefore it is not possible to remove it except by modifying the parameters of the sync operation false - this template has been added via an API method. It can be modified or removed via the API.

- Enumerate GET on **`/users/<user ID>/userCoSpaceTemplates`** supporting the standard URI parameters "limit" and "offset". The response is structured as a top-level <userCoSpaceTemplates total="N"> tag with potentially multiple <userCoSpaceTemplate> elements underneath. Each <userCoSpaceTemplate> tag includes the request and response parameters ("coSpaceTemplate" and "autoGenerated").

URI parameters	Type/Value	Description/Notes
offset		an offset and limit can be supplied to retrieve access methods other than those in the first page of the notional list
limit		

2.14.11.5 Applying userCoSpaceTemplates with LDAP

2.9 introduces the new API object **`/ldapUserCoSpaceTemplateSources`** to allow users to create spaces using LDAP methods. This allows the template to be included directly in the source object.

This new API object **`/ldapUserCoSpaceTemplateSources`** supports the following operations:

- POST to **`/ldapUserCoSpaceTemplateSources`**
- PUT to **`/ldapUserCoSpaceTemplateSources`**

Request Parameters	Type/Value	Description/Notes
coSpaceTemplate	ID	ID of the cospace template to be applied for these users
ldapSource	ID	ID of the LDAP source to be used to locate users
filter	String	Additional LDAP filter string to be applied when reading the source

- GET on **`/ldapUserCoSpaceTemplateSources/<LDAP user coSpace template source id>`**, gives the following responses:

Response elements	Type/Value	Description/Notes
coSpaceTemplate	ID	ID of the cospace template to be applied for these users
ldapSource	ID	ID of the LDAP source to be used to locate users
filter	String	Additional LDAP filter string to be applied when reading the source

- Enumerate GET on **`/ldapUserCoSpaceTemplateSources`**, gives the following responses:

URI parameters	Type/Value	Description/Notes
offset		an offset and limit can be supplied to retrieve entries other than those in the first page of the notional list
limit		

Response is structured as a top-level <ldapUserCoSpaceTemplateSources total="N"> tag with potentially multiple <ldapUserCoSpaceTemplateSource> elements within it.

Each <ldapUserCoSpaceTemplateSource> tag may include the following elements:

Response elements	Type/Value	Description/Notes
coSpaceTemplate	ID	ID of the cospace template to be applied for these users
ldapSource	ID	ID of the LDAP source to be used to locate users

2.14.11.6 New API failure reasons

The following new API failure reasons are introduced in 2.9 for this feature:

- **`coSpaceAccessMethodTemplateDoesNotExist`** – You tried to modify, remove or retrieve a coSpace access method template using an ID that did not correspond to a valid coSpace access method template on the system.
- **`coSpaceTemplateDoesNotExist`** – You tried to modify, remove or retrieve a coSpace template using an ID that did not correspond to a valid coSpace template on the system.
- **`duplicateUserCoSpaceTemplate`** – You tried to assign the same coSpace template to a user for a second time.
- **`userCoSpaceTemplateDeletionProhibited`** – You tried to withdraw an auto-generated coSpace template assignment from a user and this is not allowed.
- **`userCoSpaceTemplateDoesNotExist`** – You tried to modify, remove or retrieve a user coSpace template using an ID that did not correspond to a valid user coSpace template for that user.
- **`ldapUserCoSpaceTemplateSourceDoesNotExist`** – You tried to remove or retrieve using an ID that did not correspond to an existing LDAP user coSpace template source entry.

2.15 Summary of CDR Changes

Version 2.9 introduces the following additions to the Call Detail Records of the Meeting Server:

- new value **`webApp`** added to the **`subType`** parameter in the callLegStart Record, indicates whether the call leg sub type is web app.
- new parameter **`recorderUri`** added in the recordingStart Record. This is a string and is the URI of the recording device if it is a SIP recorder. (Previously, both path and recorderUrl would always be provided however these are not sent for a SIP recorder. There is no change to the recordingEnd record.)

2.16 Summary of MMP additions

2.16.1 Web Bridge 3 support

Version 2.9 supports these MMP changes for the new web app implementation using Web Bridge 3:

Command	Description
`webbridge3`	Displays the current set of values for Web Bridge 3
`help webbridge3`	Displays help with all the webbridge3 subcommands
`webbridge3 restart`	Restarts the Web Bridge 3
`webbridge3 (enable|disable)`	Enables or disables the Web Bridge 3
`webbridge3 https listen <`*`interface`*`:port whitelist>`	Sets up the interface(s) and port(s) for the Web Bridge 3 to listen on. Enable the service to start listening with the command **`webbridge3 enable`**. There is no default value for the port; it needs to be specified.
`webbridge3 https certs <key-file> <crt-fullchain-file>`	Sets the HTTPS certificates for the Web Bridge 3. These are the certificates that will be presented to web browsers so they need to be signed by a certification authority (CA) and the hostname/purpose etc needs to match. (The certificate file is the full chain of certificates that starts with the end entity certificate and finishes with the root certificate.)
`webbridge3 https certs none`	Removes HTTPS certificate configuration
`webbridge3 http-redirect (enable [port]|disable)`	(Optional) Enables/disables HTTP redirects by setting up a port for HTTP connections. This port will be opened for all Meeting Server interfaces on which the web app has been configured. Incoming HTTP connections will be automatically redirected to the matching HTTPS port for the interface they arrived on. The default port, if you don't specify one in **`webbridge3 http-redirect enable [port]`**, is 80.
`webbridge3 c2w listen <`*`interface`*`:port whitelist>`	Configures the C2W connection. Sets up the interface(s) and port(s) for the Web Bridge 3 to listen on. You must enable the service to start listening with the command **`webbridge3 enable`**. We recommend that you make this address/port accessible from the Call Bridge(s) only.

Command	Description
`webbridge3 c2w certs <key-file> <crt-fullchain-file>`	Configures the C2W connection certificates – you need to configure the SSL Server certificates used for the C2W connection. The C2W certificate is only presented to Call Bridges connecting to the C2W protocol connection port – the hostname/purpose etc needs to match. (The certificate file is the full chain of certificates that starts with the end entity certificate and finishes with the root certificate.)
`webbridge3 c2w certs none`	Removes C2W connection certificate configuration.
`webbridge3 c2w trust <crt-bundle>`	Sets the trust bundle that Web Bridge 3 C2W server will verify the Call Bridge client certificate against to determine whether to trust them or not.
`webbridge3 c2w trust none`	Removes C2W connection trust bundle configuration.
`webbridge3 options <space-separated options>`	Switches on the specified features, if more than one feature is to be enabled then separate the feature_names with a space. Only use this command under instruction from Cisco Support or Cisco EFT. These features are not suitable for production use. The features will remain enabled across reboots, but will be automatically cleared when using the upgrade command. (This command is currently not supported.)
`webbridge3 options none`	Switches off all features that were previously switched on using the webbridge options <feature_name> command. Only use under instruction from Cisco Support. (This command is currently not supported.)
`webbridge3 status`	Displays the current configuration for Web Bridge 3

2.17 Summary of Event Changes

There are no new Events for version 2.9.

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 2.9

This section assumes that you are upgrading from Cisco Meeting Server software version 2.8. If you are upgrading from an earlier version, then Cisco recommends that you upgrade to 2.8 first following the instructions in the 2.8.x release notes, before following any instructions in these Cisco Meeting Server 2.9 Release Notes. This is particularly important if you have a Cisco Expressway connected to the Meeting Server.

Note: Cisco has not tested upgrading from a software release earlier than 2.8.

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 2.9

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

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

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

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

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

   `Cisco_Meeting_Server_2_9_1_CMS2000.zip`

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

   Hash (SHA-256) for upgrade.img file:
   19cf569772909cfd1c4cb3e1a3bd0818f7c32cf74f491f6ab0d4a2dd5d21d646

   `Cisco_Meeting_Server_2_9_1_vm-upgrade.zip`

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

   Hash (SHA-256) for upgrade.img file:
   5550cde2f4002d6e2ca45d0f0acca457483a0b46dc3e45b17bc91ca5e127a88e

   `Cisco_Meeting_Server_2_9_1_x-series.zip`

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

   Hash (SHA-256) for upgrade.img file:
   ce2444255217433fd6515857040bbdcc66078223ede33833a22acde0eb05f5cb

   `Cisco_Meeting_Server_2_9_1.ova`

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

   For vSphere6, hash (SHA-512) for Cisco_Meeting_Server_2_9_vSphere-6_0.ova file:
   b0d548c48965b2f8e12b0289ea2ffdd5934291d649bff88a1bd053e82c10a8cbc963773adbc1949627bdcf8c
   adc8d62896e39f2cb67b8f63dedb8d9163aa6c22

   For vSphere6.5 and higher, hash (SHA-512) for Cisco_Meeting_Server_2_9_vSphere-6_5.ova file:
   27c1ea70e1d955560b6e55268778027ccb5f8809395127acae3a4f5734b12ca6eee2cefb776290d99eb0544
   143310a173e91099f820d56b43d458bd4874966ad

2. To validate the OVA file, the checksum for the 2.9.1 release is shown in a pop up box that appears when you hover over the description for the download. In addition, you can check the integrity of the download using the SHA-512 hash value listed above.

3. Using an SFTP client, log into the MMP using its IP address. The login credentials will be the ones set for the MMP admin account. If you are using Windows, we recommend using the WinSCP tool.

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

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

4. Copy the software to the Server/ virtualized server.
5. To validate the upgrade file, issue the `upgrade list` command.
   a. Establish an SSH connection to the MMP and log in.
   b. Output the available upgrade images and their checksums by executing the upgrade list command.

      ```
      upgrade list
      ```

   c. Check that this checksum matches the checksum shown above.
6. To apply the upgrade, use the SSH connection to the MMP from the previous step and initiate the upgrade by executing the `upgrade` command.
   a. Initiate the upgrade by executing the upgrade command.

      ```
      upgrade
      ```

   b. The Server/ virtualized server restarts automatically: allow 10 minutes for the process to complete.
7. Verify that the Meeting Server is running the upgraded image by re-establishing the SSH connection to the MMP and typing:

   ```
   version
   ```

8. Update the customization archive file when available.
9. If you are deploying a scaled or resilient deployment read the Scalability and Resilience Deployment Guide and plan the rest of your deployment order and configuration.
10. If you have deployed a database cluster, be sure to run the `database cluster upgrade_schema` command after upgrading. For instructions on upgrading the database schema refer to the Scalability and Resilience Deployment Guide.
11. You have completed the upgrade.

3.2 Downgrading

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

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

The Server/ virtualized server will restart automatically – allow 10-12 minutes for the process to complete and for the Web Admin to be available after downgrading the server.

3. Log in to the Web Admin and go to **Status > General** and verify the new version is showing under **System status**.

4. Use the MMP command **`factory_reset app`** on the server and wait for it to reboot from the factory reset.

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

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

   The Meeting Server will reboot to apply the backup file.

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

6. In the case of XMPP clustering, you need to re-cluster XMPP:

   a. Pick one node as the XMPP master, initialize XMPP on this node

   b. Once the XMPP master has been enabled, joining any other XMPP nodes to it.

   c. Providing you restore using the backup file that was created from the same server, the XMPP license files and certificates will match and continue to function.

7. Finally, check that:

   - the Web Admin interface on each Call Bridge can display the list of coSpaces.
   - dial plans are intact,
   - XMPP service is connected
   - no fault conditions are reported on the Web Admin and log files.
   - you can connect using SIP and Cisco Meeting Apps (as well as Web Bridge if that is supported).

   The downgrade of your Meeting Server deployment is now complete.

3.3 Cisco Meeting Server 2.9 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 `2.9`.
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

Note: Refer to the Cisco Meeting App WebRTC Important information guide for information on resolved issues that affected the WebRTC app.

Note: Refer to the Cisco Meeting Server web app Important information guide for information on resolved issues that affected web app.

Issues seen in previous versions that are fixed in 2.9.1

Cisco identifier	Summary
CSCvt91847	All participants are dropped from a Cisco Meeting Server conference unexpectedly due to inconsistent lock status between local and remote Call Bridges in a distributed conference.
CSCvt92941	In rare circumstances WebRTC participants are dropped due to an xml parsing error.

Cisco identifier	Summary
CSCvt91634	All WebRTC and web app calls are dropped after a SIP endpoint shares presentation/content while in the same space.
CSCvt86179	Call Bridge may experience an unexpected restart.
CSCvt76282	In rare circumstances an unexpected restart may occur causing active calls to drop.
CSCvt59193	Meeting Server may restart unexpectedly when processing a number of XMPP messages.

Issues seen in previous versions that are fixed in 2.9

Cisco identifier	Summary
	None listed.

4.2 Open issues

Note: Refer to the Cisco Meeting App WebRTC Important information guide for information on open issues affecting WebRTC app.

Note: Refer to the Cisco Meeting Server web app Important information guide for information on open issues affecting web app.

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

Cisco identifier	Summary
CSCvt11301	Web Bridge 3 cannot start if Web Bridge 2 or Webadmin are listening on the same https port number even if on different interfaces.
CSCvt74060	Web Bridge 3 issues the following warnings on call join: "sendRequest() failure - cannot find WB3 websocket connection". This log message doesn't have any serious implications and can be ignored.
CSCvt74035	If Web Bridge 3 is not started, it is not shown up in either the "Recent errors and warnings" or "Fault conditions" sections.
CSCvt74031	If 4k content is being shared, participants receiving content will see a lower frame rate if they are on a different Call Bridge to the one hosting the participant sharing the content.

Cisco identifier	Summary
CSCvt74033	When content is being shared and an event happens to trigger a Webex Room Panorama to drop from sending two video streams to one, the video frame rate being received by a remote endpoint from the Room Panorama can drop noticeably.
CSCvt74047	The API `/api/v1/webbridges/<webbridge id>/status` always returns `connectionFailure`, even when its connection to a Call Bridge is working correctly.
CSCvt52420	The mediaProcessingLoad parameter returned in the system/load API on Meeting Server does not correctly account for calls using VP8 codec. When using VP8, there may be a higher actual media load on the Meeting Server than the API reports.
CSCvt74045	If you explicitly activate a participant into a locked meeting by posting deactivated=false to the participant API node and then unlock the meeting, that participant doesn't hear the expected prompt "this meeting is now unlocked".
CSCvn65112	For locally hosted branding, if the audio prompt files are omitted then the default built-in prompts are used instead. To suppress all audio prompts use a zero-byte file, rather than no file at all.
CSCvm56734	In a dual homed conference, the video does not restart after the attendee unmutes the video.
CSCvj49594	ActiveControl does not work after a hold/resume when a call traverses Cisco Unified Communications Manager and Cisco Expressway.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.
CSCvh23036	DTLS1.2, which is the default DTLS setting for Meeting Server 2.4, is not supported by Cisco endpoints running CE 9.1.x. ActiveControl will only be established between Meeting Server 2.4 and the endpoints, if DTLS is changed to 1.1 using the MMP command `tls-min-dtls-version 1.0`.
CSCvh23028	Changing the interface that the Web Bridge listens on or receiving a DHCP lease expire, will cause the Web Bridge to restart. WebRTC App users may have to log in again.
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.
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.

Cisco identifier	Summary
CSCve64225	Cisco UCS Manager for Cisco Meeting Server 2000 should be updated to 3.1(3a) to fix OpenSSL CVE issues.
CSCve37087 but related to CSCvd91302	One of the media blades of the Cisco Meeting Server 2000 occasionally fails to boot correctly. Workaround: Reboot the Fabric Interconnect modules.

In addition there is the following limitation:

CAUTION: The maximum number of concurrent XMPP clients supported by the current Meeting Server software is 500.This maximum is a total number of all different clients (Cisco Meeting App, WebRTC Sign-in and WebRTC Guest clients) registered at the same time to clustered Meeting Servers. If the number of concurrent XMPP registrations exceeds 500 sessions, some unexpected problems with sign in may occur or it may lead to a situation where all currently registered users need to re-sign in, this can cause a denial of service when all users try to sign in at the same time.

Cisco Legal Information

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

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

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

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)