Cisco Meeting Server

Cisco Meeting Server Release 3.3.3

Release Notes

04 August 2022

Contents

What's changed 4

1 Introduction 5
1.1 Cisco Meeting Server web app Important Information 5
1.2 End of Software Maintenance 6

2 New features and changes in version 3.3 7
2.1 Email invitation API 7
2.1.1 API additions 8
2.2 Increased scale in the number of users 8
2.3 LDAP authentication for MMP users 9
2.3.1 MMP additions 10
2.4 Source IP address for admin actions 12
2.5 Absolute timeout for web server sessions 12
2.6 Verifying SSH fingerprints 13
2.6.1 MMP additions 13
2.7 Align web app and SIP layouts 13
2.8 Active speaker in pane placement 16
2.8.1 API additions 18
2.9 Change participant roles in a web app meeting 19
2.9.1 Available roles 19
2.9.2 Special roles 20
2.9.3 Assigning roles and coSpace membership 21
2.9.4 API additions 21
2.10 Scheduling meetings from web app (Beta support) 22
2.10.1 Web scheduler deployment overview 24
2.10.2 Scheduler in the web app UI 25
2.10.3 Deploying the scheduler 25
2.10.4 Configuring the Email server 28
2.10.5 Scheduler detailed logging 33
2.10.6 API additions 34
2.10.7 MMP additions 45
2.11 Summary of 3.3 API additions and changes 48
2.11.1 API additions 48
2.11.2 New and modified parameters 50
2.11.3 Enabling / disabling active speaker in pane placement 51

2.11.4 Retrieving Email invitation text 51
2.11.5 Changing the role of participant in a web app meeting 52
2.12 Summary of MMP additions and changes 53
2.12.1 LDAP authentication 53
2.12.2 SSH fingerprints verification 55
2.12.3 Scheduler configuration 56
2.13 Summary of CDR Changes 57
2.14 Summary of Event Changes 57

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 3.3.3 58
3.1 Upgrading to Release 3.3.3 58
3.2 Downgrading 60
3.3 Cisco Meeting Server Deployments 61

4 Bug search tool, resolved and open issues 63
4.1 Resolved issues 63
4.2 Open issues 65
4.2.1 Known limitations 66

5 Related user documentation 67

6 Accessibility Notice 68

Cisco Legal Information 69

Cisco Trademark 70

What's changed

Version	Change
August 4, 2022	Maintenance release 3.3.3. See resolved issues.
March 14, 2022	Maintenance release 3.3.2. See resolved issues.
December 22, 2021	Maintenance release 3.3.1. See resolved issues.
August 24, 2021	First release for version 3.3.

1 Introduction

These release notes describe the new features, improvements and changes in version 3.3 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 pre-configured with VMware and the Cisco Meeting Server installed as a VM deployment.
- 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.

Note: Cisco Meeting Management handles the product registration and interaction with your Smart Account for Smart Licensing support. Meeting Management 3.3 is required with Meeting Server 3.3.

- **Upgrade**: The recommended work flow is to first upgrade Meeting Management, complete Smart Licensing, and then upgrade Meeting Server.
- **Smart Licensing**: For Meeting Server 3.3 it is recommended to use Smart Licensing via Meeting Management. However, license files hosted locally on Meeting Server are still supported via Meeting Management for existing versions. As Meeting Server and Meeting Management intend to remove support for locally hosted licenses in future releases, you are advised to plan migration to Smart Licensing.

For more information on Smart Licensing and upgrading Meeting Management, see Meeting Management Release Notes .

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 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 Cisco Meeting Server web app Important Information

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 for details on when features are released

and issues resolved for the web app. These details are not included in the Meeting Server release notes.

The Important Information guide describes the following:

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

1.2 End of Software Maintenance

Table 1: 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 3.1.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.1.x is December 24, 2021.
Cisco Meeting Server version 3.2.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.2.x is April 17, 2022.

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

2 New features and changes in version 3.3

Version 3.3 of the Meeting Server software introduces the following new features and changes:

- Email invitation API for retrieving information for a coSpace
- Increased scale in the number of users
- LDAP authentication for MMP users
- Source IP address for admin actions
- Absolute timeout for web server sessions
- Verifying SSH fingerprints
- Align web app and SIP layouts
- Active speaker in pane placement
- Change participant roles in a web app
- Scheduling meetings from web app (Beta support)

2.1 Email invitation API

In version 3.2, the Email Invitation API feature was implemented in Meeting Server to retrieve text-based meeting information for a specific accessMethod. In version 3.3 this feature is extended for retrieving information for a coSpace. Conference join information can be retrieved from the coSpace using the following API call:

GET on **`/api/v1/coSpaces/<coSpace id>/emailInvitation`**

As in the previous release, the template and generation of the Email invitation text is shared with the web app Custom Email Invites feature, with the exception:

- If using tenants, and a **`webBridgeProfile`** is set at the tenant level then the **`ivrNumbers`** and **`webBridgeAddresses`** settings at the tenant level will override settings at the system/profiles level.
- If the **`ivrNumbers`** or **`webBridgeAddresses`** in the tenant **`webBridgeProfile`** are not specified, then the system level **`ivrNumbers`** and **`webBridgeAddresses`** addresses will be inherited.
- If no **`webBridgeProfile`** is configured at any level then no IVR numbers or Web Bridge addresses will be present in the invitation text.

The email invitations can be generated in different languages. For more information, see the **Invitation text customization** section in Cisco Meeting Server Customization Guidelines.

2.1.1 API additions

The following method retrieves the coSpace level meeting join information:

- GET on **`/api/v1/coSpaces/<coSpace id>/emailInvitation`**

URI Parameters	Type/Value	Description / Notes
language (optional)	String	In the form of a language tag "xx" or "xx_XX" (xx language code and XX region code) or any other string between 1 and 32 characters (allowed characters: 'a'-'z', 'A'-'Z', '0'-'9', and '_').

Response Elements	Type/ Value	Description / Notes
subject	String	Subject of the invitation.
invitation	String	Email invitation text.
language	String	Language tag of email invitation. If no language is specified, then it defaults to en_US. If the specified language is invalid, then a "400 - Bad Request" response is returned.

2.1.1.1 Failure responses

Response Elements	Type/ Value	Description / Notes
`invalidValue`	400 - Bad Request	You entered an empty string or an invalid character as a language parameter.
`valueTooLong`	400 - Bad Request	You entered a long language parameter.
`retryAfter`	503 - Service Unavailable	You tried to retrieve the text based meeting entry information when the server was busy or was fetching externally hosted template. Retry later or retry after recommended **`retryAfter`** period in seconds.

2.2 Increased scale in the number of users

From version 3.3, a Cisco Meeting Server cluster can support up to 300,000 users depending on the servers where the databases are located. All databases in the cluster must be on the same specification server.

Cisco Meeting Server	Maximum number of users
Meeting Server 2000 M5v2	300,000
Meeting Server 2000 M5v1	200,000
Meeting Server 2000 M4, Meeting Server 1000 M4, M5v1, M5v2, and Specification based servers	75,000

Note: LDAP sync for a large number of users can cause an increase in call join times. We advise adding new users/coSpaces onto the Meeting Server during a maintenance window or during off peak hours.

2.3 LDAP authentication for MMP users

Version 3.3 supports LDAP authentication for administrators as well as web app users in all Meeting Server deployments. LDAP user accounts can now log in to Web Admin Interface, SSH, SFTP, and serial console with LDAP based authentication. If authentication fails, user login is rejected.

Note: For Common access card (CAC) deployments, CAC authentication takes precedence over both, LDAP authentication and local authentication.

This feature does not support importing MMP users via LDAP, or turning existing local users to LDAP authenticated users. The administrator must pre-configure LDAP users by manually adding each user with the MMP command **`user add`**. Login names must be unique across local and LDAP users.

To enable adding LDAP users, a new option, **`[ldap]`** is added to the command:

```
user add <username> (admin|crypto|audit|appadmin|api) [ldap]
```

Note: Meeting Server API does not support access to users with LDAP authentication.

For all users added with the **`ldap`** option, authentication is done only by the LDAP server, and no local password look up is done. In case of local users, authentication is done with a local password lookup only. LDAP authentication does not support password changes.

Note: In case the LDAP server becomes unavailable or Meeting Server is unable to reach the LDAP server, then LDAP users will be unable to log in. As a backup, it is a good practice to always keep at least one local admin user configured on the MMP.

Meeting Server supports configuration of a Microsoft AD LDAP server or an Open LDAP server, with either one of hostname/IPv4/IPV6, along with port, using the new **`ldap`** option. This LDAP

server can be the same as the one used for web app user authentication provided it is a supported server type, but still has to be configured for Meeting Server separately.

2.3.1 MMP additions

The new **ldap** option is added to **user add** MMP command enables configuring details of an LDAP server, directory search parameters, TLS settings, and enabling or disabling LDAP authentication.

To enable adding LDAP users, a new option, [**ldap**] is added to the command:

```
user add <username> (admin|crypto|audit|appadmin|api) [ldap]
```

Note: Meeting Server API does not support access to users with LDAP authentication.

The output of the **help ldap** command is:

```
cms> help ldap
Configure LDAP client for MMP users
Usage:
    ldap
    ldap server <hostname|address> <port>
    ldap protocol (ldap|ldaps)
    ldap binddn <username>
    ldap basedn <base DN>
    ldap login_attr <attribute>
    ldap filter <filter>
    ldap remove <binddn|filter|trust>
    ldap trust <crt bundle>
    ldap verify (enable|disable)
    ldap min-tls-version <minimum version string>
    ldap enable
    ldap disable
    ldap status
```

Note:
The **user list** MMP command is extended to include logged in LDAP users.
The only **user rule** parameters that apply to LDAP users are max_failed_logins, max_idle, and max_sessions. Other parameters of this command do not apply to LDAP users.
The **user expire** MMP command is not supported for LDAP users.

Command/Examples	Description/ Notes
`ldap`	Displays information about the ldap configuration.
`ldap server <hostname|address> <port>`	Specifies the LDAP server with hostname or IP address, and port number. This is mandatory.
`ldap protocol (ldap|ldaps)`	Specifies the ldap protocol to use. To use a secure connection to the LDAP server, ldaps must be used. It is mandatory to specify the protocol.

`ldap binddn <username>`
`ldap binddn cn=binduser,oi=user,dc=domain,dc=com`
`ldap binddn "cn=bind user,o=My Company,dc=domain,dc=com"`
`ldap binddn domain\\username`
	Adds the distinguished name with which to bind to the directory server for lookups.The binddn parameter is optional. If not specified, anonymous bind requests are used.
	The bind user must have search permission in the directory. This command prompts for an optional bind password.
	If spaces are included in the argument, then the argument has to be quoted. If backslashes are included, they must be escaped with a preceding backslash.

`ldap basedn <base DN>`	Specifies the base distinguished name to use as search base. It is mandatory to specify basedn. If spaces are included in the argument, then the argument has to be quoted. If backslashes are included, they must be escaped with a preceding backslash.
`ldap login_attr <attribute>`	Specifies the LDAP attribute name such as uid, userPrincipalName, or sAMAccountName, which uniquely identifies users. The attribute value must match the pre-configured MMP user name for successful login. Specifying an attribute is mandatory.
`ldap filter <filter>` `ldap filter (&(objectClass=*) (memberOf=CN=admins,DC=example,DC=com))`	Sets up an LDAP search filter. Specifying a filter is optional. If no filter is specified, the default value (objectClass=*) is used. A valid LDAP filter syntax must be used and it must be enclosed in parentheses.
`ldap remove (binddn|filter|trust)`	Removes binddn, filter, or trust parameters that have been set up earlier.

Command/Examples	Description/ Notes
`ldap trust <crt bundle>`	Configures the system to use a particular bundle of certificates to validate the certificate. To use a secure connection to the LDAP server, this must be configured with a trusted CA.
`ldap verify (enable|disable)`	Enables or disables certificate verification for connection to the LDAP server. To use a secure connection to the LDAP server, certificate validation must be enabled. When disabled, Meeting Server does not request or check the trust certificates.
`ldap min-tls-version <minimum version string>`	Configures the minimum TLS version that the system will use. Possible values are 1.0, 1.1, and 1.2. The default is version 1.2.
`ldap enable`	Enables the LDAP service.
`ldap disable`	Disables the LDAP service.
`ldap status`	Displays the status of the ldap service as: running - indicates that the service is running not running - the service is enabled but not running. Check the logs for more information. disabled - the service is disabled

2.4 Source IP address for admin actions

In version 3.3, Meeting Server logs include the source IP address and SSH port in individual line commands for admin actions. These actions include logging in, logging out, and entering commands. This can be useful in identifying the source of events, especially in concurrent sessions.

2.5 Absolute timeout for web server sessions

Web sessions in Meeting Server have an absolute timeout at 24 hours from version 3.3. Sessions that continue to be active after 24 hours will be timed out, and the user will need to log in again.

Note: The idle timeout for web sessions continues to be 10 minutes and that for SSH at three minutes.

2.6 Verifying SSH fingerprints

From version 3.3, a system administrator can retrieve fingerprints of the keys installed on the Meeting Server. While connecting to the Meeting Server for the first time via SSH or SFTP, the administrator can then verify the keys prompted by the Meeting Server against the retrieved keys. This feature is enabled by a new command, **`ssh server_key list`**.

2.6.1 MMP additions

The new MMP command is added, to display a list of keys installed in the Meeting Server.

`ssh server_key list`

The output displays a list of keys along with the size, type, and fingerprints for all existing keys in the Meeting Server host, among the following keys:

- ssh_host_dsa_key.pub
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key.pub
- ssh_host_key.pub
- ssh_host_rsa_key.pub

2.7 Align web app and SIP layouts

In version 3.3, Meeting Server supports configuring dynamic, fixed, and customized layouts and pane placement of participants in web app. Meeting Server can also control permissions for web app users to change the layout.

The web app supports adaptive layouts that change based on how many people are in the meeting and the size and aspect ratio of the web app window. For example, if it is displaying 4 participant it could display one row of four, two rows of two or one column of four depending on the size and aspect ratio of the window. For most meetings, this allows the end user to decide what they want to see and is the best end user experience. However, for scenarios where a more fixed experience is required, version 3.3 now allows administrators to force the web app to have the same fixed 16:9 aspect ratio layout as a SIP endpoint. For example, if you wanted to use pane placement and ensure that everyone saw a 3 x 3 equal layout showing the same participants, this can now be achieved with participants joining via web app. In previous versions, this was only supported for SIP endpoints.

The web app and SIP endpoint users can change the layout based on the permissions assigned to them through the **`changeLayoutAllowed`** parameter on **`callLegs`**.

If a dynamic layout is chosen (i.e. one that grows as more people join like allEqual or onePlusN), then the web app will continue to use its adaptive layout described as it has in previous releases. If a static layout is chosen (i.e. one that does not change as more people join like allEqualQuarters or onePlusFive), then the web app will display that layout in a 16:9 aspect

ratio. If a user re-sizes the web app window, the layout will stay as 16:9 and shrink or grow depending on the size of the window.

See Cisco Meeting Server Administrator's Quick Reference Guide for Screen Layouts, Pane Placement, and Customizable Layouts for information on customizing layouts and assigning layouts and pane placement.

Mapping Meeting Server layouts to available web app layouts

The layout selected in Meeting Server determines the layout that will be displayed on the web app, and the layout icon that is highlighted in web app. Each Meeting Server layout family is mapped to most suitable web app layout as shown in the table below.

Layout assigned in Meeting Server	Layout displayed / Icon highlighted in web app
speakerOnly	Speaker Only
allEqual	All Equal
allEqualQuarters	
allEqualNinths	
allEqualSixteenths	
allEqualTwentyFifths	
stacked	Speaker Large
telepresence	
onePlusFive	
onePlusSeven	
onePlusNine	
onePlusN	
automatic + no layout template is configured	Speaker Large
automatic + layout template is configured	Custom
Layout other than 'automatic' assigned + layout template is configured	Corresponding web app icon is highlighted and layout is displayed + Custom layout icon is also available for the user to select. If user selects Custom layout, the layout configured in the template is displayed.

Note: The exception to this feature is when Meeting Server API or Meeting Management configure a dynamic layout which changes as more participants join. In this case, web app chooses its own layout - either All Equal or Speaker Large - which might result in a minor difference in layout between web app and SIP endpoints.

For any layout assigned by Meeting Server (other than what appears in web app as Custom layout), if a user switches to a different layout and then comes back to the assigned layout, the layout changes to web app's adaptive layout. For example, if allEqualNinths is assigned in Meeting Server, the web app initially displays All Equal with nine panes. If the user changes the layout to a different layout and then comes back to All Equal, the layout will not be a static allEqualNinths, but web app's own All Equal adaptive layout.

Permissions to change layout

If admins want all participants to see the same layout, they can use pane placement or a static layout, and SIP and web app participants will see the same layout. It is important for the admins to disallow participants to change layouts if they want to keep this layout throughout the meeting. Meeting Server can now set permissions for web app users to change layout using the **`changeLayoutAllowed`** parameter on **`callLegs`**. If this is set to false, the web app users can only choose between two layouts: Audio Only and the configured layout; all other layouts are disabled.

APIs used

This feature uses existing APIs and parameters. See the Cisco Meeting Server API Reference Guide for more information.

- POST to **`/coSpaces`**
- PUT to **`/coSpaces/<coSpace id>`**
- POST to **`/calls/<call id>/participants`**
- POST to **`/calls/<call id>/callLegs`**
- PUT to **`/callLegs/<callLeg id>`**
- POST to **`/callLegProfiles`**
- PUT to **`/callLegProfiles/<call leg profile id>`**

The effective value of **`defaultLayout`** (as calculated based on the hierarchy of call leg profiles) determines the layout at the start of the call. This parameter can be set on the following API objects:

The **`chosenLayout`** parameter can be used to change the layout during the call and is supported on the following API nodes:

- POST to **`/calls/<call id>/callLegs`**
- PUT to **`/callLegs/<callLeg id>`**
- GET on **`/callLegs/<callLeg id>`**

The **`layout`** parameter is supported on GET on **`/callLegs/<callLeg id>`** to retrieve the layout selected in web app or the SIP endpoint.

Note: The **defaultLayout** setting for **/callLegProfiles** will be inherited if **defaultLayout** is left blank for **/coSpaces**, **/calls**, **/callLegs**. If both **defaultLayout** and **layout** are set then **defaultLayout** takes precedence.

Pane placement is enabled by the existing parameters, **panePlacementHighestImportance** and **panePlacementSelfPaneMode** supported on the following methods:

- POST to **/coSpaces**
- PUT to **/coSpaces/<coSpace id>**
- POST to **/calls**
- PUT to **/calls/<call id>**

The **changeLayoutAllowed** parameter is supported on the following API methods to assign the permissions to change the layout in web app and SIP endpoints:

- POST to **/callLegProfiles**
- PUT to **/callLegProfiles/<call leg profile id>**
- POST to **/calls/<call ID>/callLegs**
- PUT to **/callLegs/<callLeg id>**
- POST to **/calls/<call id>/participants**

For details on using the API see the Cisco Meeting Server API Reference Guide.

2.8 Active speaker in pane placement

Version 3.3 supports active speaker in pane placement for SIP endpoints and web app. This feature can be configured on single, dual, and three screen endpoints.

When this feature is enabled, the first pane of the layout is reserved for the active speaker. Since the active speaker is displayed in the first pane, other participants who have been assigned a specific pane using pane placement are moved to the next pane. For example, a participant assigned to the n^{th} pane is displayed in the $(n+1)^{th}$ pane. The active speaker is displayed in the first pane in addition to the pane assigned with pane placement.

The feature can be configured using the new API parameter **panePlacementActiveSpeakerMode** on the **coSpace** and **calls** level. This parameter takes the values none, allowself, and suppressself.

Note: This feature requires pane placement to be enabled and impacts the pane assignment behavior.

Let's take the example of the following pane placement assignment for the participants:

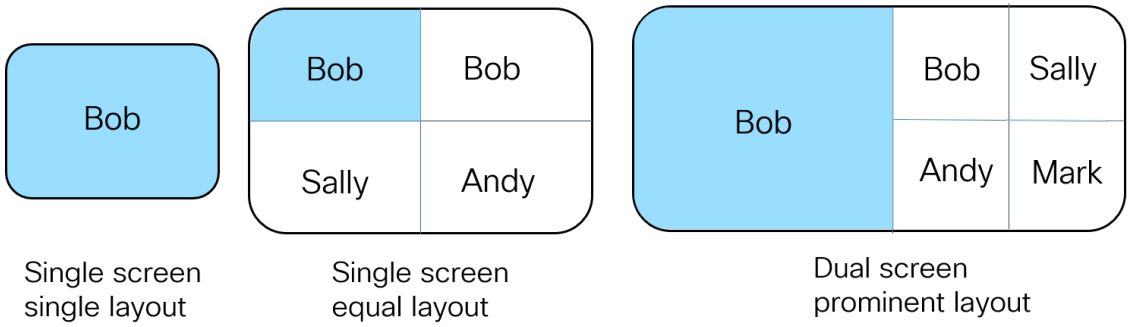
Participant	Pane
Bob	1
Sally	2
Andy	3
Mark	4

Note: In all layouts, the first pane is reserved for the active speaker or the previous speaker depending on the **`panePlacementActiveSpeakerMode`** parameter setting.

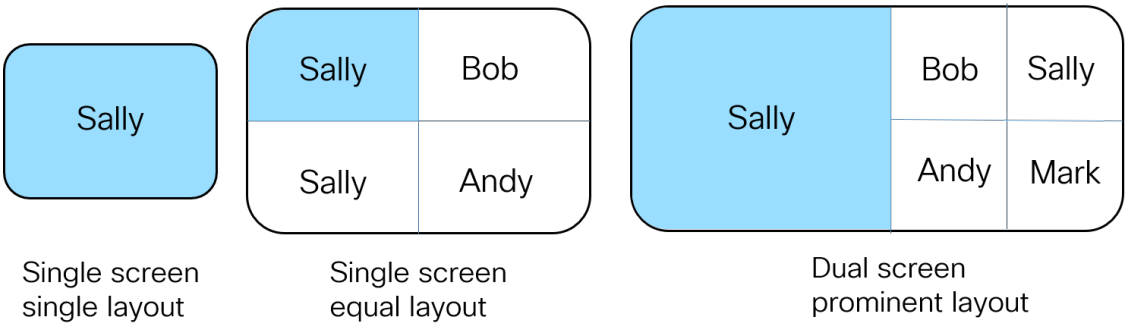
allowself setting

In this setting, the first pane is reserved for the active speaker and the same view is displayed to all the participants including the active speaker.

When **`panePlacementActiveSpeakerMode`** is set to allowself and Bob is the active speaker, this is the view for all the participants:



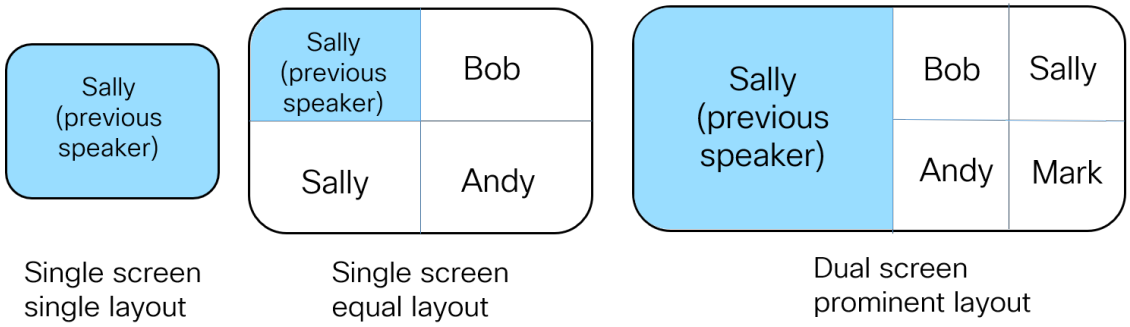
If Sally is the active speaker, this is the view for all participants:



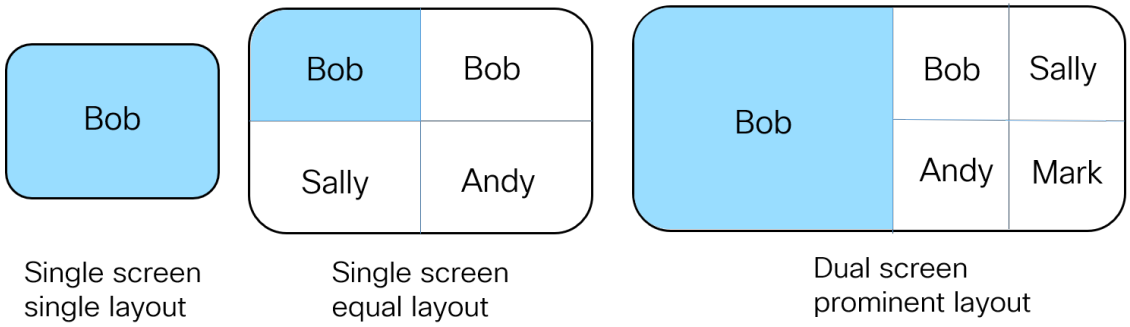
suppressself setting

With this option, the active speaker's view is different from the view of the other participants. In the other participants' view, the active speaker is seen in the first pane. In the active speaker's view, the previous speaker is seen in the first pane.

When the parameter **panePlacementActiveSpeakerMode** is set to suppressself and Bob is the speaker, this is Bob's view:



When the parameter **panePlacementActiveSpeakerMode** is set to suppressself and Bob is the speaker, this is the view for all other participants:



When active speaker is enabled for main video and presentation in a single screen video endpoint, active speaker pane is always the first in the row. In this case, the active speaker will only be shown twice if they are placed in one of the first five panes.

2.8.1 API additions

The new **panePlacementActiveSpeakerMode** API parameter can be configured to enable active speaker in pane placement. This parameter is supported by the following methods:

- POST to **/coSpaces**
- PUT to **/coSpaces/<coSpace id>**
- GET on **/coSpaces/<coSpace id>**
- POST to **/calls**
- PUT to **/calls/<call id>**
- GET on **/calls/<call id>**

The parameter setting at the calls level takes precedence over the setting at coSpace level. If unset at both levels, active speaker is disabled.

Parameter	Type/Value	Description/ Notes
panePlacementActiveSpeakerMode	allowself | suppressself | none	• allowself - displays the participant in the first pane if they are the active speaker, additional to displaying the participant in the pane set by pane placement. The same view is displayed for all participants. • suppressself - displays the active speaker in the first pane for all other participants other than the active speaker. For the active speaker, the previous speaker is displayed in the first pane. • none - the feature is disabled.

2.9 Change participant roles in a web app meeting

Meeting Server does not have pre-configured roles for the meeting participants. Admins define the role names and their associated permissions while provisioning Meeting Server using Meeting Management (see Meeting Management User Guide for Administrators for more information). Users will be assigned these roles based on the access method they use to join the meeting. Version 3.3 allows meeting participants connected via the Cisco Meeting server web app to change the role of other participants. This feature is also supported via the Web Admin API for coSpace calls.

Note: In this release, this feature is supported for participants joining from web app and SIP/CE endpoints or clients only. Changing the role for participants who have joined from other clients like Lync or Skype is not supported.

Note: Cisco Endpoints with ActiveControl enabled will not change their video or video+presentation permissions with a mid call role change. This could be changing video or video+presentation from disabled to enabled or vice-versa. For example, a participant joined as a Guest where video permission is disabled. During the call, if their role is changed to Host where video permission is enabled, video still remains disabled on the endpoint.

The new **`changeRoleAllowed`** parameter supported on callLegProfiles, callLegs, and participants determines whether a participant is allowed to change the role of other participants in-call. The effective value of **`changeRoleAllowed`** is computed based on the existing rules for the hierarchy of call leg profiles and, if undefined at all levels of the hierarchy, it defaults to false.

2.9.1 Available roles

In the web app

The initiator (who changes the role of a participant) has certain roles available to assign based on their:

- Access method Scope
- coSpace membership / ownership
- Initial role of the initiator participant
- Current role of the target participant (whose role is being changed)

The initiator participant has access to:

- all access methods of the coSpace regardless of their scope, if the initiator participant is the owner of the coSpace.
- all public and directory access methods of the coSpace.
- access methods with member scope only if they are the coSpace owner or they are a member of the coSpace.
- access methods with private scope if they are the coSpace owner or if they joined using that particular access method as a coSpace member.

If the initiator participant has access to an access method, they can assign it to another participant provided that they are able to revert the role back to what it was. The exception to this rule is the role “Space default”: the initiator can not assign a “Space default” role to a participant who has another role. Refer to Space default role for more information on "Space default" role.

From the Web Admin

An Admin user can change the access method of a participant or a call leg object by specifying a value for accessMethod when doing PUT on /callLegs/<call leg id>. The Admin user has access to all access methods configured on the coSpace and in addition can unset the access method, i.e. provide a value “”, which also removes the access methods’s call leg profile from the call leg profile hierarchy of the object and unsets the access method’s importance value.

2.9.2 Special roles

The role of a participant is displayed as "Space default" or "Custom" in the following scenarios:

2.9.2.1 Space default role

If meetings are provisioned by Meeting Management admin (using the procedure provided in the Meeting Management User Guide for Administrators) then all users or access methods will be assigned a named role. If the spaces were created using older methods then it is possible that the role will be shown as "Space default".

- If the coSpace has a callId/uri on the coSpace object, a virtual access method "Role 1" is created on the web app space portal. When coSpace members join a call using this role, the in-call role is shown as "Space default".
- In the absence of this virtual access method, if a coSpace member has an In-call role assigned as "Space default" from the web app space portal, the in-call role is shown as "Space default".
- During a call, the Change Role menu does not display "Space default" as one of the options. If a participant's role is changed from "Space default" to any other role, their role can not be changed back to "Space default".

2.9.2.2 Custom role

If the callLegprofile set for a coSpaceUser does not match the call leg profile of any of the access methods or the coSpace object, the role will be shown as "Custom" in-call on web app. This role cannot be changed in web app.

2.9.3 Assigning roles and coSpace membership

2.9.3.1 Members

A role by any name such as Host or Guest corresponds to the assigned settings or permissions. For coSpace members, the role is changed by changing the coSpace user call leg profile. Since the access method is not changed, the result of a role change will not be reflected in GET on /callLegs/<call leg id> and on /participants/<participant id>. The importance value is also not affected.

2.9.3.2 Other participants

For non-coSpace members, the role is changed by changing the accessMethod. The value of the parameter accessMethod when doing GET on /callLegs/<call leg id> and on /participants/<participant id> reflects the change. In addition, the access method's call leg profile is plugged in the call leg profile hierarchy and the access method's importance value is applied to the participant as well.

2.9.4 API additions

The new **`changeRoleAllowed`** parameter is introduced in 3.3 to enable participants to change the role of other participants in web app. The parameter is supported in the following API methods:

- POST to **`/callLegProfiles`**
- PUT to **`/callLegProfiles/<call leg profile id>`**
- GET on **`/callLegProfiles/<call leg profile id>`**
- PUT to **`/callLegs/<call leg id>`**

- GET on **/callLegs/<call leg id>**
- POST to **/calls/<call id>/callLegs**
- POST to **/calls/<call id>/participants**

Request parameters	Type/Value	Description/ Notes
changeRoleAllowed	**true**, **false**, or <**unset**>	Determines whether or not the participant can change the role of another participant in a call when using the web app. The usual rules for the hierarchy of call leg profiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to false.

Modifying a participant's role is enabled by the **accessMethod** parameter on the following operation:

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

Request parameters	Type/ Value	Description/ Notes
accessMethod	GUID | ""	Access method GUID.

2.10 Scheduling meetings from web app (Beta support)

Version 3.3 introduces the ability to schedule meetings and see upcoming meetings in web app. Web app users can schedule meetings, modify the scheduled meetings, and notify participants via email. Scheduler is a new component that enables scheduling meetings, and is enabled by the new **scheduler** MMP commands. Scheduler component is included in the base multiparty licensing (PMP Plus and SMP Plus), and does not require a separate feature license.

The Scheduler component is supported on Meeting Server 1000 and Meeting Server on VM deployments. For Meeting Server on specification-based VM platforms, an additional 4 GB of RAM is required for running the scheduler component. There is no additional RAM requirement for Meeting Server 1000.

In this release, IPv6 is not supported on the Scheduler.

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

Note: The scheduler component is not supported on Meeting Server 2000. Call Bridges running on the Meeting Server 2000 are supported in the deployment, but the Scheduler component must run on Meeting Server 1000 or a Meeting Server on VM.

The Scheduler supports meetings with single and recurring instances. If the meeting template has different roles (such as host and guest), then participants can be assigned to these roles. Web app users can schedule meetings in a persistent space or in a temporary space that is created for the purpose of the meeting. The temporary spaces that are created at the time of scheduling the meeting are deleted by the scheduler component 24 hours after the end of the scheduled meeting, whilst taking meeting recurrences into account. A meeting participant or space member can dial in to this space at any time during the lifetime of the space, even if it is outside the hours of the scheduled meeting. Meeting Server supports multiple meeting series per space.

Email notifications are sent to the participants when a meeting is scheduled or canceled, or the list of participants is modified. If a scheduled meeting is updated, then the updated invitation is sent only to the invitees included by the Scheduler.

Note: Emails are sent using the From address of the meeting organizer, which does not require any configuration. Authentication with the SMTP server requires an email address to be configured using the MMP command **`scheduler email username <smtp user-name>`**. This account configured on the MMP must have appropriate permissions to be able to send emails on behalf of web app users.

Meeting invitation emails consist of the following:

- Conference join information, which is retrieved by the scheduler using an API call to the Call Bridge. This information is present in the body of the email.
- Meeting details in an industry standard iCalendar (.ics) file attached to the email. The ICS file can be saved by participants to their calendar.

For information on how to customize the email invitation text, see Cisco Meeting Server Customization Guidelines.

Note: If there are changes to a coSpace that can impact the scheduled meetings in that space, and if these changes are made through the API, the scheduler may not be aware of these changes. In such cases, it is the API user's responsibility to refresh the email invitations via the Scheduler's refreshEmails API. See API additions.

Web app users can invite two types of participants to the scheduled meetings:

1. Web app participants: The scheduled meetings are visible to web app users when they are signed in to the web app. An email invitation will be sent, provided the user's email

address was successfully imported during the Call Bridge LDAP sync.

2. Email participants: An email address can be specified, for example, to invite someone who does not have a web app account. In this case an email invitation will be sent.

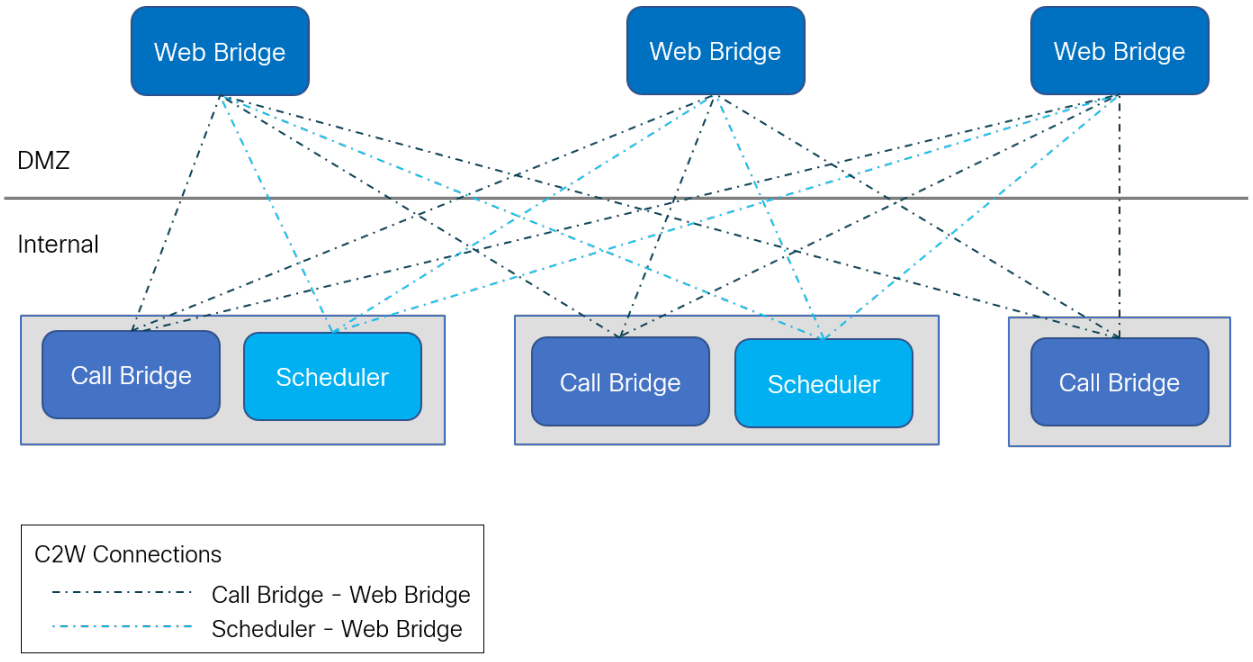
The scheduler does not support proposing new times and does not track acceptance or rejection of invitations. For more information on using the Scheduler through web app, see Cisco Meeting Server web app Important Information.

2.10.1 Web scheduler deployment overview

The scheduler is deployed as a new component using the Meeting Server MMP. When the scheduler is enabled, it makes API requests to the Call Bridge over the loopback interface. It is therefore a requirement that the scheduler is deployed on a Meeting Server which is also hosting a Call Bridge. It is not possible to configure the scheduler to use a remote Call Bridge.

The list of configured Web Bridges is retrieved by the scheduler using the Call Bridge APIs. Persistent C2W connections are established to each Web Bridge similar to how the Call Bridge also establishes a C2W connection to each Web Bridge. No explicit configuration is required to enable connection between the scheduler and Call Bridge, because this happens automatically over the loopback interface. Similarly, the C2W connections are all automatic but it is necessary to configure a trust bundle between the scheduler and Web Bridges.

Note: The scheduler will need to be able to establish a C2W connection to all Web Bridges in a cluster.



It is not necessary to deploy a scheduler alongside every Call Bridge. One scheduler supports 150,000 meetingsA scheduler on a Meeting Server 1000 and Meeting Server on VM

deployments supports 150, 000 meetings and a scheduler on Meeting server 2000 supports 200,000 meetings. Two or three schedulers can be added to provide resiliency but the capacity remains at 150K scheduled meetings. Scheduled meeting data is stored in the Meeting Server database and both clustered and single box database deployments are supported.

The Call Bridge may log API requests from the scheduler as user "scheduler". This is for logging purposes only and not a real account. There is no built in account and the scheduler user does not need to explicitly create an account. The scheduler uses the Call Bridge API over the loopback interface and is automatically a trusted source to issue API commands.

2.10.2 Scheduler in the web app UI

- The user interface for scheduling meetings will be displayed to web app users, provided at least one scheduler has established a connection to the Web Bridge. If no schedulers are enabled then the web app user will not see the user interface for scheduling meetings.
- When the administrator adds, removes, or changes Web Bridges via the Call Bridge /Web Bridges API, the scheduler does not automatically become aware of those changes. Therefore, the schedulers must be restarted. Similarly, when a scheduler is disabled, the Web Bridges are not aware that the scheduler is purposely disabled rather than just down for some unexpected reason. If the scheduler is intentionally disabled by the administrator, a restart of the Web Bridges is recommended so that the scheduling user interface is not displayed.
- When a scheduler is down due to being disabled or some other issue, the Web Bridge uses a different scheduler if available. Otherwise, an error is displayed to the web app users.

2.10.3 Deploying the scheduler

To enable connection between the scheduler and Call Bridge, no explicit configuration is needed. This happens automatically over the loopback interface. Similarly, the C2W connections are all automatic, but it is necessary for a trust bundle to be configured between the scheduler and Web Bridges.

1. Configure C2W Trust.

   C2W is a TLS-based WebSocket connection established from the scheduler to each Web Bridge. Each scheduler needs to be able to connect to each Web Bridge in a cluster. The scheduler requires configuration of a client certificate and key to be used for this connection. To do this, create a certificate and upload it to the Meeting Server via SFTP or use the **`pki`** MMP commands to create a certificate.

   Configure the scheduler to use the certificate:

```
scheduler c2w certs <key-file> <crt-fullchain-file>
```

For example:

```
scheduler c2w certs scheduler_c2w.key scheduler.cer
```

It is necessary for the scheduler to be able to trust each Web Bridge it connects to. Upload a trust bundle which contains each Web Bridge certificate, via SFTP.

Configure the scheduler using the command:

```
scheduler c2w trust webbridge_bundle.cer
```

It is also necessary for the Web Bridge to be able to trust the scheduler. So it is important to include the scheduler certificate in the bundle configured using the command:

```
webbridge3 c2w trust <crt-bundle>
```

All the necessary certs for both schedulers and Call Bridges should be included in the <crt-bundle>.

2. (Optional) Configure scheduler's HTTPS interface.

   The scheduler has its own HTTPS interface which if enabled, can be used to configure scheduler meetings using the scheduler APIs. The Web Bridge however, does not communicate with the scheduler using the management API. Though it is not mandatory to enable the HTTPS server, it is recommended that you do so because it provides some diagnostic and troubleshooting functionality.

   Configure the HTTPS server listen interface using the command:

   ```
   scheduler https listen <interface> <port>
   ```

   For example:

   ```
   scheduler https listen a 8443
   ```

   Configure a certificate key pair for the server using the command:

   ```
   scheduler https certs <key-file> <crt-fullchain-file>
   ```

   For example:

   ```
   scheduler https certs scheduler_https.key scheduler_https.cer
   ```

3. (Optional) Configure the email server.

   For more information about configuration of the email server and types of email configuration, see Installation Guide.

   The configuration of the server address and port, enabling email protocol, and configuring a username for authentication are specified via the following scheduler MMP commands:

   ```
   scheduler email server <hostname|address> <port>
   scheduler email server none
   scheduler email username <smtp username>
   ```

```
scheduler email protocol <smtp|smtps>
scheduler email auth <enable|disable>
scheduler email starttls <enable|disable>
```

Email will not be configured on a scheduler if no server address is configured on it. At least one email server must be configured for the scheduler to send email invites. Emails can be sent from any scheduler and not necessarily from the scheduler which was used to schedule the meeting. If an email server is down, then a different scheduler sends the email.

4. After configuring the email server, enable the scheduler using the command:

   ```
   scheduler enable
   ```

5. Check the configuration and status of the service using the command:

   ```
   scheduler status
   ```

   Sample output of a successful configuration:

```
cms> scheduler status
Status: enabled
Running
Database responsive at start
HTTPS configured
C2W configured
Email server configured

Scheduler application status:
{
    "status": "UP",
    "components": {
        "c2w": {
            "status": "UP",
            "details": {
                "guid": "dc06c10f-a220-42d8-b4eb-f9be3d07faf4",
                "webbridges": "webbridge1.mycompany.com:4443:CONNECTED,
webbridge1.mycompany.com:8443:CONNECTED,
webbridge3.mycompany.com:8443:CONNECTED"
            }
        },
        "db": {
            "status": "UP"
        },
        "mail": {
            "status": "UP",
            "details": {
                "location": "smtp.mycompany.com:25"
            }
        },
        "ping": {
            "status": "UP"
```

```
31          }
32      }
33  }
```

2.10.4 Configuring the Email server

Scheduler supports the following types of email configurations:

1. SMTP
2. SMTP with Authenticated Login (Auth Login)
3. SMTP and STARTTLS
4. SMTP with Auth Login and STARTTLS
5. SMTPS (end to end TLS Encryption for the entire SMTP transaction)
6. SMTPS with Auth Login

Note: Emails are sent using the From address of the meeting organizer, which does not require any configuration. Authentication with the SMTP server requires an email address to be configured using the MMP command **`scheduler email username <smtp user-name>`**. This account configured on the MMP must have appropriate permissions to be able to send emails on behalf of web app users.

If the email invites fail to deliver, the Scheduler retries to send them in regular intervals. The Scheduler email queue cleaner cleans up the queued failed emails after specific expiry time.

2.10.4.1 Scheduler Email configuration with SMTP

To enable the Scheduler to send email notifications via the SMTP, configure the email server to listen on a specified port for the SMTP protocol.

1. Disable the Scheduler component if it is currently running:

   `scheduler disable`

2. Configure the email server and port:

   `scheduler email server <hostname|address> <port>`

   For example,

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. Enable the Scheduler:

   `scheduler enable`

2.10.4.2 Scheduler SMTP with Auth Login configuration

To enable the Scheduler to send email notifications via the SMTP with Auth Login, configure the email server to listen on a specified port for the SMTP protocol, enable the SMTP server to support Auth Login, and configure a user account for authentication. This account configured on the MMP must have appropriate permissions to be able to send emails on behalf of web app users.

1. Disable the Scheduler component if it is currently running:

   ```
   scheduler disable
   ```

2. Configure the email server and port:

   ```
   scheduler email server <hostname|address> <port>
   ```

   For example,

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. Enable the Auth Login option:

   ```
   scheduler email auth enable
   ```

4. Set the username to be used for authentication:

   ```
   scheduler email username <username>
   ```

   Enter the password:

   ```
   scheduler email username test@test.com
   Please enter password:
   Please enter password again:
   ```

5. Enable the Scheduler:

   ```
   scheduler enable
   ```

2.10.4.3 Scheduler SMTP and STARTTLS configuration

To enable the Scheduler to send email notifications via the SMTP and STARTTLS, configure the email server to listen on a specified port for the SMTP protocol and enable STARTTLS.

To establish a TLS connection, the TLS handshake involves a certificate exchange between the email server and the Scheduler. By default, the Scheduler is set to trust all certificates and establishes a successful TLS connection by accepting any certificate coming from the email server. However, there is an additional option on the scheduler to configure a specific certificate. In this mode, the Scheduler accepts and trusts only the configured certificate.

1. Disable the Scheduler component if it is currently running:

   ```
   scheduler disable
   ```

2. Configure the email server and port:

   ```
   scheduler email server <hostname|address> <port>
   ```

For example,

```
scheduler email server exchange.example.com 25
scheduler email server 10.27.33.55 25
```

3. Enable the STARTTLS option:

   ```
   scheduler email starttls enable
   ```

4. To use a specific certificate, first import and upload the certificate to the Meeting Server VM via SFTP. Then, configure the certificate by running the command:

   ```
   scheduler email trust <cert or bundle name>
   ```

   The configured certificate must be a valid certificate. For example, the common name or SAN names must match the FQDN of the email server, the certificate must not have expired, and so on. Likewise, if the certificate is issued by a Certificate Authority or there are intermediate certificates in the chain, configure the Root CA certificate or alternatively a certificate bundle containing the root certificate, intermediate certificate 1, intermediate certificate 2 and onwards, in that order.

5. Enable the Scheduler component:

   ```
   scheduler enable
   ```

2.10.4.4 Scheduler SMTP with Auth Login via STARTTLS configuration

To enable the Scheduler to send email notifications via the SMTP using Auth Login and STARTTLS, configure the email server to listen on a specified port for the SMTP protocol. Additionally, enable the SMTP server to support Auth Login, configure a user account that will be used for authentication, and enable STARTTLS.

To establish a TLS connection, the TLS handshake involves a certificate exchange between the email server and the Scheduler. By default, the Scheduler is set to trust all certificates and establishes a successful TLS connection by accepting any certificate coming from the email server. However, there is an additional option on the scheduler to configure a specific certificate. In this mode, the Scheduler accepts and trusts only the configured certificate.

1. Disable the Scheduler component if it is currently running:

   ```
   scheduler disable
   ```

2. Configure the specified email server and port:

   ```
   scheduler email server <hostname|address> <port>
   ```

   For example,

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. Enable the Auth Login option:

   ```
   scheduler email auth enable
   ```

4. Set the username to be used for authentication:

scheduler email username <username>

Enter the password:

```
scheduler email username test@test.com
Please enter password:
Please enter password again:
```

5. Enable the STARTTLS option:

   scheduler email starttls enable

6. To use a specific certificate, first import and upload the certificate to the Meeting Server VM via SFTP. Then, configure the certificate by running the command:

   scheduler email trust <cert or bundle name>

   The configured certificate must be a valid certificate. For example, the common name or SAN names must match the FQDN of the email server, the certificate must not have expired, and so on. Likewise, if the certificate is issued by a Certificate Authority or there are intermediate certificates in the chain, configure the Root CA certificate or alternatively a certificate bundle containing the root certificate, intermediate certificate 1, intermediate certificate 2 and onwards, in that order.

7. Enable the Scheduler component:

   scheduler enable

2.10.4.5 Scheduler SMTPS configuration

To enable the Scheduler to send email notifications via the SMTPS, configure the email server to support end to end SMTP encryption on a specific port.

To establish a TLS connection, the TLS handshake involves a certificate exchange between the email server and the Scheduler. By default, the Scheduler is set to trust all certificates and establishes a successful TLS connection by accepting any certificate coming from the email server. However, there is an additional option on the scheduler to configure a specific certificate. In this mode, the Scheduler accepts and trusts only the configured certificate.

1. Disable the Scheduler component if it is currently running:

   scheduler disable

2. Configure the specified email server and port:

   scheduler email server <hostname|address> <port>

   For example,

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. Set the email protocol to SMTPS:

   scheduler email protcol smtps

4. To use a specific certificate, first import and upload the certificate to the Meeting Server VM via SFTP. Then, configure the certificate by running the command:

   scheduler email trust <cert or bundle name>

   The configured certificate must be a valid certificate. For example, the common name or SAN names must match the FQDN of the email server, the certificate must not have expired, and so on. Likewise, if the certificate is issued by a Certificate Authority or there are intermediate certificates in the chain, configure the Root CA certificate or alternatively a certificate bundle containing the root certificate, intermediate certificate 1, intermediate certificate 2 and onwards, in that order.

5. Enable the Scheduler component to complete the email configuration using SMTPS:

   scheduler enable

2.10.4.6 Scheduler SMTPS with Auth Login configuration

To enable the Scheduler to send email notifications via the SMTPS using Auth Login, configure the email server to support end to end SMTP encryption on a specific port. Additionally, enable the SMTPS server to support Auth Login and configure a user account that will be used for authentication.

To establish a TLS connection, the TLS handshake involves a certificate exchange between the email server and the Scheduler. By default, the Scheduler is set to trust all certificates and establishes a successful TLS connection by accepting any certificate coming from the email server. However, there is an additional option on the scheduler to configure a specific certificate. In this mode, the Scheduler accepts and trusts only the configured certificate.

1. Disable the Scheduler component if it is currently running:

   scheduler disable

2. Configure the specified email server and port:

   scheduler email server <hostname|address> <port>

   For example,

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. Enable the Auth Login option:

   scheduler email auth enable

4. Set the username of the user which will be used for authentication:

   scheduler email username <username>

   Enter the password:

   ```
   scheduler email username test@test.com
   Please enter password:
   ```

```
Please enter password again:
```

5. Set the email protocol to SMTPS:

   ```
   scheduler email protcol smtps
   ```

6. To use a specific certificate, first import and upload the certificate to the Meeting Server VM via SFTP. Then, configure the certificate by running the command:

   ```
   scheduler email trust <cert or bundle name>
   ```

   The configured certificate must be a valid certificate. For example, the common name or SAN names must match the FQDN of the email server, the certificate must not have expired, and so on. Likewise, if the certificate is issued by a Certificate Authority or there are intermediate certificates in the chain, configure the Root CA certificate or alternatively a certificate bundle containing the root certificate, intermediate certificate 1, intermediate certificate 2 and onwards, in that order.

7. Enable the Scheduler component to complete the email configuration using SMTPS with Auth Login:

   ```
   scheduler enable
   ```

2.10.5 Scheduler detailed logging

The Scheduler supports the option to enable detailed logging for Web Bridge connections, email notifications, and API using the scheduler timedLogging MMP command.

When timedLogging is not enabled, Meeting Server displays the following output:

```
cms-vm> scheduler timedLogging
{
"webBridge": "0",
"api": "0",
"email": "0"
}
```

To enable any of the timedLogging options, use the command:

```
scheduler timedLogging (webBridge|api|email) <time>
```

For example,

```
cms-vm> scheduler timedLogging webBridge 600
SUCCESS
```

The time variable is expressed in seconds, and enables timedLogging for the set duration.

```
cms-vm> scheduler timedLogging
{
"webBridge": "594",
```

```
"api": "0",
"email": "0"
}
```

After the set duration expires or the specific investigation or troubleshooting step is completed download the log files using SFTP.

2.10.6 API additions

Scheduler introduces new API nodes in version 3.3. Meeting Server management API interface does not support Scheduler APIs. The scheduler has its own HTTPS interface which if enabled, can be used to configure scheduler meetings using the scheduler APIs.

The new nodes are available at the address specified in the new command **`scheduler https listen <interface> <port>`**, and are prefixed with **`https://hostname:port/api/v1/scheduler`**.

For example,

`https://hostname:port/api/v1/scheduler/health` or
`https://hostname:port/api/v1/scheduler/meetings`

The Scheduler API nodes are:

- **`/health`**
- **`/meetings`**
- **`/meetings/<meeting id>`**
- **`/meetings/<meeting id>/participants`**
- **`/meetings/<meeting id>/recurrences/<recurrence id>`**
- **`/meetings/<meeting id>/recurrences/<recurrence id>/participants`**
- **`/meetings/<meeting ID>/refreshEmails`**
- **`/meetings/<meeting ID>/recurrences/<recurrence id>/refreshEmails`**
- **`/timedLogging`**

2.10.6.1 Scheduler API message format

For its API operations, the Scheduler message body uses the JSON format.

For example,

POST to **`/timedLogging`** with

```
{
"email": 1000
}
```

2.10.6.2 Retrieving service health status

Retrieving service health status is supported by the API node **`/health`** using the method:

- GET on **`/health`**

Request element	Type/Value	Description/ Notes
status	String	Overall service health status
component	Array	See nested table below

Response element	Type/Value	Description
db:		
status	String	UP or DOWN
mail:		
status	String	UP or DOWN
details	Object	Server address and port.
cmsWebScheduler:		
status	String	UP or DOWN
details	Object	guid used as the Scheduler's identification on c2w connections.
ping:		
status	String	UP or DOWN

2.10.6.3 Creating, modifying, and deleting meetings in a coSpace

- POST to **`/scheduler/meetings`**
- GET on **`/scheduler/meetings`**
- DELETE on **`/scheduler/meetings`**

Creating a meeting is supported by POST to **`/scheduler/meetings`** with the following parameters:

Parameters	Type/Value	Description/ Notes
coSpace*	ID	coSpace ID.
organizerEmail	string	Meeting organizer's email.
organizerUserName	string	Meeting organizer's userName.
summary	string	Meeting summary, max length 50.

Parameters	Type/Value	Description/ Notes
isSchedulerSpaceOwner	true | false	true if the scheduler component is responsible for managing the lifetime of the coSpace. **Note:** When set to true, the scheduler will delete the coSpace approximately 24 hours after the end of the meeting / meeting series.
isFullDayMeeting	true | false	true if Meeting is a full day meeting. Either dtEnd or isFullDayMeeting is required.
dtEnd	string	Meeting end date in LocalDateTime full-time format. Example: 2021-01-30T08:30:00.000 Either dtEnd or isFullDayMeeting is required.
dtStart*	string	Meeting start date in LocalDateTime full-time format. Example: 2021-01-30T08:30:00.000
rrule	string	Frequency of the recurring meeting. Example: FREQ=YEARLY; BYMONTH=10; BYDAY=-1SU;UNTIL=20301105T082754Z
participants	Array	List of participants objects.
timeZone	string	The region or location corresponding to the dtStart and dtEnd elements. Example: "Europe/London" If not supplied, defaults to "UTC".

Parameters	Type/Value	Description/ Notes
email	string	User's email with email verification.
userName	string	Meeting participant's userName.
accessMethod	ID	accessMethod ID. If not supplied, then the cospace level join information will be used for invites.

Retrieving meeting occurrences is supported by GET on **`/scheduler/meetings`** with the following request parameters.

Parameters	Type/Value	Description/ Notes
coSpace	ID	coSpace ID.
maxMeetings	numeric	The maximum number of meetings to retrieve. Returns the first n meetings (after fromTime), ordered in ascending order of startDate. The minimum value is 1 minimum and default is 5.
fromTime	string	Calculated against meeting end date in ISO 8601 full-time format. Example: 2021-01-30T08:30:00Z. If unset, it defaults to the current time.
untilTime	string	Calculated against meeting start date in ISO 8601 full-time format. Example: 2021-01-30T08:30:00Z. If unset, then there is no upper limit on untilTime.
userName	string	Either organizerUserName or participant's userName.

Response element for GET on **`/scheduler/meetings`** is a list of meetings, each of which can have the following parameters:

Response elements	Type/Value	Description/ Notes
coSpace	ID	coSpace ID.
summary	string	Meeting title.
dtStart	string	Meeting start date in LocalDateTime full-time format. Example: 2021-01-30T08:30:00.000
dtEnd	string	Meeting end date in LocalDateTime full-time format. Example: 2021-01-30T08:30:00.000 Either dtEnd or isFullDayMeeting is returned.
meeting	ID	Meeting ID.
isSchedulerSpaceOwner	true | false	true if the scheduler component is responsible for managing the lifetime of the coSpace. **Note:** When set to true, the scheduler will delete the coSpace approximately 24 hours after the end of the meeting / meeting series.
isFullDayMeeting	true | false	true if Meeting is full day meeting. Either dtEnd or isFullDayMeeting is returned.

Response elements	Type/Value	Description/ Notes
rrule	string	Frequency of the recurring meeting. Example: FREQ=YEARLY; BYMONTH=10; BYDAY=-1SU; UNTIL=20301105T082754Z
organizerEmail	string	Meeting organizer's email.
organizerUserName	string	Meeting organizer's userName
participantCount	numeric	Number of participants invited to the meeting.
recurrence	string	Start time of the first occurrence of the recurrent meeting in ISO 8601 full-time format.
timeZone	string	The region or location corresponding to the dtStart and dtEnd elements. Example: "Europe/London" If not supplied, defaults to "UTC"

Deleting meetings in a coSpace is supported by DELETE on **`/scheduler/meetings`** with the **`coSpace`** parameter.

Request element	Type/Value	Description/ Notes
coSpace*	string	coSpace ID, with guid verification, length 36

2.10.6.4 Retrieving, modifying, or deleting individual meetings

Retreiving information on a individual meeting is supported by GET on **`/scheduler/meetings/<meeting id>`** and can return the following parameters:

Response elements	Type/Value	Description/ Notes
coSpace	ID	coSpace ID.
summary	string	Meeting title.
dtStart	string	Meeting start date in LocalDateTime full-time format. Example: 2021-01-30T08:30:00.000
dtEnd	string	Meeting end date in LocalDateTime full-time format. Example: 2021-01-30T08:30:00.000 Either dtEnd or isFullDayMeeting is returned.
meeting	ID	Meeting ID.

Response elements	Type/Value	Description/ Notes
isSchedulerSpaceOwner	true | false	true if the scheduler component is responsible for managing the lifetime of the coSpace. **Note:** When set to true, the scheduler will delete the coSpace approximately 24 hours after the end of the meeting / meeting series.
isFullDayMeeting	true | false	true if Meeting is full day meeting. Either dtEnd or isFullDayMeeting is returned.
rrule	string	Frequency of the recurring meeting. Example: FREQ=YEARLY; BYMONTH=10; BYDAY=-1SU; UNTIL=20301105T082754Z
organizerEmail	string	Meeting organizer's email.
organizerUserName	string	Meeting organizer's userName
participantCount	numeric	Number of participants invited to the meeting.
recurrence	string	Start time of the first occurrence of the recurrent meeting in ISO 8601 full-time format.
timeZone	string	The region or location corresponding to the dtStart and dtEnd elements. Example: "Europe/London" If not supplied, defaults to "UTC"

Modifying an individual meeting is supported by PUT to **`/scheduler/meetings/<meetingId>`** with the following parameters:

Parameters	Type/Value	Description/ Notes
coSpace	ID	coSpace ID.
organizerEmail	string	Meeting organizer's email.
organizerUserName	string	Meeting organizer's userName.
summary	string	Meeting title.
isSchedulerSpaceOwner	true | false	true if the scheduler component is responsible for managing the lifetime of the coSpace. **Note:** When set to true, the scheduler will delete the coSpace approximately 24 hours after the end of the meeting / meeting series.

Parameters	Type/Value	Description/ Notes
isFullDayMeeting	true | false	true if Meeting is full day meeting. Either dtEnd or isFullDayMeeting is returned.
dtStart	string	Meeting start date in LocalDateTime full-time format. Example: 2021-01-30T08:30:00.000
dtEnd	string	Meeting end date in LocalDateTime full-time format. Example: 2021-01-30T08:30:00.000 Either dtEnd or isFullDayMeeting is returned.
timeZone	string	The region or location corresponding to the dtStart and dtEnd elements. Example: "Europe/London" If not supplied, defaults to "UTC".
rrule	string	Frequency of the recurring meeting. Example: FREQ=YEARLY; BYMONTH=10; BYDAY=-1SU; UNTIL=20301105T082754Z
participants	Array	List of participants objects.

Parameters	Type/Value	Description/ Notes
email	string	User's email with email verification.
userName	string	Meeting participant's userName.
accessMethod	ID	accessMethod ID. If not supplied, then the cospace level join information will be used for invites.

Deleting meeting instances is supported by DELETE on **`/scheduler/meetings/<meeting Id>`**

Parameters	Type/Value	Description/ Notes
meetingId	ID	Meeting ID of the meeting to be deleted.

2.10.6.5 Modifying or retrieving the list of participants in a meeting

Retrieving participants of a meeting is supported by GET on **`/scheduler/meetings/<meetingId>/participants`** and each participant can include the

following objects:

<table>
<tr><th>Request element</th><th>Type/Value</th><th>Description/ Notes</th></tr>
<tr><td>participants</td><td>Array</td><td>List of participants objects.
<table>
<tr><th>Parameters</th><th>Type/Value</th><th>Description/ Notes</th></tr>
<tr><td>email</td><td>string</td><td>User's email with email verification.</td></tr>
<tr><td>userName</td><td>string</td><td>Meeting participant's userName.</td></tr>
<tr><td>accessMethod</td><td>ID</td><td>accessMethod ID. If not supplied, then the cospace level join information will be used for invites.</td></tr>
</table></td></tr>
</table>

Modifying the participants in a meeting or meeting series is supported by PUT to **`/scheduler/meetings/<meetingId>/participants`** with the following parameters:

<table>
<tr><th>Parameter</th><th>Type/Value</th><th>Description/ Notes</th></tr>
<tr><td>newParticipants</td><td>Array</td><td>Participants to be added to the invite list.
<table>
<tr><th>Parameters</th><th>Type/Value</th><th>Description/ Notes</th></tr>
<tr><td>email</td><td>string</td><td>User's email with email verification.</td></tr>
<tr><td>userName</td><td>string</td><td>Meeting participant's userName.</td></tr>
<tr><td>accessMethod</td><td>ID</td><td>accessMethod ID. If not supplied, then the cospace level join information will be used for invites.</td></tr>
</table></td></tr>
<tr><td>deletedEmailParticipants</td><td>array or strings</td><td>Participants with these email addresses will be removed from the invited list.</td></tr>
<tr><td>deletedUserParticipants</td><td>array or strings</td><td>Participants with these userNames will be removed from the invited list.</td></tr>
</table>

2.10.6.6 Creating, modifying, and deleting meeting occurrences

Retrieving meeting occurrences is supported by GET on **`/scheduler/meetings/<meeting id>/recurrences/<recurrence id>`** and returns the following values:

Response elements	Type/Value	Description/ Notes
coSpace	ID	coSpace ID.
summary	string	Meeting title.
dtStart	string	Meeting start date in LocalDateTime full-time format. Example: 2021-01-30T08:30:00.000
dtEnd	string	Meeting end date in LocalDateTime full-time format. Example: 2021-01-30T08:30:00.000 Either dtEnd or isFullDayMeeting is returned.
timeZone	string	The region or location corresponding to the dtStart and dtEnd elements. Example: "Europe/London" If not supplied, defaults to "UTC.
meeting	ID	Meeting ID.
isSchedulerSpaceOwner	true | false	true if the scheduler component is responsible for managing the lifetime of the coSpace. **Note:** When set to true, the scheduler will delete the coSpace approximately 24 hours after the end of the meeting / meeting series.
isFullDayMeeting	true | false	true if Meeting is full day meeting. Either dtEnd or isFullDayMeeting is returned.
rrule	string	Frequency of the recurring meeting. Example: FREQ=YEARLY; BYMONTH=10; BYDAY=-1SU; UNTIL=20301105T082754Z
organizerEmail	string	Meeting organizer's email.
organizerUserName	string	Meeting organizer's userName.
participantCount	integer	Number of participants invited to the meeting.
isCancelled	true | false	true if the meeting is canceled.

Modifying a meeting occurrence is supported by PUT to **`/scheduler/meetings/<meeting id>/recurrences/<recurrence id>`** with the following parameters:

Request parameters	Type/Value	Description/ Notes
summary	string	Meeting title.

<table>
<tr><th>Request parameters</th><th>Type/Value</th><th>Description/ Notes</th></tr>
<tr><td>isFullDayMeeting</td><td>true | false</td><td>true if Meeting is full day meeting.
Either dtEnd or isFullDayMeeting is required.</td></tr>
<tr><td>dtStart</td><td>string</td><td>Meeting start date in LocalDateTime full-time format.
Example: 2021-01-30T08:30:00.000</td></tr>
<tr><td>dtEnd</td><td>string</td><td>Meeting end date in LocalDateTime full-time format.
Example: 2021-01-30T08:30:00.000
Either dtEnd or isFullDayMeeting is required.</td></tr>
<tr><td>timeZone</td><td>string</td><td>The region or location corresponding to the dtStart and dtEnd elements.
Example: "Europe/London"
If not supplied, defaults to "UTC".</td></tr>
<tr><td>participants</td><td>Array</td><td>List of participants objects.
<table>
<tr><th>Parameters</th><th>Type/Value</th><th>Description/ Notes</th></tr>
<tr><td>email</td><td>string</td><td>User's email with email verification.</td></tr>
<tr><td>userName</td><td>string</td><td>Meeting participant's user-Name.</td></tr>
<tr><td>accessMethod</td><td>ID</td><td>accessMethod ID. If not supplied, then the cospace level join information will be used for invites.</td></tr>
</table></td></tr>
<tr><td>isCancelled</td><td>true | false</td><td>Indicates if the meeting is cancelled. If set to true, it cancels the meeting instance by recurrence ID.</td></tr>
</table>

2.10.6.7 Retrieving or modifying the participants in a meeting occurrence

Retrieving a list of participants in a meeting occurrence is supported by GET on **`/scheduler/meetings/<meeting id>/recurrences/<recurrence id>/participant`** with the following parameters:

<table>
<tr><th>Request element</th><th>Type/Value</th><th>Description/ Notes</th></tr>
<tr><td>participants</td><td>Array</td><td>List of participants objects.
<table>
<tr><th>Parameters</th><th>Type/Value</th><th>Description/ Notes</th></tr>
<tr><td>email</td><td>string</td><td>User's email with email verification.</td></tr>
<tr><td>userName</td><td>string</td><td>Meeting participant's userName.</td></tr>
<tr><td>accessMethod</td><td>ID</td><td>accessMethod ID. If not supplied, then the cospace level join information will be used for invites.</td></tr>
</table></td></tr>
</table>

Modifying the participants in a meeting occurance is supported by PUT to **`/scheduler/meetings/<meeting id>/recurrences/<recurrence id>/participants`** with the following parameters:

<table>
<tr><th>Parameter</th><th>Type/Value</th><th>Description/ Notes</th></tr>
<tr><td>newParticipants</td><td>Array</td><td>Participants to be added to the invite list.
<table>
<tr><th>Parameters</th><th>Type/Value</th><th>Description/ Notes</th></tr>
<tr><td>email</td><td>string</td><td>User's email with email verification.</td></tr>
<tr><td>userName</td><td>string</td><td>Meeting participant's userName.</td></tr>
<tr><td>accessMethod</td><td>ID</td><td>accessMethod ID. If not supplied, then the cospace level join information will be used for invites.</td></tr>
</table></td></tr>
<tr><td>deletedEmailParticipants</td><td>array or strings</td><td>Participants with these email addresses will be removed from the invited list.</td></tr>
<tr><td>deletedUserParticipants</td><td>array or strings</td><td>Participants with these userNames will be removed from the invited list.</td></tr>
</table>

2.10.6.8 Refreshing emails for a coSpace

Refreshing emails for a coSpace is supported by:

POST on **`/scheduler/meetings/refresh?coSpace=<coSpace id>`**

Parameters	Type/Value	Description/ Notes
meeting*	ID	Meeting id.

2.10.6.9 Refreshing emails for single meeting and whole meeting series

Refreshing emails for a meeting is supported by:

PUT to **`/scheduler/meetings/<meeting ID>/refreshEmails`**

Parameters	Type/Value	Description/ Notes
meeting*	ID	Meeting id.

Refreshing emails for one meeting recurrence from the meeting series is supported by:

PUT to**`/scheduler/meetings/<meeting ID>/recurrences/<recurrence id>/refreshEmails`**

Parameters	Type/Value	Description/ Notes
meeting*	ID	Meeting id.
reccurence*	string	Id of single instance in LocalDateTime full-time format. Example: 2021-01-30T08:30:00Z

2.10.6.10 Modifying and retrieving timed logging information

This feature introduces a new API node **`/scheduler/timedLogging`** to support the following operations:

- PUT to **`/scheduler/timedLogging`**
- GET on **`/scheduler/timedLogging`**

Parameters	Type/Value	Description/ Notes
webBridge	numeric	time remaining (in seconds) for which detailed Web Bridge logging should be enabled.
api	numeric	Time remaining for HTTPS side logging (in seconds).
email	numeric	Time remaining for email logging (in seconds).

2.10.7 MMP additions

The output of the **`help scheduler`** command is:

```
cms> help scheduler
```

```
scheduler
scheduler https listen <interface> <port>
scheduler https listen none
scheduler https certs <key-file> <crt-fullchain-
file>
scheduler https certs none
scheduler c2w certs <key-file> <crt-fullchain-file>
scheduler c2w certs none
scheduler c2w trust <crt-bundle>
scheduler c2w trust none
scheduler email server <hostname|address> <port>
scheduler email server none
scheduler email username <smtp username>
scheduler email remove username
scheduler email protocol <smtp|smtps>
scheduler email auth <enable|disable>
scheduler email starttls <enable|disable>
scheduler email trust <bundle>
scheduler email trust none
scheduler timedLogging get
scheduler timedLogging put <webBridge> <api> <email>
scheduler enable
scheduler disable
scheduler restart
scheduler status
```

The configuration details of the email server are provided via the new **scheduler** MMP commands listed below:

Command / Examples	Description / Notes
scheduler **scheduler status**	Displays current status of the Scheduler.
scheduler (enable | disable)	Enables or disables the Scheduler.
scheduler restart	Restarts the Scheduler.

Command / Examples	Description / Notes
scheduler https listen <interface> <port>	Configures an interface:port pair for the Scheduler to listen on.
scheduler https listen none	Disables the Scheduler's management API interface.
scheduler https certs <key-file> <crt-fullchain-file>	Configures the server certs used in the management API but also the certs used when making outbound connections.For example, the c2w link or any API calls to the Call Bridge.
scheduler https certs none	Removes certificate configuration for the management API.
scheduler c2w certs <key-file> <crt-fullchain-file>	Configures the certificate bundle presented to a Web Bridge 3.
scheduler c2w certs none	Removes certificate configuration for the TLS connection to Web Bridge 3.
scheduler c2w trust <crt-bundle>	Configures the trust bundle for verifying connections to the Web Bridges.
scheduler c2w trust none	Removes the certificate bundle for the Web Bridge 3 from the Scheduler's trust store.
scheduler email server <hostname | address> <port>	Configures the SMTP server to which the Scheduler will send emails.
scheduler email server none	Removes email server configuration from the Scheduler.
scheduler email username <smtp user-name>	Configures the email account used for authentication with the SMTP server. This account must have appropriate permissions to be able to send emails on behalf of the meeting organizers. Note: Emails to participants will not sent from the account configured using this command, but will be sent using the From address of the meeting organizer.
scheduler email remove username	Removes the email username configured for SMTP authentication.
scheduler email protocol <smtp | smtps>	Specifies the Scheduler's communication with the email server as: smtp: over plain text TCP (smtp) smtps: over an encrypted TLS channel
scheduler email auth (enable | disable)	Enables or disables SMTP authentication.
scheduler email starttls (enable | disable)	Enables or disables opportunistic TLS for SMTP connections.

Command / Examples	Description / Notes
`scheduler email trust <bundle> | none`	(Optional) Allows configuration of a trust bundle for the email server. If configured, verification is done for the certificate of the email server using the configured bundle. If not configured, verification of the certificate is not done.
`scheduler timedLogging`	Retrieves timed logging status.
`scheduler timedLogging (webBridge|api|email) <time>`	Activates logging for the specified time period.

2.11 Summary of 3.3 API additions and changes

API functionality for the Meeting Server 3.3 includes:

- New API parameter to support active speaker in pane placement
- New API parameter to change role of a participant during a meeting
- Modification to API objects and parameters to support Email invitation
- Modification to API parameter to support web app and SIP layout alignment
- New API objects and parameters to support the Scheduler component

2.11.1 API additions

New API functionality for the Meeting Server 3.3 include new API objects and minor API enhancements.

New API objects

Version 3.3 introduces the Scheduler, a new component that enables scheduling meetings through web app. Scheduler APIs include new nodes that support scheduling, modifying or deleting meetings with single or multiple occurrences, adding or removing participants, retrieving health information, and sending or refreshing email notifications. .

Minor API enhancements

- The following parameters have been modified to support web app and SIP layout alignment:
  - POST to **`/coSpaces`**
  - PUT to **`/coSpaces/<coSpace id>`**
  - POST to **`/calls/<call id>/participants`**
  - POST to **`/calls/<call id>/callLegs`**
  - PUT to **`/callLegs/<callLeg id>`**

- POST to **/callLegProfiles**
- PUT to **/callLegProfiles/<call leg profile id>**

The effective value of **defaultLayout** (as calculated based on the hierarchy of call leg profiles) determines the layout at the start of the call. This parameter can be set on the following API objects:

The **chosenLayout** parameter can be used to change the layout during the call and is supported on the following API nodes:

- POST to **/calls/<call id>/callLegs**
- PUT to **/callLegs/<callLeg id>**
- GET on **/callLegs/<callLeg id>**

The **layout** parameter is supported on GET on **/callLegs/<callLeg id>** to retrieve the layout selected in web app or the SIP endpoint.

Note: The **defaultLayout** setting for **/callLegProfiles** will be inherited if **defaultLayout** is left blank for **/coSpaces**, **/calls**, **/callLegs**. If both **defaultLayout** and **layout** are set then **defaultLayout** takes precedence.

Pane placement is enabled by the existing parameters, **panePlacementHighestImportance** and **panePlacementSelfPaneMode** supported on the following methods:

- POST to **/coSpaces**
- PUT to **/coSpaces/<coSpace id>**
- POST to **/calls**
- PUT to **/calls/<call id>**

The **changeLayoutAllowed** parameter is supported on the following API methods to assign the permissions to change the layout in web app and SIP endpoints:

- POST to **/callLegProfiles**
- PUT to **/callLegProfiles/<call leg profile id>**
- POST to **/calls/<call ID>/callLegs**
- PUT to **/callLegs/<callLeg id>**
- POST to **/calls/<call id>/participants**

For details on using the API see the Cisco Meeting Server API Reference Guide.

- The following parameter is added to the coSpace object.

  The **emailInvitation** parameter is added to retrieve text based meeting information for a coSpace.

  - GET on **/api/v1/coSpaces/<coSpace id>/emailInvitation**

    The GET method on this node also returns subject as a separate response element, in addition to invitation and language response elements.

New/modified error code reasons introduced in version 3.3

- **invalidValue** - You entered an empty string or an invalid character as a language parameter.
- **retryAfter** - You tried to retrieve the text based meeting entry information when the server was busy or was fetching externally hosted template. Retry later or retry after recommended retryAfter period in seconds.
- **valueTooLong** - You entered long language parameter.

2.11.2 New and modified parameters

New parameters in version 3.3

- **panePlacementActiveSpeakerMode** is introduced on
  - POST to **/coSpaces**
  - PUT to **/coSpaces/<coSpace id>**
  - GET on **/coSpaces/<coSpace id>**
  - POST to **/calls**
  - PUT to **/calls/<call id>**
  - GET on **/calls/<call id>**
- **changeRoleAllowed** is introduced on
  - POST to **/callLegProfiles**
  - GET on **/callLegProfiles/<call leg profile id>**
  - PUT to **/callLegProfiles/<call leg profile id>**
  - GET on **/callLegs/<call leg id>**
  - PUT to **/callLegs/<call leg id>**
  - POST to **/calls/<call id>/callLegs**
  - POST to **/calls/<call id>/participants**

Modified parameters in version 3.3

- The **accessMethod** parameter is modified to enable changing a participant's role using following operation:
    - PUT to **/callLegs/<call leg id>**

2.11.3 Enabling / disabling active speaker in pane placement

The new **panePlacementActiveSpeakerMode** API parameter can be configured to enable active speaker in pane placement. This parameter is supported by the following methods:

- POST to **/coSpaces**
- PUT to **/coSpaces/<coSpace id>**
- GET on **/coSpaces/<coSpace id>**
- POST to **/calls**
- PUT to **/calls/<call id>**
- GET on **/calls/<call id>**

The parameter setting at the calls level takes precedence over the setting at coSpace level. If unset at both levels, active speaker is disabled.

Parameter	Type/Value	Description/ Notes
panePlacementActiveSpeakerMode	allowself | suppressself | none	• allowself - displays the participant in the first pane if they are the active speaker, additional to displaying the participant in the pane set by pane placement. The same view is displayed for all participants. • suppressself - displays the active speaker in the first pane for all other participants other than the active speaker. For the active speaker, the previous speaker is displayed in the first pane. • none - the feature is disabled.

2.11.4 Retrieving Email invitation text

The following method retrieves the coSpace level meeting join information:

- GET on **/api/v1/coSpaces/<coSpace id>/emailInvitation**

URI Parameters	Type/Value	Description / Notes
language (optional)	String	In the form of a language tag "xx" or "xx_XX" (xx language code and XX region code) or any other string between 1 and 32 characters (allowed characters: 'a'-'z', 'A'-'Z', '0'-'9', and '_').

Response Elements	Type/ Value	Description / Notes
subject	String	Subject of the invitation.
invitation	String	Email invitation text.
language	String	Language tag of email invitation. If no language is specified, then it defaults to en_US. If the specified language is invalid, then a "400 - Bad Request" response is returned.

2.11.4.1 Failure responses

Response Elements	Type/ Value	Description / Notes
invalidValue	400 - Bad Request	You entered an empty string or an invalid character as a language parameter.
valueTooLong	400 - Bad Request	You entered a long language parameter.
retryAfter	503 - Service Unavailable	You tried to retrieve the text based meeting entry information when the server was busy or was fetching externally hosted template. Retry later or retry after recommended **retryAfter** period in seconds.

2.11.5 Changing the role of participant in a web app meeting

The new **changeRoleAllowed** parameter is introduced in 3.3 to enable participants to change the role of other participants in web app. The parameter is supported in the following API methods:

- POST to **/callLegProfiles**
- PUT to **/callLegProfiles/<call leg profile id>**
- GET on **/callLegProfiles/<call leg profile id>**
- PUT to **/callLegs/<call leg id>**

- GET on **/callLegs/<call leg id>**
- POST to **/calls/<call id>/callLegs**
- POST to **/calls/<call id>/participants**

Request parameters	Type/Value	Description/ Notes
changeRoleAllowed	**true**, **false**, or <**unset**>	Determines whether or not the participant can change the role of another participant in a call when using the web app. The usual rules for the hierarchy of call leg profiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to false.

2.12 Summary of MMP additions and changes

Version 3.3 supports the MMP additions described in this section.

2.12.1 LDAP authentication

The new **ldap** option is added to **user add** MMP command enables configuring details of an LDAP server, directory search parameters, TLS settings, and enabling or disabling LDAP authentication.

To enable adding LDAP users, a new option, [**ldap**] is added to the command:

```
user add <username> (admin|crypto|audit|appadmin|api) [ldap]
```

Note: Meeting Server API does not support access to users with LDAP authentication.

The output of the **help ldap** command is:

```
cms> help ldap
Configure LDAP client for MMP users
Usage:
    ldap
    ldap server <hostname|address> <port>
    ldap protocol (ldap|ldaps)
    ldap binddn <username>
    ldap basedn <base DN>
    ldap login_attr <attribute>
    ldap filter <filter>
```

```
ldap remove <binddn|filter|trust>
ldap trust <crt bundle>
ldap verify (enable|disable)
ldap min-tls-version <minimum version string>
ldap enable
ldap disable
ldap status
```

Note:
The **user list** MMP command is extended to include logged in LDAP users.
The only **user rule** parameters that apply to LDAP users are max_failed_logins, max_idle, and max_sessions. Other parameters of this command do not apply to LDAP users.
The **user expire** MMP command is not supported for LDAP users.

Command/Examples	Description/ Notes
ldap	Displays information about the ldap configuration.
ldap server <hostname|address> <port>	Specifies the LDAP server with hostname or IP address, and port number. This is mandatory.
ldap protocol (ldap|ldaps)	Specifies the ldap protocol to use. To use a secure connection to the LDAP server, ldaps must be used. It is mandatory to specify the protocol.
ldap binddn <username> **ldap binddn cn=binduser,oi=user,dc=domain,dc=com** **ldap binddn "cn=bind user,o=My Company,dc=domain,dc=com"** **ldap binddn domain\\username**	Adds the distinguished name with which to bind to the directory server for lookups.The binddn parameter is optional. If not specified, anonymous bind requests are used. The bind user must have search permission in the directory. This command prompts for an optional bind password. If spaces are included in the argument, then the argument has to be quoted. If backslashes are included, they must be escaped with a preceding backslash.
ldap basedn <base DN>	Specifies the base distinguished name to use as search base. It is mandatory to specify basedn. If spaces are included in the argument, then the argument has to be quoted. If backslashes are included, they must be escaped with a preceding backslash.

Command/Examples	Description/ Notes
ldap login_attr <attribute>	Specifies the LDAP attribute name such as uid, userPrincipalName, or sAMAccountName, which uniquely identifies users. The attribute value must match the pre-configured MMP user name for successful login. Specifying an attribute is mandatory.
ldap filter <filter> **ldap filter (&(objectClass=*) (memberOf=CN=admins,DC=example,DC=com))**	Sets up an LDAP search filter. Specifying a filter is optional. If no filter is specified, the default value (objectClass=*) is used. A valid LDAP filter syntax must be used and it must be enclosed in parentheses.
ldap remove (binddn|filter|trust)	Removes binddn, filter, or trust parameters that have been set up earlier.
ldap trust <crt bundle>	Configures the system to use a particular bundle of certificates to validate the certificate. To use a secure connection to the LDAP server, this must be configured with a trusted CA.
ldap verify (enable|disable)	Enables or disables certificate verification for connection to the LDAP server. To use a secure connection to the LDAP server, certificate validation must be enabled. When disabled, Meeting Server does not request or check the trust certificates.
ldap min-tls-version <minimum version string>	Configures the minimum TLS version that the system will use. Possible values are 1.0, 1.1, and 1.2. The default is version 1.2.
ldap enable	Enables the LDAP service.
ldap disable	Disables the LDAP service.
ldap status	Displays the status of the ldap service as: running - indicates that the service is running not running - the service is enabled but not running. Check the logs for more information. disabled - the service is disabled

2.12.2 SSH fingerprints verification

To verify the keys prompted by the Meeting Server against the retrieved keys before logging in, use the MMP command, **ssh server_key list.**

The new MMP command is added, to display a list of keys installed in the Meeting Server.

ssh server_key list

The output displays a list of keys along with the size, type, and fingerprints for all existing keys in the Meeting Server host, among the following keys:

- ssh_host_dsa_key.pub
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key.pub
- ssh_host_key.pub
- ssh_host_rsa_key.pub

2.12.3 Scheduler configuration

The configuration details of the email server are provided via the new **scheduler** MMP commands listed below:

Command / Examples	Description / Notes
scheduler **scheduler status**	Displays current status of the Scheduler.
scheduler (enable | disable)	Enables or disables the Scheduler.
scheduler restart	Restarts the Scheduler.
scheduler https listen <interface> <port>	Configures an interface:port pair for the Scheduler to listen on.
scheduler https listen none	Disables the Scheduler's management API interface.
scheduler https certs <key-file> <crt-fullchain-file>	Configures the server certs used in the management API but also the certs used when making outbound connections.For example, the c2w link or any API calls to the Call Bridge.
scheduler https certs none	Removes certificate configuration for the management API.
scheduler c2w certs <key-file> <crt-fullchain-file>	Configures the certificate bundle presented to a Web Bridge 3.
scheduler c2w certs none	Removes certificate configuration for the TLS connection to Web Bridge 3.
scheduler c2w trust <crt-bundle>	Configures the trust bundle for verifying connections to the Web Bridges.
scheduler c2w trust none	Removes the certificate bundle for the Web Bridge 3 from the Scheduler's trust store.
scheduler email server <hostname | address> <port>	Configures the SMTP server to which the Scheduler will send emails.
scheduler email server none	Removes email server configuration from the Scheduler.

Command / Examples	Description / Notes
scheduler email username <smtp username>	Configures the email account used for authentication with the SMTP server. This account must have appropriate permissions to be able to send emails on behalf of the meeting organizers. **Note:** Emails to participants will not sent from the account configured using this command, but will be sent using the From address of the meeting organizer.
scheduler email remove username	Removes the email username configured for SMTP authentication.
scheduler email protocol <smtp | smtps>	Specifies the Scheduler's communication with the email server as: smtp: over plain text TCP (smtp) smtps: over an encrypted TLS channel
scheduler email auth (enable | disable)	Enables or disables SMTP authentication.
scheduler email starttls (enable | disable)	Enables or disables opportunistic TLS for SMTP connections.
scheduler email trust <bundle> | none	(Optional) Allows configuration of a trust bundle for the email server. If configured, verification is done for the certificate of the email server using the configured bundle. If not configured, verification of the certificate is not done.
scheduler timedLogging	Retrieves timed logging status.
scheduler timedLogging (webBridge|api|email) <time>	Activates logging for the specified time period.

2.13 Summary of CDR Changes

There are no new additions to the Call Detail Records of the Meeting Server in version 3.3.

2.14 Summary of Event Changes

There are no new Events for version 3.3.

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 3.3.3

The Meeting Server 3.2.2 is the minimum version required to upgrade to version 3.3. If you are upgrading from an earlier version, then you must upgrade to 3.2.2 first following the instructions in the 3.2.2 release notes, before following any instructions in these Cisco Meeting Server 3.3 Release Notes.

Note: Cisco has not tested upgrading from a software release earlier than 3.2.2.

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

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

3.1 Upgrading to Release 3.3.3

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

CAUTION: Before upgrading 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.

Note: If you have deployed a clustered database, before upgrading your meeting servers, uncluster all the nodes using the **`database cluster remove`** command. Users must uncluster the nodes, upgrade the Meeting Server and cluster the nodes back using the MMP commands. See Scalable and Resilient guide for steps on clustering databases.

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.

Note:
Meeting Server 3.0 introduced a mandatory requirement to have Cisco Meeting Management

---

3.0 (or later). Meeting Management handles the product registration and interaction with your Smart Account (if set up) for Smart Licensing support.

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_3_3_3_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:
   abb1b1a560685e6596b5f2932262344061c8ece2803a1c06a29c694bb537f07c

   Cisco_Meeting_Server_3_3_3_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:
   c5923ec392826c911e26c79989a681da546cd25feee4e62f6461ff03d62f0bba

   Cisco_Meeting_Server_3_3_3.ova

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

   For vSphere6, hash (SHA-512) for Cisco_Meeting_Server_3_3_3_vSphere-6_0.ova:
   acd3e7aa3e0ce29b4b3997b1e5c44c1c1f58b90b33458d396bdeeab189cc63260575a44e7b2802fcdccebed4c6fad61d283996ec7fcf6ef2a76e754b5841f3ec

   For vSphere6.5 and higher, hash (SHA-512) for Cisco_Meeting_Server_3_3_3_vSphere-6_5.ova:
   eb51ea3c0810e69c05b22b82499c21e0bfa096df1ea64ce7ca41a5d2cfef5bffd1d9fae115e4730f74ef498c18b414afe369e4a409c1e30c0d2f92702be94164

2. To validate the OVA file, the checksum for the 3.3.3 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 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" 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 cms.lic 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. a. In the case of XMPP clustering, if applicable, you need to re-cluster XMPP:
   a. Pick one node as the XMPP primary, initialize XMPP on this node
   b. Once the XMPP primary 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, if applicable,
   - 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 Deployments

To simplify explaining how to deploy the Meeting Server, deployments are described in terms of three models:

- single combined Meeting Server – all Meeting Server components (Call Bridge, Web Bridge 3, Database, Recorder, Uploader, Streamer and TURN server) are available, the Call Bridge and Database are automatically enabled but the other components can be individually enabled depending upon the requirements of the deployment. All enabled components reside on a single host server.
- single split Meeting Server – in this model the TURN server, Web Bridge 3, and MeetingApps are enabled on a Meeting Server located at the network edge in the DMZ, while the other components are enabled on another Meeting Server located in the internal (core) network.
- the third model covers deploying multiple Meeting Servers clustered together to provide greater scale and resilience in the deployment.

Deployment guides covering all three models are available here. Each deployment guide is accompanied by a separate Certificate Guidelines document.

Points to note:

The Cisco Meeting Server 2000 only has the Call Bridge, Web Bridge 3, and database components. It is suited for deployment on an internal network, either as a single server or a cascade of multiple servers. The Cisco Meeting Server 2000 should not be deployed in a DMZ network. Instead if a deployment requires firewall traversal support for external Cisco Meeting Server web app users, then you will need to also deploy either:

- a Cisco Expressway-C in the internal network and an Expressway-E in the DMZ, or
- a separate Cisco Meeting Server 1000 or specification-based VM server deployed in the DMZ with the TURN server enabled.

The Cisco Meeting Server 1000 and specification-based VM servers have lower call capacities than the Cisco Meeting Server 2000, but all components (Call Bridge, Web Bridge 3, Database, Recorder, Uploader, Streamer and TURN server) are available on each host server. The Web Bridge 3, Recorder, Uploader, Streamer and TURN server require enabling before they are operational.

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 `3.2`.
2. From the list of bugs that appears, filter the list using the *Modified Date*, *Status*, *Severity*, *Rating* drop down lists.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

4.1 Resolved issues

Issues seen in previous versions that are fixed in 3.3.3.

Cisco identifier	Summary
CSCwa68125	When a participant applies a custom layout, the video in the fixed pane is not displayed through the entire screen.
CSCwb39239	Cisco has evaluated the impact of vulnerability, identified by CVE - CVE-2022-0778, in openssl. The product is affected by the vulnerability and hence the openSSL version has been upgraded to OpenSSL 1.1.1n.
CSCwb31492	Cisco has evaluated the impact of vulnerability, identified by CVE - CVE-2022-22719, CVE-2022-22720, CVE-2022-22721, CVE-2022-23943 in Apache-2.4.52. For details on the vulnerabilities, see Apache HTTP Server Vulnerabilities. The product is affected by the vulnerabilities and hence the Apache HTTP Server version is upgraded to Apache-2.4.53.
CSCwb43662	The spring framework version of Spring boot has been upgraded to 5.2.20.

Issues seen in previous versions that are fixed in 3.3.2.

Cisco identifier	Summary
CSCwa19318	When active speaker with pane placement is enabled in a customized layout, fixed pane window might flicker when the active speaker is changing frequently.
CSCwa58708	On September 16, 2021 the Apache Software Foundation disclosed five vulnerabilities affecting the Apache HTTP Server (httpd) 2.4.48 and earlier releases identified by CVE IDs: CVE-2021-40438, CVE-2021-33193, CVE-2021-34798, CVE-2021-36160, CVE-2021-39275. For details on the vulnerabilities, see Apache HTTP Server Vulnerabilities. Cisco has evaluated the impact of the vulnerability on this product and concluded that the product is affected by: • CVE-2021-34798 - NULL pointer dereference in httpd core • CVE-2021-40438 - mod_proxy SSRF However, the product is not affected by the following vulnerabilities: • CVE-2021-33193 - Request splitting via HTTP/2 method injection and mod_proxy • CVE-2021-39275 - ap_escape_quotes buffer overflow • CVE-2021-36160 - mod_proxy_uwsgi out of bound read

Issues seen in previous versions that are fixed in 3.3.1.

Cisco identifier	Summary
CSCvy95143	Occasionally in a SIP call, Meeting Server sends and receives an INVITE from the same call dialog at the same time, disconnecting the call due to time out.
CSCvz76478	When the participants use Safari (iOS 15) to join web app meeting, they are unable to hear audio and view video in the meeting. **Note:** A fix has been introduced in Meeting Server 3.3.1 release to resolve this issue in iOS 15.0 and iOS 15.2. The issue still persists in iOS 15.1.

Issues seen in previous versions that are fixed in 3.3.

Cisco identifier	Summary
CSCvy83131	ESXi 7.0 based new installations of Cisco Meeting Server 1000 M4 and M5v1 variants fail to boot due to insufficient disk space on the server. An error message "Module 'MonitorLoop' power on failed" is displayed. Resolution: Edit the Virtual Hardware settings of the VM and select **Reserve all guest memory (All locked)** in the Memory settings.

Cisco identifier	Summary
CSCvy42970	The MMP command **`user rule max_sessions <number>`** sets the limit for maximum SSH, SFTP, and Web Admin sessions individually. In previous releases, the command only worked for SFTP and Web Admin sessions.
CSCvy43380	Administrator logout events should be recorded in Meeting Server audit logs for all SSH client applications. For some clients like PuTTY and WinSCP, these events were not being recorded.

4.2 Open issues

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
CSCvz01886	When a participant's role does not have permissions to share video and presentation, then the role is changed and they have permissions to share video and presentation, the presentation is not visible to other participants when they share content.
CSCvw61547	On very rare occasions, calls through a Meeting Server TURN component may fail to connect or may lack a media channel. An error similar to "TURN 437 allocation mismatch in state RefreshTurnAllocationPending" will be seen in the Call Bridge syslog.
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.
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.
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.

Cisco identifier	Summary
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`.
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.

4.2.1 Known limitations

Cisco identifier	Summary
CSCvz35014	Web bridge 3 is not reachable when using an IPv6 address.

- From version 3.1, Cisco Meeting Server supports TURN short-term credentials. This mode of operation can only be used if the TURN server also supports short-term credentials, such as the Meeting Server TURN server in version 3.1 onwards. Using Cisco Meeting Server with Expressway does not support short-term credentials.
- When scheduling meetings using web app, display names are not included in emails.

5 Related user documentation

The following sites contain documents covering installation, planning and deployment, initial configuration, operation of the product, and more:

- Release notes (latest and previous releases): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-release-notes-list.html
- Install guides (including VM installation, Meeting Server 2000, and using Installation Assistant): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-guides-list.html
- Configuration guides (including deployment planning and deployment, certificate guidelines, simplified setup, load balancing white papers, and quick reference guides for admins): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html
- Programming guides (including API, CDR, Events, and MMP reference guides and customization guidelines): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html
- Open source licensing information: https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-licensing-information-listing.html
- Cisco Meeting Server FAQs: https://meeting-infohub.cisco.com/faq/category/25/cisco-meeting-server.html
- Cisco Meeting Server interoperability database: https://tp-tools-web01.cisco.com/interop/d459/s1790

6 Accessibility Notice

Cisco is committed to designing and delivering accessible products and technologies.

The Voluntary Product Accessibility Template (VPAT) for Cisco Meeting Server is available here:

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence

You can find more information about accessibility here:

www.cisco.com/web/about/responsibility/accessibility/index.html

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