Cisco Meeting Server

Cisco Meeting Server Release 2.7.1

Release Notes

May 11, 2020

Contents

What's changed

Version	Change
May 11, 2020	Open issues updated.
December 06, 2019	Issues resolved updated. (Documentation omission)
December 03, 2019	OVA file hashes added.
November 29, 2019	Added caution related to changing loadLimit value for Cisco Meeting Server 2000 in the Upgrading section.
November 28, 2019	First maintenance release. Beta support for Yandex and Chromium-based Microsoft Edge browsers, and new meeting join options introduced. See Issues resolved in 2.7.1 Hashes updated
September 19, 2019	Resolved issues updated (documentation omission).
August 28, 2019	Resolved issues updated (documentation omission).
August 13, 2019	New release of Cisco Meeting Server software.

1 Introduction

These release notes describe the new features, improvements and changes in release 2.7 of the Cisco Meeting Server software.

The Cisco Meeting Server software can be hosted on:

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

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.

CAUTION: Upgrading to version 2.7 may affect the operation of your database cluster. Before upgrading to version 2.7, ensure client and server certificates signed by the same Certificate Authority are uploaded to each Meeting Server holding or connecting to a database node in the cluster. For more information, see Section 2.4.

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.

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

1.1 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.

1.1.1 Cisco Meeting Server 1000 and other virtualized platforms

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

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

Note: Although you are encouraged to ensure the virtualized platform running the Cisco Meeting Server software is up to date with the latest patches, only the Cisco Meeting Server 1000 M5 should be upgraded to ESX 6.7 or ESXi 6.5 Update 2. For more information, see here.

1.1.2 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.

Note: From around August 2019, Fabric Interconnect failover should be enabled by default on new Cisco Meeting Server 2000s. However, If you need to manually configure your device to enable failover, see here for more information.

1.1.3 Call capacities

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

Table 1: Call capacities

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

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 from software version 2.6.

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

1.2 Cisco Meeting App WebRTC Important information

For information on when features are released and bugs fixed for the WebRTC app, refer to the Cisco Meeting App WebRTC Important information guide. All of the information relevant to the WebRTC app has been combined into one document, and is no longer included in the Meeting Server release notes.

The document describes the following:

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

WebRTC is still an evolving technology and frequent changes are implemented by browser vendors. The Cisco Meeting App WebRTC Important information guide will be updated when we need to inform you of upcoming changes.

Note: 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.

1.3 End Of Software Maintenance

On release of Cisco Meeting Server software version 2.7, 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 2.5.x	4 months after the first release of Cisco Meeting Server version 2.7.

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

2 New Features/Changes in version 2.7

Version 2.7 of the Meeting Server software, adds the following:

- enhancements to the pane placement feature first introduced in version 2.4,
- performance improvements in content sharing between Lync/Skype for Business clients and non-Lync clients (SIP endpoints and Cisco Meeting App users),
- enforces the use of certificates on database clients and database servers within a database cluster,
- utilization statistics added to syslog to aid understanding of Meeting Server utilization,
- ICE tracing added to the **Detailed tracing** page of the Web Admin Interface. Log into to the Web Admin Interface of your Meeting Server. Go to **Logs > Detailed tracing**, scroll down to find the ICE tracing and select the appropriate Enable button. This new serviceability feature will help Cisco Support in diagnosing issues.

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.

2.1 New features introduced in version 2.7.1

2.1.1 Beta support for Yandex browser in WebRTC app

Version 2.7.1 introduces Beta support for Cisco Meeting App for WebRTC using Yandex browsers on Windows. This is beta quality in current version.

2.1.2 Beta support for Chromium-based Microsoft Edge browser in WebRTC app

Version 2.7.1 adds Beta support for Cisco Meeting App for WebRTC using Chromium-based Microsoft Edge browser on Windows. This is beta quality in current version.

2.1.3 Joining options with no microphone or camera for WebRTC app

Version 2.7.1 introduces some new joining call options.

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

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

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

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

2.2 Pane placement improvements

Version 2.4 introduced the API pane placement feature to allow you to control which participant appears in which pane on the screen of endpoints dialing into a space on the Meeting Server. This feature is extended in version 2.7 by the addition of the following enhancements:

- the **`panePlacementHighestImportance`** can be configured for **`/calls`** in addition to **`/coSpaces`**,
- a self pane mode to enable participants with an assigned importance level to see their own self pane displayed within the pane layout.

In addition, from version 2.7, Cisco Meeting Management supports applying Pane placement and Self-view to active calls, for more information refer to the Cisco Meeting Management 2.7 User Guide for Video Operators. Cisco Meeting Management does not support pane placement on spaces.

The information in this section is also provided in the Cisco Meeting Server 2.7 Administrator Quick Reference Guide on Screen Layouts and Pane Placement.

2.2.1 `panePlacementHighestImportance` extension

In version 2.7, the API parameter **`panePlacementHighestImportance`** can now be applied when creating a new call using the API method POST on the **`/calls`** node, and to an active call using PUT to **`/calls/<call id>`**.

`panePlacementHighestImportance` on **`/calls`** provides the same functionality as **`panePlacementHighestImportance`** on **`/coSpaces`**, but with the following additional order of precedence:

- use the value set for **`panePlacementHighestImportance`** on **`/calls`**
- if **`panePlacementHighestImportance`** on **`/calls`** is unset, then use the value set for

panePlacementHighestImportance on **/coSpace** (if the call is to a space)

- if **panePlacementHighestImportance** is still unset, then pane placement is disabled.

If the **panePlacementHighestImportance** parameter is set to a value smaller than the number of panes in the screen layout, then the remaining panes unused for important participants will be taken by participants with no importance assigned, these panes will remain dynamically allocated.

Note: Setting the **panePlacementHighestImportance** parameter on an active call will only apply to that call, and will not persist between calls. This differs to setting the **panePlacementHighestImportance** parameter on a specific space which will persist between calls to that space.

Note: If pane placement is activated at a **/coSpace** level, it can not be deactivated at a **/call** level.

2.2.2 Self pane mode

The self pane mode extends the pane placement feature introduced in version 2.4, and follows the same placement logic as pane placement, but with the addition of showing the self pane of the important participant within the layout displayed on the important participant's endpoint. Self pane mode is supported across a Call Bridge cluster .

Prior to version 2.7, an important participant never saw a pane showing themselves, it was skipped over and never displayed within the pane layout on their endpoint, which resulted in the participant seeing a different layout to others. From version 2.7, an administrator setting the parameter **panePlacementSelfPaneMode** on a call or a space can select whether participants with an assigned importance level are able to see their "self" pane in the layout, or a blank pane, or skipped over. Setting the **panePlacementSelfPaneMode** parameter to self or blank and setting the value for **panePlacementHighestImportance** to match the number of panes in the selected screen layout has the effect of fixing the pane placement on all SIP endpoints dialing into the call or the space.

It is recommended that each importance level is only assigned to a single participant if using the self pane mode, assigning an importance level to more than one participant can result in an incorrect self pane being displayed to the participant.

If the **panePlacementHighestImportance** parameter is set to a value smaller than the number of panes in the layout, then the remaining panes not used for important participants will be taken by participants with no importance assigned, these panes will remain dynamically allocated. Similarly, if the number of panes in the selected layout is less than the number of participants with an assigned importance, then only those assigned the highest importance levels will appear in the panes and only their self panes will be displayed.

Self pane mode is typically used in conjunction with setting the screen layout and preventing a participant from changing their screen layout (through **/dtmfProfiles**).

Use the API to set **panePlacementSelfPaneMode** for:

- an existing specific space. PUT to **/coSpaces/<coSpace id>** the request parameter **panePlacementSelfPaneMode** set to **self**, **skip**, **blank** or leave unset, see below.
- a new space. POST to **/coSpaces** with the request parameter **panePlacementSelfPaneMode** set to the chosen value,
- an active call, that is already in existence. PUT to **/calls/<call id>** the request parameter **panePlacementSelfPaneMode** set to the chosen value,
- a new call that is being created. POST to **/calls** with the request parameter **panePlacementSelfPaneMode** set to the chosen value.

The parameter **panePlacementSelfPaneMode** can take the values:

self - participants with importance set will see themselves in a specific pane in the pane layout.

skip - same as the pre-2.7 version behavior, on a per-viewer basis the screen layout skips the self pane and displays the pane of the next important participant.

blank - leaves a blank pane instead of displaying the important participant, so the important participant still sees the other participants in the same pane position as all other viewers.

if the **panePlacementSelfPaneMode** parameter value is left unset, the self pane mode follows this order of precedence:

- use the value set for **panePlacementSelfPaneMode** on **/calls**,
- if **panePlacementSelfPaneMode** on **/calls** is unset, then use the value set for **panePlacementHighestImportance** on **/coSpace** (if the call is to a space),
- if **panePlacementSelfPaneMode** on **/coSpace** is also unset, then it reverts to the **skip** behavior defined above.

By default, the **panePlacementSelfPaneMode** parameter value is left unset.

Setting self pane mode

To use the self pane mode:

1. Set the importance levels of participants, as appropriate for the call or the space
2. Set a value for the **panePlacementHighestImportance** parameter. Note: if **panePlacementHighestImportance** is unset, then self pane mode does not take effect.
3. Set **panePlacementSelfPaneMode** = **self** or **skip** or **blank** or **<unset>** on **/coSpaces**, **/coSpaces/<coSpace id>**, **/calls** or **/calls/<call id>** as required.

Note: If a participant is assigned an importance level greater than the value set for **panePlacementHighestImportance**, then they will not see their self pane. Self panes are only included in the end point layout for participants with importance set equal or less than the **panePlacementHighestImportance**. However, participants with importance values greater than **panePlacementHighestImportance** will still be displayed to other participants.

Note: If participant labels are turned on, then the participant labels will be displayed on the self pane.

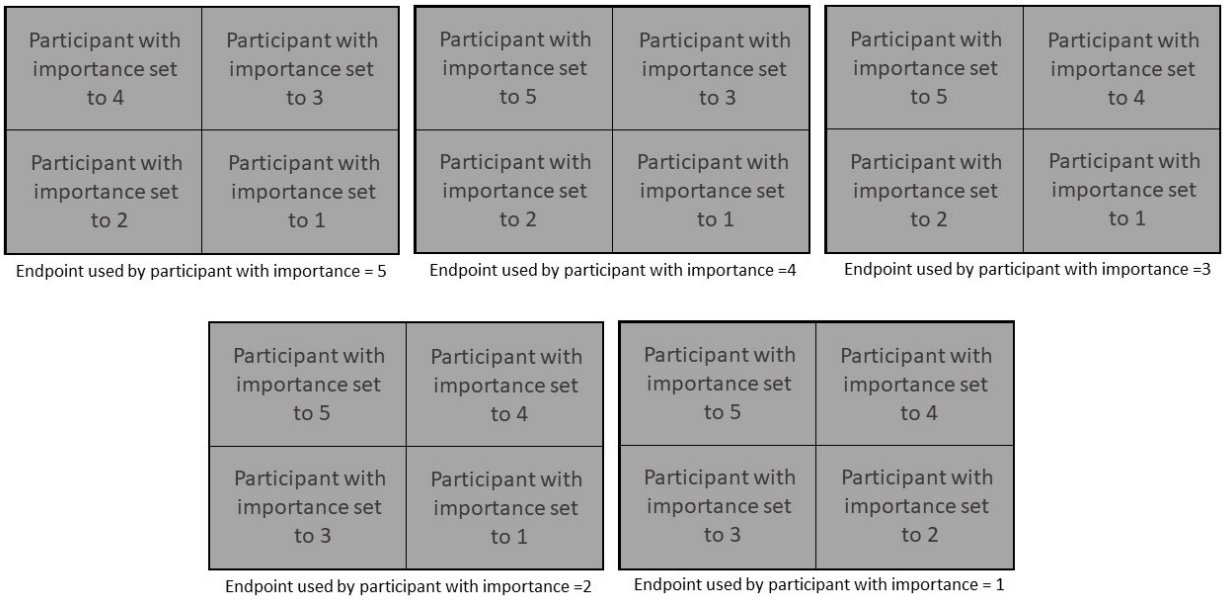
Note: Although a participant using an endpoint without "self-view" can use their self pane to ensure they are correctly framed within the pane, it is not recommended that participants use self pane in this way on endpoints capable of locally rendering self-view. The quality of self pane will not be as good as the locally rendered self-view, as the video stream for self pane is transcoded which adds latency.

Example

Figure 1 and Figure 2 below illustrate the pane layout on SIP endpoints used by 5 participants dialing into the same call. The example assumes:

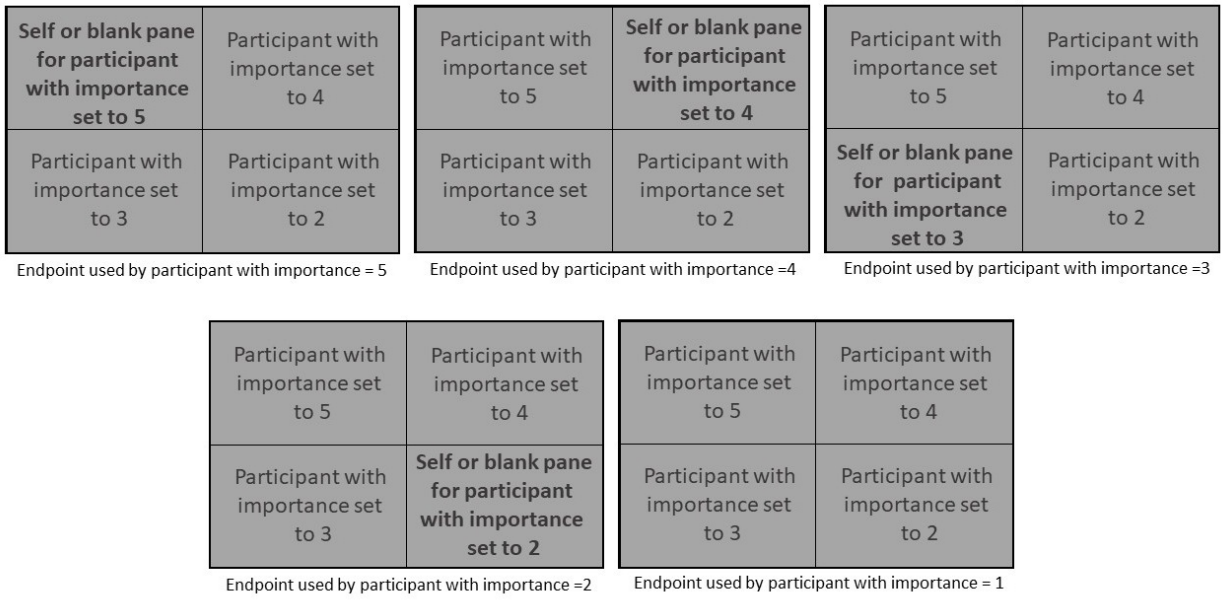
- each endpoint is configured to use **allEqualQuarters** screen layout in a fixed 2x2 layout,
- each participant has a unique importance level set from 5 to 1 when they dial into the call,
- the call has **panePlacementHighestImportance** = **5**
- **panePlacementSelfPaneMode** is set either to **skip**, **self** or **blank**

Figure 1: **panePlacementSelfPaneMode** set to **skip** (default mode)



Setting **panePlacementSelfPaneMode**= **skip** results in each of the five endpoints displaying a different pane layout.

Figure 2: **panePlacementSelfPaneMode** set to **self** or **blank**



Setting **panePlacementSelfPaneMode**= **self** or **blank** results in a fixed layout across the five endpoints. Participant with importance set to 1 will not be displayed on any of the 5 endpoints, in addition if others join the call without an importance set, then the endpoint they use will show the same pane placement as that for participant with an importance of 1.

2.3 Remote Desktop Protocol (RDP) improvements

Version 2.7 includes improvements in content sharing from Microsoft Lync/Skype for Business/Office365 clients to clients connected to a Meeting Server. The improvement requires the Skype client to support the Graphics Pipeline Extension. Depending upon the content shared, a 4x faster initial content share or 4x improvement in frame rate may be observed; this performance improvement results from reduced bandwidth per frame when the Graphics Pipeline Extension is supported by the Skype client. The latest Window's Skype client supports the Graphics Pipeline Extension, where as the Mac iOS Skype clients do not.

2.4 Certificates required for a database cluster

From version 2.7, database clusters require client and server certificates signed by the same CA configured in each Meeting Server holding or connecting to a database in the cluster. Enforcing the use of certificates ensures both confidentiality and authentication across the cluster.

If you already have certificates configured then they should continue to work on upgrade. There is no change to the certificate requirements – the only change is that from 2.7 it's now mandatory to have certificates configured.

Note: Configuring certificates is not required on a database running in local mode which is not part of a database cluster. "Cautions" in this section do not apply in local mode.

CAUTION: The database nodes forming the cluster must be configured with a trusted root CA certificate so that only legitimate nodes can connect to the cluster. The nodes will trust connections that present a certificate chain that ends with a trusted root certificate. Therefore each database cluster must use a dedicated root certificate, the root certificate or intermediate certificates must not be used for any other purpose.

CAUTION: If a database cluster was configured without certificates using an earlier version of Meeting Server software which did not require certificates, then on upgrading to version 2.7 the database will stop and remain unreachable until certificates are configured and the database cluster is recreated.

Certificates can only be assigned to a disabled database cluster. If you have already set up a database cluster you must run the **`database cluster remove`** command on every server in the cluster, then run the commands to upload and assign the certificates to the host servers , before re-creating the cluster. See the Certificate Guidelines for full information on creating, uploading and assigning the certificates and certificate bundles to the database cluster.

To support this change:

- the **database cluster initialize**, **database cluster join** and **database cluster connect** commands will not run without valid certificates, keys and CA certificates uploaded to the database clients and servers. A message is given to this effect.
- the **database cluster status** command will highlight the lack of configured certificates.

2.4.1 New error message

FAILURE: certificates must be configured

Displayed when creating, joining or connecting to a database cluster, indicates that certificates have not been configured on this database server or client.

2.4.2 Updated and new pki commands

As database cluster certificates are mandatory from 2.7, to make it easier to setup Meeting Server database clustering there are updated/new pki commands to create signed certificates for the database cluster as follows:

- **pki selfsigned <key/cert basename>[<attribute>:<value>]**
- **pki sign <csr/cert basename> <CA key/cert basename>**

Note: These updated and new pki commands are an additional way of creating certificates. You can still use other methods, for example openssl, to create certificates. See the Certificate Guidelines for more information.

2.4.3 Creating certificates for a database cluster using pki commands

From 2.7 you can generate all certificates directly from the MMP using the new/updated pki commands. Follow the steps below to generate a local private key and a self-signed certificate on the Meeting Server:

1. Log in to the MMP and use the command:

   For example:

   pki selfsigned dbca CN:"My company CA"

   creates a local private key named **dbca.key** and a self-signed certificate with the common name **CN=My company CA** in dbca.crt

2. Create a private key and Certificate Request File for the database server. You can use the same certificate on all of the servers in the database cluster; specify the FQDN of one of the servers in the CN field and specify the FQDN of the other servers in the SAN field.

   For example:

   pki csr dbserver CN:server01.db.example.com subjectAltName:server02.db.example.com

   generates a CSR file named dbserver.csr and private key named dbserver.key

3. Create a private key and Certificate Request File for the database client. The CommonName (CN) for a database client must equal 'postgres'.

   For example:

   ```
   pki csr dbclient CN:postgres
   ```

   generates a CSR file named dbclient.csr and private key named dbclient.key

4. Sign the dbserver.csr and dbclient.csr certificate signing request files and obtain the corresponding dbserver.crt and dbclient.crt certificates, as well as the Internal CA certificate (bundle).

   For example:

   ```
   pki sign dbserver dbca
   ```

   ```
   pki sign dbclient dbca
   ```

5. Install the certificates and private keys for database clustering – firstly, download via SFTP and then upload to each Meeting Server that belongs to the same database cluster.

CAUTION: These pki instructions can be run anytime. However, the database cluster must be disabled for the configuration of the generated certificates (i.e. database cluster certificates). If you have already set up a database cluster you must run the **`database cluster remove`** command on every server in the cluster to disable it, then run the commands to configure the generated certificates before re-creating the cluster.

The certificate for the database client must have CN set to "postgres". You can check that certificate is suitable using the **`pki inspect`** command. For example:

```
cms> pki inspect dbclient.crt
Checking ssh public keys...not found
Checking user configured certificates and keys...found
File contains a PEM encoded certificate
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            58:00:00:00:1c:3b:92:8a:95:d2:21:89:58:00:00:00:00:00:1c
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=com, DC=support, CN=support-DC2-CA
        Validity
            Not Before: Sep 13 13:32:38 2015 GMT
            Not After : Sep 13 13:42:38 2017 GMT
        Subject: CN=postgres
```

If you have CN set to anything other than postgres for the database client certificate you will see the error message: "ERROR: Client certificate common name incorrect" when configuring the cluster.

Note: the **`database cluster initialize`**, **`database cluster join`** and **`database cluster connect`** commands will not run without valid certificates, keys and CA certificates uploaded to

---

the database clients and servers. The error message: **`FAILURE: certificates must be configured`** displays to indicate that certificates have not been configured on this database server or client.

2.4.4 Uploading certificates for a database cluster

You now need to upload the certificates to the Meeting Server and then configure clustering.

1. On the host server of every database (whether co-located with a Call Bridge or not):
    a. SFTP the following certificate and keys to the Call Bridge server:
        - dbserver.key
        - dbserver.crt
        - dbclient.key
        - dbclient.crt
        - the certificate bundle provided by the internal CA. As per this example, the file will be dbca.crt
    b. Specify the certificates that will be used when the database cluster is built. For example:

```
cms>database cluster certs dbserver.key dbserver.crt dbclient.key
dbclient.crt dbca.crt
Certificates updated
cms> database cluster status
Status                    : Disabled
Interface                 : a
Certificates
  Server Key              : dbserver.key
  Server Certificate      : dbserver.crt
  Client Key              : dbclient.key
  Client Certificate      : dbclient.crt
  CA Certificate          : dbca.crt
```

Note: The **`database cluster status`** command will highlight if there is a lack of configured certificates.

2. For every Call Bridge not co-located with a database:
    a. SFTP the following certificate and keys to the Call Bridge server:
        - dbclient.key
        - dbclient.crt
        - the certificate bundle provided by the internal CA. As per this example, the file will be dbca.crt

b. Configure the database cluster to use these certificates:

```
cms> database cluster certs dbclient.key dbclient.crt dbca.crt
Certificates updated
cms> database cluster status
Status                    : Disabled
Interface                 : a
Certificates
  Client Key              : dbclient.key
  Client Certificate      : dbclient.crt
  CA Certificate          : dbca.crt
```

3. Now return to the Server Deployment Guide for information on selecting the master database and building the database cluster.

For more information on creating and uploading certificates to the Meeting Server, see the Cisco Meeting Server 2.7, Certificate Guidelines for Scalable and Resilient Server Deployments.

2.5 Utilization statistics

From version 2.7, the syslog mechanism can be used to trace utilization metrics from the Meeting Server at regular 5 minute intervals. The following utilization statistics have been added as syslog messages:

```
STATS: {"callsLegsPS":X, "callLegs":"<A>/<B>", "CMA":<A>/<B>", "sip":
{"std":"<A>/</B">, "peer":<A>/<B>} }
```

where:

"callsLegsPS" provides the high water mark rate of new call legs per second, this is the maximum rate observed in the last 5 minutes on the Meeting Server returning the statistic.

<A> is the number of call legs of that type that were active at the time of logging,

<B> is the high water mark for call legs of that type,

"callLegs" gives the total across all call types listed.

"CMA" covers callLegs created by using native Cisco Meeting App for Window, Mac or iOS, and by using the WebRTC app.

"sip" is broken down into **"std"** for standard calls to SIP endpoints, and includes Nortel SIP gateway call legs and Avaya call legs, and **"peer"** for distribution links placed between separate Call Bridges for sharing media in distributed conferences.

For example:

```
STATS: {"callsLegsPS":23, "callLegs":"139/262", "CMA":43/43", "sip":
{"std":"43/221, "peer":42/120} }
```

```
STATS: {"lync":{"AV":"A/B", "Tx":"A/B", "Rx":"A/B", "proxy":"A/B",
"conf":"A/B", "focus":"A/B", "IM":"A/B"}}
```

where:

Lync includes Skype for Business and Office 365,

"AV" means Audio-Video,

"Tx" and **"Rx"** represent application sharing outgoing and incoming,

"proxy" is a LyncProxy call leg,

"conf" is the conference subscription call leg,

"IM" is the Instant Messaging (IM) call leg.

For example:,

```
STATS: {"lync":{"AV":"2/7", "Tx":"1/3", "Rx":"0/1", "proxy":"1/4",
"conf":"2/14", "focus":"2/14", "IM":"2/13"}}
```

```
STATS: {"mediaLoad": 0}
```

"mediaLoad" is a snapshot of the media load on the Call Bridge at the time of printing the stats. It is the same value that can be obtained by performing a GET on the **/system/load** API node.

For example:

```
STATS: {"mediaLoad": 0}
```

In clustered deployments, the statistics for each Meeting Server should be syslog'ed around the same time, but not necessarily synchronized. Assuming that NTP is configured on each Meeting Server, combining the cluster wide syslog messages should make it possible to obtain a sufficiently accurate representation of cluster utilization.

2.6 Summary of MMP changes

Version 2.7 supports these MMP changes:

Command	Description
database cluster status	Updated command. From 2.7, this command will highlight the lack of configured certificates. Displays the clustering status, from the perspective of this database instance.
database cluster initialize	Updated command. From 2.7, this command will not run without valid certificates, keys and CA certificates uploaded to the database clients and servers . Creates a new database cluster, with this server's current database contents as the one and only database instance—the master.
database cluster join <host-name/IP address>	Updated command. From 2.7, this command will not run without valid certificates, keys and CA certificates uploaded to the database clients and servers . Creates a new database instance as part of the cluster copying the contents of the master database to this server and destroying the current contents of any database on it.
pki selfsigned <key/cert basename>[<attribute>:<value>]	Updated command. From 2.7, allows you to specify attrib-utes/values.
pki sign <csr/cert basename> <CA key/cert basename>	New command. From 2.7, this command signs the csr identified by <csr/cert basename> and generates a certificate with the same basename, signed with the CA certificate and key identified by <CA key/cert basename> .

2.6.1 New error message

FAILURE: certificates must be configured

Displayed when creating, joining or connecting to a database cluster, indicates that certificates have not been configured on this database server or client.

2.6.2 Default cipher string changed

ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES:!aDH:!aECDH

in addition **:!aDH:!aECDH:!SEED:!eNULL:!aNULL** is automatically appended to the configured cipher string to disallow very weak ciphers.

2.7 Summary of 2.7 API Additions & Changes

New API functionality for the Meeting Server 2.7 includes:

- support for the API parameter **panePlacementHighestImportance** to be set on the API **/calls** object.
- new API parameter **panePlacementSelfPaneMode** on the API **/coSpaces** and **/calls** objects. This enables a "self" pane to be inserted into a screen layout on the SIP endpoint,

2.7.1 Setting **panePlacementHighestImportance** on **/calls**

To set the highest importance value for pane placement for all calls:

- POST to **/calls** the request parameter **panePlacementHighestImportance** set to the chosen value.

To set the highest importance value for pane placement on a specific call:

- PUT to **/calls/<call id>** the request parameter **panePlacementHighestImportance** set to the chosen value.

To retrieve the **panePlacementHighestImportance** value for a call, use GET on **/calls/<call id>**.

To remove pane placement leave the **panePlacementHighestImportance** parameter as unset (leave parameter value as blank).

Note: Setting the **panePlacementHighestImportance** parameter on a specific call will only apply to that call, and will not persist between calls. This differs to setting the **panePlacementHighestImportance** parameter on a specific space which will persist between calls to that space.

2.7.2 Setting **panePlacementSelfPaneMode**

The **panePlacementSelfPaneMode** parameter can take the value of "skip", "self", "blank" or "", see below. This parameter will only have any effect when **panePlacementHighestImportance** is also configured. **panePlacementHighestImportance** can be set on the **/coSpaces** or **/calls** objects.

skip	This has the same effect of pane placement prior to version 2.7, the pane of the participant with importance level "n" is not displayed in the screen layout on their endpoint and instead the participant with the next importance level is displayed.
self	The pane of the participant with importance level "n" is displayed in the screen layout on their endpoint, so they see themselves.
blank	Important participants see a blank pane rather than their self pane. This ensures that important participants see the same pane layout as all other viewers.

<unset> or ""	Follows the precedence order determined by the **panePlacementHighestImportance** setting at **/call** level, or if after this it remains unset, reverts to **skip** behavior defined above.

To set the self pane mode for all calls and spaces:

- POST to **/calls** the request parameter **panePlacementSelfPaneMode** set to the value of "skip", "self", "blank" or "" (see table above)
- POST to **/coSpaces** the request parameter **panePlacementSelfPaneMode** set to the chosen value.

To set the self pane mode on a specific call or specific space:

- PUT to **/calls/<call id>** the request parameter **panePlacementSelfPaneMode** set to the chosen value.
- PUT to **/coSpaces/<coSpace id>** the request parameter **panePlacementSelfPaneMode** set to the chosen value.

To retrieve the **panePlacementSelfPaneMode** value for a call or space, use GET on **/calls/<call id>** or a GET on **/coSpaces/<coSpace id>**.

2.8 Summary of CDR Changes

There are no new CDR records or parameters for version 2.7.

2.9 Summary of Event Changes

There are no new Events for version 2.7.

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 2.7

This section assumes that you are upgrading from Cisco Meeting Server software version 2.6. If you are upgrading from an earlier version, then Cisco recommends that you upgrade to 2.6 first following the instructions in the 2.6.x release notes, before following any instructions in these Cisco Meeting Server 2.7 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 2.6.

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

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

3.1 Upgrading to Release 2.7

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.

CAUTION: Upgrading to version 2.7 may affect the operation of your database cluster. Before upgrading to version 2.7, ensure client and server certificates signed by the same Certificate Authority are uploaded to each Meeting Server holding or connecting to a database node in the cluster. For more information, see Section 2.4.

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.

CAUTION: When upgrading Meeting Server 2000 from 2.5 (or earlier) to 2.6 (or later), you need to increase the loadLimit value for load balanced Meeting Server 2000 deployments to ensure maximum capacity. If you have already increased the loadLimit value when you installed version 2.6, then no further increase is required.

For each Meeting Server 2000 being upgraded, change the **`loadLimit`** field in **`system/configuration/cluster`** API:

- from 500,000 (suitable for 2.5 and earlier)
- to 700,000 (suitable for 2.6 and later)

This change is required to benefit from the increased capacity in HD/fullHD explained in the 2.6 release notes. If this configuration change is not done, it will result in a capacity decrease for SD calls in load balancing deployments.

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_7_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:
   d51d3ef90854a7dd10aa9acb11975f8f5cf6de683c4ae4471ac0e77087912c2e

   `Cisco_Meeting_Server_2_7_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:
   dd0d49a729da16d31aa3658dc4d0193f3431216f4200082438057040e443413e

   `Cisco_Meeting_Server_2_7_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:
   3820cee312feb2b4e7eaa6419a0fecb575def8e84fecf51a1e5a48098c7d81a3

   `Cisco_Meeting_Server_2_7_1.ova`

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

   For vSphere6, hash (SHA-512) for Cisco_Meeting_Server_2_7_vSphere-6_0.ova file:
   939133faf0397ed5d56ebf5193674413dc9d1b9e37b6ba103daf8b6e7093f8226165b0705efde65a5d0a9ed6d764479ea89a79445134dc9b885c41e4e5fec06c

   For vSphere6.5 and higher, hash (SHA-512) for Cisco_Meeting_Server_2_7_vSphere-6_5.ova file:

2dd07380a3eca5bd5f56e7b96aa82599f678f907c3c92521413c932c3be0df0218d1c79843b4bb3fdc969dbe82e8d2b16e0fe112382aba3df8bbf0f42ff1f50c

2. To validate the OVA file, the checksum for the 2.7.1 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.
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 2.7 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 `2.7.1`.
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.

Issues seen in previous versions that are fixed in 2.7.1

Cisco identifier	Summary
CSCvr86934	In some scenarios, if the recording is started before a peer link call, that recording may intermittently stop after peer link is received from the remote Call Bridge.
CSCvs12175	Calls to Skype For Business may fail when the FQDN for a specific Meeting Server Call Bridge is not specified in contact header when answering INVITE for invitation to AVMCU meeting.
CSCvr80166	Auto recording fails to start in a meeting scheduled by TMS where TMS makes end-points dial into different Call Bridges to join the same meeting.

Cisco identifier	Summary
CSCvs03934	Cisco Meeting Server running version 2.7 or below may unexpectedly restart when an unexpected Microsoft RDP sharing capability is received.
CSCvs08721	Skype participants video is not seen on SIP side of call when speaking.
CSCvr58520	Dual home calls and presentation calls may fail when Call Bridge answers the call sending the incorrect contact header in "200 Ok" response to Skype/Lync environment.
CSCvr71743	When participantLimit is set in tenant level, a streaming or recording session is counted as a participant. This reduces the number of actual participants who can join meetings.
CSCvq88442	In a clustered environment, when applying rxVideoMute=true to "/calls/<call id>/participants/*" the video in all peer nodes is frozen.
CSCvq84608	A splash screen momentarily displays (< 1 second) on the upper left video pane when a participant joins a conference. This occurs so quickly that the newly joined participant may not notice it.
CSCvq64378	On Cisco Meeting Server the Call Bridge up time is being reset silently. This doesn't affect normal operations.
CSCvq81546	Significant packet loss and jitter reported by multiple endpoints on Meeting Server 2000.
CSCvo80460	Occasionally a SIP call is dropped by the far end due to an INVITE timeout.
CSCvo91844	Degraded audio may occur on a fully loaded Meeting Server with many audio participants.
CSCvq45298	On a webRTC/Meeting App point-to-point call where each of the calls is hosted on a separate Call Bridge, the peer link that connects them intermittently terminates resulting in call disconnection.
CSCvq93115	A Skype for Business client is not able to unmute their endpoint for the first time when the endpoint joins a default-muted AVMCU meeting via Meeting Server. It works from the second unmute and thereafter.
CSCvk65529	On rare occasions Cisco Meeting Server may unexpectedly restart with the following message: sf_assert failed server/media/startup/server_media_xccp_handler.cpp:767
CSCvr13451	The Streamer disconnects and reconnects under packet loss conditions.

Issues seen in previous versions that are fixed in Cisco Meeting Server 2.7 software.

Cisco identifier	Summary
CSCvo41211	In a Skype for Business gateway call consisting of multiple clients and SIP endpoints, when a Skype for Business client shares the content, it is seen on some SIP endpoint but not on others.

Cisco identifier	Summary
CSCvq19622	This issue has been filed to evaluate the product against the vulnerability released by the Netflix on June 17th affecting FreeBSD and Linux kernels, identified by CVE IDs: - CVE-2019-11477: SACK Panic - CVE-2019-11478: SACK Slowness or Excess Resource Usage - CVE-2019-11479: Excess Resource Consumption Due to Low MSS Values Cisco has reviewed this product and concluded that it is affected by this vulnerability as it contains a vulnerable version of Linux Kernel.
CSCvp43740	DTMF from three screen systems may not be recognized correctly by the Meeting Server. These systems may be unable to navigate a CMS IVR or enter a passcode for a meeting.

4.2 Open issues

Note: Refer to the Cisco Meeting App WebRTC Important information guide for information on open issues affecting the WebRTC 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
CSCvu14250	Distortion and video corruption can be seen on SIP calls where just the branding background image is displayed and that image has not been subsampled at 4:2:0 or 4:2:2 format. To workaround this issue: • Subsample the background image at 4:2:0 or 4:2:2 or • Use the default Cisco branding image
CSCvp34817	In a Cisco Expressway deployment, a participant's display name is not retained when moving a participant between meetings, this affects the display name returned in the Web Admin interface, API, CDR records etc. In addition, when the participant's call leg is load balanced across Meeting Server, the participant's display name will not display correctly in apps (for example Cisco Meeting Management) that use CDRs to determine the participant's display name.
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.

Cisco identifier	Summary
CSCvm48344	If the Recorder suddenly stops recording, a temporary recording file is created which is not suitable for playback. Currently there is no tool available to convert .temp file to .mp4 playback.
CSCvj49594	ActiveControl does not work after a hold/resume when a call traverses Cisco Unified Communications Manager and Cisco Expressway.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.
CSCvh23036	DTLS1.2, which is the default DTLS setting for Meeting Server 2.4, is not supported by Cisco endpoints running CE 9.1.x. ActiveControl will only be established between Meeting Server 2.4 and the endpoints, if DTLS is changed to 1.1 using the MMP command `tls-min-dtls-version 1.0`.
CSCvh23028	Changing the interface that the Web Bridge listens on or receiving a DHCP lease expire, will cause the Web Bridge to restart. WebRTC App users may have to log in again.
CSCvg62497	If the NFS is set or becomes Read Only, then the Uploader component will continuously upload the same video recording to Vbrick. This is a result of the Uploader being unable to mark the file as upload complete. To avoid this, ensure that the NFS has read/write access.
CSCve64225	Cisco UCS Manager for Cisco Meeting Server 2000 should be updated to 3.1(3a) to fix OpenSSL CVE issues.
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

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

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

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

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

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

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

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

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

Cisco Trademark