Avaya Meetings® Management for Meetings® Server R9.1 FP15 SP1 (9.1.15.1.4)

Release Notes

Avaya Meetings® Management
Version 9.1.15.1.4
for Meetings® Server R9.1 FP15 SP1

November 2025

Release Notes for Avaya Meetings Management for Meetings Server R9.1 FP15, May 2025

http://support.avaya.com

Contents

Document changes

Date	Description
25-11-2025	**First Release of the document**

Product Downloads

Avaya Meetings Server applications can be downloaded using their respective Download IDs as shown below:

9.1.15 SP1 Downloads

PLDS Download ID	File Name	Product Description
EQMNG000918	MeetingsMgmt_9_1_15_1_4.zip	Avaya Meetings Management Server (AMMG) 9.1.15 SP1
EQMS0000917	MeetingsMediaServer_9_1_15_1.zip	Avaya Meetings Media Server 9.1.15 SP1

Introduction

This document provides late-breaking information to supplement **Avaya Meetings® Management** software and documentation. For updated documentation, product support notices, and service pack information, go to the Avaya Support site at https://support.avaya.com/products/P1777/avaya-meetings-management/9.1.x.

Note: Prior to Release 9.1 FP11, this product was known as Avaya Equinox Management.

Installation

Product compatibility

At the time of this publication, Avaya Meetings Management 9.1.15.1.4 for Meetings® Server R9.1 FP15 SP1 is compatible with the product versions below. For the most accurate and up to date compatibility information go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Component	Version
Avaya Meetings Management Bundle	9.1.15.1.4 Bundle 9.1.15.1.3 (Management) 9.1.0.40 (GK) 2.2.0.12 (SIP B2BUA) 9.1.15.1.1 (UCCS) 10.2.0.0.41 (Portal/AAWG) 9.1.14.1.10 (PMGR)
Avaya Meetings Media Server Bundle	9.1.15.1.1 Bundle 9.1.15.1.1 (MCU) 10.1.0.176 (AAMS) 1.2.8.16 (WCS) 9.1.14.1.10 (PMGR)
Avaya XT5000 / XT4200 / XTE240	9.2.5.145
Avaya XT7000	9.2.5.145
Avaya Collaboration Unit CU360	11.4.0.41
Collaboration Control Application (iOS)	9.2.0.1.2
Collaboration Control Application (Android)	1.0.0.6
Avaya Meetings H.323 Server	9.1.0.36

Avaya Meetings H.323 Client	9.0.0.10
Avaya Meetings Streaming & Recording	9.1.13.1.3
Avaya Meetings Recording Gateway	9.1.15.0.1
Web Client (SWC)	9.1.15.0.4
JS Client SDK	4.10.0.5

Component	Version
Avaya Workplace Client for Windows: Avaya Workplace Client for Mac: Avaya Workplace Client for Android: Avaya Workplace Client for iOS:	3.30.0.64 3.30.0.64 3.30.0.64 3.30.0.64.15
ASBCE	FIPS Fedramp Deployments – 8.0.1.0-10-17555 Commercial Deployments – 8.1.3.0-31-21052
AAWG for TE Deployments	10.2.0.0.41
AAMS for TE Deployments	10.1.0.176
Aura for TE Deployments	FIPS Fedramp Deployments – 8.0.1.1 Commercial Deployments – 10.1
AADS for TE Deployments	FIPS Fedramp Deployments – 8.1.4.0.165 Commercial Deployments – 10.1.0.0.112

Installation Overview

Avaya Meetings Management 9.1.15 SP1 is delivered as a Service Pack for the Meetings Management OVA deployment. This Service Pack can be applied on top of an existing Meetings Management 9.1.15 installation.

Meetings Management continues to be available as a Virtualized Software OVA that includes the Linux Red Hat 8.10 operating system and is supported on VMware ESXi 7.0.3 and higher versions

Note:

1. The OVA can be deployed using vSphere web client for vCenter, and also directly via the ESXi web client. The OVA can also be deployed on Avaya Solutions Platform (ASP) servers running VMware based Appliance Virtualization Platform.
2. Use of iDRAC9 with Avaya ASP servers for Avaya Meetings applications and OVAs is permitted and recommended. See the Avaya Solutions Platform 130 Series iDRAC9 Best Practices.

Service Pack Applicability

For upgrades from prior versions or for fresh OVA installations, first complete the installation or upgrade to Meetings Management **9.1.15 GA** and then apply this **Service Pack (9.1.15.1.4)**.

Note: Applying this Service Pack requires the platform to be running **Meetings Management 9.1.15** (bundle version 9.1.15.0.6, exact GA bundle reference as per PLDS).

Meetings Management 9.1.x can be deployed in two main environments:

• TE (Team Engagement) Model. This model is purchased through Power Suite and addresses customers who already have or plan to deploy a full Avaya Aura UC platform versions 10.x that includes System Manager(SMGR), Session Manager (SM) and all other Avaya Aura UC components. Such customers will have access to the **"per named user"** business model and will obtain Meetings as part of the Power Suite (permanent or subscription) licensing entitlement. In TE deployment, the connection of 3rd Party videoconferencing terminals requires a specific enabling license, named "Third Party Videoconferencing Connectivity". Each license enables 10 concurrent ports for terminals connection.

• OTT (Over the Top) Model. This model is purchased as Enterprise Edition or Multi-tenant edition. Customers can use an UC platform, other than Avaya Aura, integrating to the Meetings Solution through a SIP trunk, or simply use the conferencing platform. Such customers will use the **"per port"** based model and might already be using Scopia Release 8.3 or Avaya Aura Conferencing (AAC) Release 8 "turnkey" solution. Such customers will benefit from new features as Meet me Web (WebRTC) connectivity, software only, virtualized MCU with HD video, high-capacity audio, web content sharing and more.

The above deployment models, as well as their options and installation scenarios, are described in detail in the Avaya Meetings Server 9.1.14 Offer Definition.

Required patches

No patches required for the Meetings Management 9.1.15 SP1 version.

However once the above version is deployed, the Meetings Management must be upgraded with Security Update package SSP-015-36.

Backing up the software

Please refer to the documentation, which is available at: https://support.avaya.com.

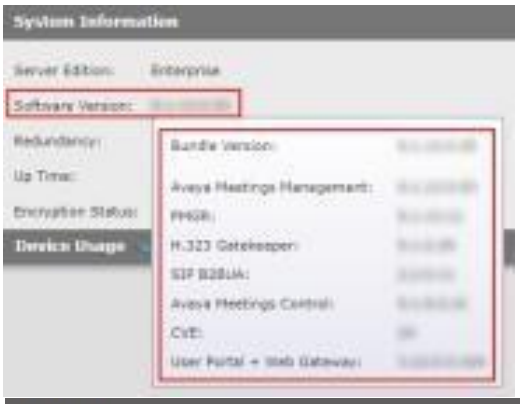
- Deploying Avaya Meetings Server 9.1
- Administering Avaya Meetings Management

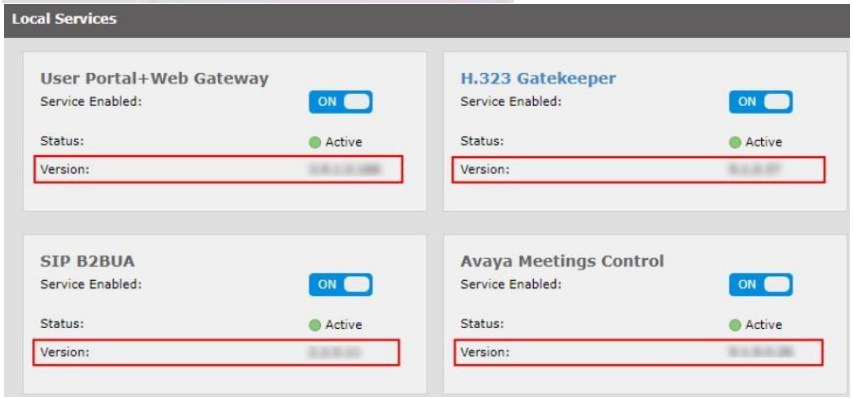
Installing Avaya Meetings Management by full OVA deployment or by Upgrade from the previous version (when applicable):

- Full Deployment of the Avaya Meetings Management should be performed after all other relevant components of the Meetings Solution are deployed and ready for registering with the Meetings Management.
- Upgrade of the Avaya Meetings Management must be performed before any other relevant (registered) components of the Meetings Solution are upgraded. Make sure to upgrade the Meetings Management first.

It is mandatory to perform all installation procedures from a computer located on the same network as your Meetings Management in order to ensure that there are no failures due to network connectivity issues.

Once the Installation procedure has been completed, the versions of the installed components can be checked in the System Information pop-up window in the Meetings Management Dashboard or on the Local Services page: Settings > System Preferences > Local Services.





Upgrading to Avaya Meetings Management 9.1.15 SP1

The Meetings Management version 9.1 FP15 SP1 (9.1.15.1.4) upgrade package supports upgrading from Meetings Management 9.1 FP15 GA releases (Management 9.1.15.0.9 / Bundle 9.1.15.0.6).

If your current environment is 9.1.15.x, earlier 9.1 releases, first upgrade to the above versions, refer to the relevant Release Notes

The Software Upgrade archive downloaded from PLDS (MeetingsMgmt_9_1_15_1_4.zip) contains two files (Management_9.1.15.1.4.zip **and SecurityUpdate_9-1_SSP-015-36**) – those must be extracted and upgrade security patch after upgrading 9.1.15.1.4 SP1. Do not extract them further.

Attempting to install the archive downloaded from PLDS directly will result in an error.

Not-Redundant Deployment (no High Availability and no Geo-redundancy) The required installation order is as follows:

1. Create an image snapshot of the Meetings Management as a backup. Use your company approved procedure for creating the image.
2. Ensure that your Meetings Management is running one of the following versions: 9.1.15 GA (Management 9.1.15.0.9 / Bundle 9.1.15.0.6).
3. Upgrade the Management platform security using the Platform Security Update file SecurityUpdate_9-1_SSP-015-36.zip, if applicable. This file is included in the Meetings Management 9.1 FP15 SP1 archive MeetingsMgmt_9_1_15_1_4.zip.
4. Upgrade the Management application software using the Management_9.1.15.1.4.zip upgrade file. This file is included in the Meetings Management 9.1 FP15 SP1 archive MeetingsMgmt_9_1_15_1_4.zip and upgrades all Management Server application components – Management (iView), H.323 GK (ECS), SIP B2BUA, UCCS and AAWG/Portal.

Redundant Deployment (Including High Availability and optional Geo-redundancy)

For Redundant Deployments (including High Availability and optional Geo-redundancy), the upgrade process must start with the secondary Meetings Management server. This is to ensure that the primary Meetings Management server will be the same server that was primary before the upgrade process.
For the detailed upgrade procedure for this deployment, please see the Administering Avaya Meetings Management guide, chapter 15: Maintaining your Video conferencing Network, sub-section ‘Upgrading, Backing up and Restoring Meetings Management’.

The required installation order is as follows:

1. Create an image snapshot of all the Meetings Management servers as a backup. Use your company approved procedure to create the image.
2. Ensure that your Meetings Management is running one of the following versions: 9.1.15 GA (Management 9.1.15.0.9 / Bundle 9.1.15.0.6).

3. Upgrade the system platform security for both servers using the Platform Security Update file SecurityUpdate_9-1_SSP-015-36.zip, if applicable. This file is included in the Meetings Management 9.1 FP15 SP1 archive MeetingsMgmt_9_1_15_1_4.zip.

4. Upgrade the Management application software for both servers using the Management_9.1.15.1.4.zip upgrade file. This file is included in the Meetings Management 9.1 FP15 SP1 archive MeetingsMgmt_9_1_15_1_4.zip, and upgrades all Management Server application components – Management (iView), H.323 GK (ECS), SIP B2BUA, UCCS, AAWG/Portal.

Security Notes

Note 1: Starting from Meetings Server 9.1.8 release, upgrading will prompt the administrator to change the "admin" user password if the default password has never been changed.

NOTE 2: For migration from a non-fully GDPR data privacy compliant Management server to a fully GDPR data privacy

compliant server, please refer to Release Notes for Avaya Equinox® Management for Equinox® R9.1.9 SP1 (9.1.9.1).
For information about patches and product updates, see the Avaya Technical Support Web site https://support.avaya.com

Full Deployment of Meetings Management 9.1 FP15 SP1

Full deployment of Meetings Management 9.1 FP15 SP1 Virtual Machine uses the 9.1 FP15 OVA.

The archive downloaded from PLDS - MeetingsMgmt_9_1_15_0_OVA.zip (PLDS Download ID EQMNG000915) - contains the Meetings Management virtual machine OVA deployment file Management_9_1_15_0_5.ova.
Extract and deploy the Management_9_1_15_0_5.ova file. It installs all Management Server components and Platform Manager (PMGR) 9.1.14.1.10.
List of supported servers suitable for the Meetings Management OVA can be found in the Avaya Solution Platform (ASP) Offer Definition, which is referred to in the Avaya Meetings Server 9.1.14 Offer Definition.

Note 1: The default login to Meetings Management is: user "admin" and password "meetingsmanagement".
Note 2: Starting with Meetings Server 9.1 FP11 release, for full OVA deployment the default password to access the database has been changed to be a random one, so an end user cannot access the database. If needed, contact the Avaya Support Team.
Note 3: The pmgradmin, root and bios passwords of the newly deployed server must be changed.
Note 4: Starting with Solution 9.1 FP9 Release, for new installations, support for WebRTC Clients requires a WebRTC Gateway. The WebRTC Gateway must be registered with the Meetings Management and be configured to be used as a default front end for the Meetings Media Server.
Refer to the Administering Avaya Meetings Management for details

Migration to Meetings Management 9.1 FP15

Meetings Management 9.1 FP15 employs an upgraded Linux OS version - RHEL 8.10. For this reason, upgrade of older Management deployments to 9.1 FP15 is not possible. Management 9.1 FP15 requires full OVA deployment.

A special Migration Procedure from Management 9.1.14 SP1 to 9.1 FP15 is available. It includes backing up 9.1.14 SP1 info, full OVA deployment of 9.1 FP15 and updating the last with the 9.1.14 SP1 backup info.

Important notes for Migrating from Meetings Management 9.1.14 SP1 to 9.1 FP15:

- This process is only supported for migrating from Meetings Management 9.1.14 SP1 (Bundle 9.1.14.1.11 / Management 9.1.14.1.14) for TE / OTT / MT. If your current environment is 9.0, 9.0.x, 9.1 to 9.1.14, first upgrade to 9.1.14 SP1 release. Refer to the relevant Release Notes.
- There are limitations on what can be restored, for example the Administrator will have to obtain new License Keys.
- Certificates can be saved and restored, given that the IP/FQDN remains the same. If not, the newly installed Meetings Management 9.1 FP15 should be handled as a new device.
- First migrate the components of the deployment (Media Server, distributed AAWG / UCCS / ECS) and only after that migrate the Meetings Management (iView).
- For detailed procedures on how to migrate devices into new VM servers, see Appendix A: How to migrate devices into new VM Servers for Avaya Meetings Server solution.

Full Deployment of Meetings Management 9.1 FP15

Full deployment of Meetings Management 9.1 FP15 Virtual Machine uses the 9.1 FP15 OVA.

The archive downloaded from PLDS - MeetingsMgmt_9_1_15_0_OVA.zip (PLDS Download ID EQMNG000915) - contains the Meetings Management virtual machine OVA deployment file Management_9_1_15_0_5.ova.
Extract and deploy the Management_9_1_15_0_5.ova file. It installs all Management Server components and Platform Manager (PMGR) 9.1.14.1.10.

List of supported servers suitable for the Meetings Management OVA can be found in the Avaya Solution Platform (ASP) Offer Definition, which is referred to in the Avaya Meetings Server 9.1.14 Offer Definition.

Note 1: The default login to Meetings Management is: user “admin” and password “meetingsmanagement”.

Note 2: Starting with Meetings Server 9.1 FP11 release, for full OVA deployment the default password to access the database has been changed to be a random one, so an end user cannot access the database. If needed, contact the Avaya Support Team.

Note 3: The pmgradmin, root and bios passwords of the newly deployed server must be changed.

Note 4: Starting with Solution 9.1 FP9 Release, for new installations, support for WebRTC Clients requires a WebRTC Gateway. The WebRTC Gateway must be registered with the Meetings Management and be configured to be used as a default front end for the Meetings Media Server.

Refer to the Administering Avaya Meetings Management for details.

What's new

Avaya Meetings Management 9.1.15 SP1

Tomcat upgrade:

Meeting Management 9.1.15.1.4 patch is built on top of the 9.1.15 release line and includes partial AEMG (iView) upgrade package. This patch will update tomcat from version 7.0.109 to tomcat version 9.0.109.

Tomcat security updates:
Tomcat vulnerabilities CVE-2025-48989, CVE-2024-24549, CVE-2024-23672 are fixed in this release.

Components Version Information:
AEMG (iView): 9.1.15.1.3

Download archives:
AEMG (iView): MeetingsMgmt_9_1_15_1_4.zip

Mute Feature:

Avaya Meetings Server 9.1 FP15 SP1 introduces an enhancement that allows standard WebRTC (SWC) users to mute other participants in a meeting, including moderators. This feature improves audio control during live sessions where participants may need to manage disruptive background noise without relying solely on moderator privileges.
To enable this capability, specific configuration options must be activated in the Meetings Management (iView) interface. Administrators can turn on mute permission at either the User Level or Profile Level, depending on the desired scope of control:

iView Configuration Requirements:
User-Level Setting:

Navigate to **Users → Select User → Virtual Room Settings and** enable the option:
"**Allow user to mute other participants**."

Profile-Level Setting:

Navigate to Profiles → Select Profile → User Settings and enable the mute permission for all users under that profile.
User-level settings override profile-level configurations, allowing fine-grained control when required. Once enabled, SWC WebRTC clients will display a mute icon next to each participant in the roster, allowing authorized users to mute others directly.
This capability is supported only on SWC WebRTC clients. Avaya Workplace desktop/mobile applications and hardware endpoints (such as J100/C100s) do not support this feature at this time.

Note: The warning message shown during unmute (e.g., "You do not have permission for this action.") is **not changed** in this release.

- If a user is muted by any non-moderator, the muted user will still see the system message **"You were muted by Moderator"**, and the unmute button hover text will continue to show the moderator icon.
- User-Level settings override Profile-Level settings.
- Message behavior will be improved in a future enhancement cycle.

Avaya Meetings Management 9.1 FP15

The following table lists the enhancements and modifications in the Avaya Meetings Management (previously known as Avaya Equinox Management) for Meetings Server Solution 9.1 FP15 and is cumulative since the last major/minor release, showing the most recent release first and oldest release last.

The Avaya Meetings management 9.1.15.0.5 is a feature pack. The base operating system has been upgraded from RHEL 8.4 to RHEL 8.10. This software release implements multiple security vulnerabilities and system stability improvements.

Enhancement / Modification	Description
Operating System	Meetings management 9.1.15 is packaged with RHEL 8.10 OS
Harman Integration:	Avaya Meetings Server 9.1 FP15 implements integration with Harman Media Suite. This integration handles the Recording operations for Meetings hosted by the Meetings Server. The Harman Media Suite is a replacement of the Avaya Streaming and Recording solution. The following Recording operations are supported: • Start Recording • Stop Recording • Pause Recording • Resume Recording More detailed information regarding settings and enabling Avaya Meetings Server-Harman Media Suite integration is provided in the following document: **Harman Media Suite-Avaya Meeting Server Integration** Note: When using Avaya Aura SM with Harman Media Suite a limitation of the CM rule exists, The maximum length of the dial plan rule on the CM is 18 (Virtual room ID+"***"+PIN). Harman would not join a meeting if the respective dial plan rule is longer than 18.

Resolved Issues

Avaya Meetings Management 9.1 FP15 SP1

ID	Visible symptoms
1-23121601340	Mute functionality. Lecturer can be muted by anybody
1-22544559782	Screen share is grayed out / Sharing not available on workplace client when using adhoc call
1-23077109352	Upgrade Utility displays version 8.5 when upgrading to 9.1.14.0.24
1-23183509782	Tomcat bugs found in iView 9.1.14 CVE-2024-24549
1-23183509782	Tomcat bugs found in iView 9.1.14 CVE-2024-23672
1-23121601340	Mute functionality changes. SW changes unification
1-22608433022	Unable to access securely active GEO Management Portal and cannot make Client (WebRTC and Workplace) Calls
1-22999634164	pmgradmin Password expiry forces a password update after 9.1.14 SP1 Upgrade.
1-22990806501	Meeting Customized Arabic Audio Prompt Issue
1-22636850812	Customized Audio prompts are not played properly after failover from Primary to Secondary Management Server
1-23077109352	AMMG 9.1.14.0.17 -- configure 2 session manager servers - take one offline and SIP calls fail
1-22999634164	Media Server 9.1.14 SP1: EASG Command not available in ssh during initial login. Working OK in MS 9.1.14 GA
1-22743977534	Document Sharing on C190 (BFCP) fails
1-22418956322	New Recurring / Overlapping Meetings Scheduling related issues with Management /Portal
ECONF-5614	Meetings can be scheduled with a PIN exceeding 16 digits
ECONF-5606	Cannot escalate from P2P call to Adhoc conference on FedRamp
ECONF-5594	C130,C190,C170 do not leave the meeting right away on meeting server web portal though they left the meeting on their local side
ECONF-5587	C130,C190 and C170 left the meeting automatically after joining approx 4 mins
ECONF-5584	Private chat user list was not showed on IXWP Android in case meeting type is audio service

ECONF-4503	Change of WebRTCStrings field in Text adjustment does not affect on Web client
ECONF-5620	FedRAMP - P3S3 - Cannot save as PDF in Reports on iView
ECONF-5555	Show Name banners option is still checked when sharing screen is viewed mainly although it is un-checked previously
ECONF-5577	SWC user cannot see and take actions on whiteboard if new whiteboard page is added in detach window
ECONF-5548	After the moderator sets the Lecture mode for the meeting, the moderator will hear the prompt "All participants are now muted"
ECONF-5569	Cannot schedule meeting on web portal while location is delegated rooms and recurring is not once only
ECONF-5578	The 'watching the presentation' icon of the user will disappear from the participants list after the moderator changes his name
ECONF-5880	After swapping the view, a gray screen appears. Stopping and starting the Whiteboard again allows making annotations on the small Whiteboard screen after swapping the view once more Workaround: When this issue happens, we need to be terminated the meeting and re-join the meeting again. Then this issue won't be happened.
ECONF-5873	New Recurring / Overlapping Meetings Scheduling related issues with Management /Portal. No popup for meeting time conflicts in same virtual room
ECONF-5867	After stopping event on Harman, the user is not able to take any action on the recording or start/stop recording again, even though the recording is still occurring in the meeting.
ECONF-5863	Harman Recorder is not hidden on Web Portal when iView changes name and Web Portal start recording
ECONF-5860	C100 R1.2.0.1 - VHD cannot join the strong encryption virtual room with SRTP AES-256
ECONF-5883	No user profile is created when adding the second or subsequent organization.
ECONF-5856	Sometimes a warning popup "ResizeObserver loop completed with undelivered notifications." appears after turning video on or off
ECONF-5889	Portal does not display Sort/Filter options or the participant count after starting a meeting
ECONF-5854	VM model of all Media servers change to Flex after applying 9.1.15 SP1 patch
ECONF-5853	Speaker button is pressed on Hide pen when pressing Chat tab or Participant tab on IOS
ECONF-5852	User portal's name is not updated when starting to share whiteboard after changing name
ECONF-5850	FedRAMP mode - Change of WebRTCStrings field in Text adjustment does not effect on Web client
ECONF-5848	The function has been enabled by Profile User but new User can still change the PIN type
ECONF-5847	Mute option for All the Users' does not take effect immediately in the meeting even though the option has been updated in the user
ECONF-5842	Event of Prompt does not load the corresponding folder when triggered in a newly created language
ECONF-5840	Unable to upgrade SSP015-36 one of MCU, error "Upgrade failed - <?xml version='1.0'?><FileHandlingStatus>FileNotUploaded</FileHandlingStatus> "
ECONF-5839	No prompt for meeting auto extend for instant meeting

ECONF-5836	No Avaya meetings Logo in Meetings Invitations in iView
ECONF-5834	Cannot check log Unified Plan on console tab after the meeting starts successful with Audio/Video
ECONF-5832	Display error in Activate Slider when detaching Whiteboard window
ECONF-5830	Nothing is displayed when clicking Audio and Video Check
ECONF-5829	Cannot escalate from P2P call to Adhoc conference with Meeting type Strong Encryption
ECONF-5826	The "Microphone Off" tooltip text on Web Client does not go to a new line after the period
ECONF-5825	Screen share is grayed out when escalating WP P2P Call without Enable Web Collaboration Transcoding
ECONF-5824	Harman Media server 4.3.2 is offline when adding to iView
ECONF-5583	IXWP Android cannot do private chat in case meeting type is audio service. Also, I don't see pop-up chat when new messages came.
ECONF-5568	The 'Slider' button is missing when the participant takes a sharing in the meeting with the Audio and Web Colab meeting type.
ECONF-5534	User details on J1xx/96x1 phones were displayed incorrectly in each time while setting lecturer on meeting portal
ECONF-5219	The recording file only captures audio during the meeting/streaming, excluding screen/whiteboard sharing with AMS-audio web Collab
ECONF-5744	MT system - Unable to update "Can record meetings" option in Custom User Profile for admin tenants User
ECONF-5849	Prompts not played: "The meeting will now begin" and "Welcome to the conference recorder playback service" after Web Client started video meeting
ECONF-5855	Workplace's pop-up should display exactly like Web Portal's 'Your audio has been unmuted' after unmuting itself.s
ECONF-5261	Wrong timezone displayed when exporting recording file

Avaya Meetings Management 9.1 FP15

ID	Visible symptoms
1-22631600216	Web Collab is not working after MCU Patch installation
1-22675570571	After the 30-day Lockout feature locks the admin account there is no possibility to recover it.
1-22060923862	TLS handshake with Media Server after the last was upgraded to 8.0.2.264
1-22047334152	Signed certificate is not installed on the ECS Slave node
1-22049047342	When one date within a scheduled meetings series is cancelled, Outlook receives an email with a cancellation of the entire series

Known Issues and Workarounds

Avaya Meetings Management 9.1 FP15 SP1

Issue	Visible Symptoms
ECONF-5858	The lecture mode stuck when the moderator disconnect the current lecture
ECONF-5822	Upgrade software wizard update incorrect current version of Off-site Backup Server
ECONF-5833	When a web client joins a meeting with the &autojoin parameter and then leaves the meeting, the "auto close in n seconds" message does not appear on the landing page.
ECONF-5888	Failed to apply certificate for MCU.
ECONF-5855	Workplace's popup should display exactly like Web Portal's "Your audio has been unmuted" after unmuting itself

Avaya Meetings Management 9.1 FP15

Issue	Visible Symptoms
ECONF-5621	No contact is shown in the Contact or Terminal when searching.
ECONF-5620	Report cannot be saved as a PDF file in the iView Reports

Avaya Meetings Management 9.1 FP14

Issue	Workaround
In some rare cases, it is not possible to enable a secured connection to AMMS. The following error message is seen: “The trusted intermediate CA certificate for Avaya Meetings Management does not exist. Upload a valid one to Avaya Meetings Management.”	The issue could happen when the AMMG certificate was renewed by different sub CA-s for more than 1 time. The workaround is to remove the old sub CA certificate from the directory /opt/avaya/iview/tomcat/certificate/ca manually. For example, if the old subCA file is intermediate_ca_1.pem, then AMMG will generate a .crt file for it and name it as "intermediate_ca1.cert.crt" and put it under /opt/avaya/iview/tomcat/certificate/ca.
In some rare cases, the Management Server may fail to upgrade the CVE with the following error: “File Not Uploaded”	This may be caused by the space shortage for /tmp directory. Please check the disk space and remove unused files under /tmp directly.
If the MCU password includes special characters, changing it from iView UI will fail.	Make sure the password doesn’t include any of the following characters: “~`%&+:;'",.<>?/\=”
Intermittently, while deploying new solution OVAs including AEMS (High- capacity audio) and WebRTC GW, meetings are not started.	Move AEMS to Maintenance mode and back to normal.
Scheduled recurring Yearly Meetings can be synchronised to the Meetings Management and the Portal but the meeting details would show only one instead of multiple meetings.	

For SNMP V3 Engine ID is not supported	
For FedRAMP deployments: Management Cannot enable FedRAMP mode while on redundancy mode, setup FedRAMP before setting up redundancy. Before setting up redundant AEMG for FedRAMP deployment, replace the self-signed certificates with the certificates signed by third party CA.	
There is a problem to do the certificate replacement from self-signed to third-party CA-signed once the redundancy AEMG has been set up.	
Auto Attendant use cases are not supported with IX workplace clients (Meetings). Client users should either click the meeting call button from the “Next Meeting” list or dial the Virtual Room number directly on the “name and number” pad. The Auto Attendant number should be used by audio devices.	

GDPR data privacy compliancy with secure processing (encryption) of Personal Data: A boot passcode must be provided whenever encryption enabled, while passcode is not required when encryption is disabled. Currently there is no configuration setup constraint to enter the passcode if encryption is Enabled. If the admin does not enter a passcode when enabling encryption, the machine must be deployed without encryption. This validation logic will be added to the OVA deployment in a future release.	
GDPR data privacy compliancy with secure processing (encryption) of Personal Data: If the Remote key server is down, Admin can access the web console of AEMG but cannot enter the passphrase to start AEMG.	
When Admin changes the Elite 6000 MCU configuration and presses the "Apply” button, the operation may result in a pop-up message "The operation failed due to unknown error, contact your system administrator”. This is a false warning message; the configuration will be saved properly.	
H.323 Gatekeeper distributed node in Alternate Mode (HA) a. When breaking H.323 Gatekeeper HA cluster setup (aka Alternate mode) of distributed nodes, the name of each H.323 GK node will be changed to its own IP address (e.g. GK01 is changed to 10.103.3.52) and the Service FQDN of secondary GK will have the service FQDN of Alternate pair (usually it is the one of the primary GK). After such an operation the original names and FQDN’s should be manually restored by the admin. Please refer to Services for the exact solution. b. Renewing Certificates for H.323 Gatekeeper distributed node in Alternate Mode can be applied without breaking the Alternate mode. Please refer to Services for the exact procedure	

The preferred CM configuration for Video Conferencing is **Initial IP-IP Direct Media** enabled, and **Direct IP-IP Audio connection** enabled. There are some known issues related **to Initial IP-IP Direct Media** disabled and **Direct IP-IP Audio connection** enabled on the CM configuration while working with Video Conferencing. If XT or CU360 room systems configured on SM with a CM profile, with the above settings, the CU/XT might get black video when joining meeting via Auto Attendant. Use case where XT/CU devices are invited into the calls may not work, and when placed in a waiting room, the waiting prompt is delayed.	A way to overcome this is to enable IP-IP Direct Media or configure the XT/CU on SM without a CM profile.
If new users are added to Meetings Server in TE deployments after a change is applied to the Meetings configuration (example a profile change which impacts all users), those new users will be delayed in becoming available for login on the portal. The reason for this is that the original Meetings changes are still being processed, and the new user data is queued up to be pushed to the Portal.	Either add the new users prior to making any configuration changes, or have the new users try again in a few hours. The actual wait time will depend upon many factors, such as system size and existing user count.
H.323 video endpoints cannot connect to High-Capacity Audio Media server which is SIP only.	

Meetings Management cannot manage Scopia Elite 5000 series MCU audio prompts.	If prompts customization is needed, admin can access Scopia Elite 5000 MCU admin GUI to perform the customization.

Using Internet Explorer 11, we recommend adding the Meetings Management URL as well as the Google Maps URLs as trusted sites.	Refer to Make Google Maps load faster for detailed instructions.
When a meeting has more than 300 participants, we recommend using a PC with a high spec PC (Memory is 4 GB or higher and the CPU pass mark should be higher than 6000) to operate the in-meeting control.	
Admins cannot move a participant from one meeting to another for the following endpoints: · Telepresence endpoints · Lync clients · Meetings Clients with Web Collaboration. · WebRTC clients. · SIP call that joined the High Audio Capacity Media server.	
The administrator portal supports the following languages: English, French, Simplified Chinese and Japanese. Some events/alarms messages remain in English because they come from other devices / endpoints.	
AAWG Cores displays UTC time instead of displaying configured NTP time GMT. That is actually the correct time. Both offsets are correct. It is confusing, Linux and Meetings Management use two different methods to show the relative offset from GMT. See here: https://www.gnu.org/software/libc/manual/html_node/TZ-Variable.html Basically, one format tells you how far behind UTC you are (-), while the other tells you how many hours to add to be the same as UTC (+). Two different ways to get the same result. So, in this case they should have the opposite sign, but the same absolute value. For example, I am in GMT minus 6 hours. So, GMT-6=my correct local- time. Linux system shows the correct time, just using the notation +6, indicating I add 6 to my time to get GMT. [root@PMGR pmgradmin]> date --utc Thu Nov 3 18:51:50 UTC 2016 [root@PMGR pmgradmin]> date Thu Nov 3 12:51:59 GMT+6 2016 [root@PMGR pmgradmin]>	
TLS1.2 can't be correctly set in Redundancy setup	To enable/disable the TLS1.2, as a workaround, you should follow the steps as following: 1. Power off one node 2. Enable/Disable TLS1.2 in active node and required a restart 3. After this node starts, power off this node and power on another node 4. Enable/Disable TLS1.2 in active node and required a restart 5. After this node starts, power on another node
Meetings Client and CU360 on P2P, EC start sharing to escalate to ad- hoc meeting, CU360 start presenting then CU360 is dropped immediately when he starts sharing in ad-hoc meeting. Issue doesn't happen when CU360 dials to meeting directly.	

Documentation Note

Please note that in the “Port Security for the Equinox Conferencing 9.x Solution” the bidirectional ports to open on the Firewall for the Avaya Meetings (Equinox) Media Server are specified incorrectly. The actual RTP / RTCP / SRTP (UDP) port range to be opened is 12000-13599 and not 12000-13200.

Supported Languages

The supported languages for audio messages are those covering the G14 countries:

English (U.K.), English (U.S.), Spanish, French, French (Canadian), Italian, Japanese, Korean, Portuguese, Russian, Simplified Chinese, German.

The supported languages for video messages are:

English, Chinese, Traditional Chinese, Japanese, Korean, Hebrew, French, Thai, German.

Contacting support

Contact Support Checklist

If you are having trouble with **Avaya Equinox Media Server Version 9.1.x**, you should:

1. Retry the action. Carefully follow the instructions in the written or the online documentation.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.

If you continue to have a problem, contact Avaya Technical Support:

1. Log in to the Avaya Technical Support Web site https://support.avaya.com.
2. Contact Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information refer to the Escalation Contacts listings on the Avaya Web site.

Contact Support Tasks

You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

Appendix A: How to migrate devices into new VM Servers for Avaya Meetings Server solution?

This procedure was tested and is approved for 9.1.13 SP1 deployments migrating to 9.1.14.

Before proceeding, ensure your system is running release 9.1.3 SP1. If your current environment is 9.0, 9.0.x, 9.1 to 9.1.13, first use the relevant RN to upgrade to this release.

IMPORTANT NOTES:

- The Meetings Server components which require migration into new VM servers are:

- Meetings Management
- Distributed AAWG (Management Node)
- Distributed UCCS (Management Node)
- Distributed ECS (Management Node)
- Meetings Media Server

- First migrate the other components in the deployment (Media Server, distributed AAWG/UCCS/ECS), and only then migrate Meetings Management (iView).

- This procedure was tested and is approved for 9.1.13 SP1 deployments migrating to 9.1.14.

Migration for Distributed AAWG (OTT deployment)

Prerequisites:

- Before the migration, make sure the single AAWG (or cluster) is working fine and no alarms are displayed on the Meetings Management dashboard.
- Make note of the current IP address and FQDN used for all AAWG nodes. The IP address and the FQDN used for each newly deployed AAWG should be the same as is used for the existing AAWGs.
- Create a VM backup/snapshot, and make sure the target host has **ESXi 7.0.3 and above**.
- The procedures apply to all the nodes in the AAWG cluster, but the Seed Node should be the first one migrated.
- The admin can tell which node is the seed node via the advanced parameter **com.avaya.iview.esg.seednode.ip** in Meetings Management.

Procedure:

1. Update the Meetings Management advanced parameter **com.avaya.iview.esg.seednode.ip** to an invalid IP address such as "192.168.1.1".
2. SSH to the old VM with "root" user and manually back up all the certificates into a zip file named **certs.tar.gz** using the following command: "**tar czvf certs.tar.gz /opt/avaya/pmgr/.cert**".
3. Copy the cert file **certs.tar.gz** out of the server (with sFTP / winSCP). You may need to copy the file from /root to /home/pmgradmin directory (cp /root/certs.tar.gz /home/pmgradmin), and chmod 777 to be able to copy it out of the server with WinSCP.
4. Shutdown the old VM.
5. Deploy a new VM and configure the network settings (IP address, subnet mask, default GW, DNS Server and NTP settings) to be the same as were used for the old AAWG.
6. Power on the new VM.
7. SSH to the new VM with "root" user, then extract the cert file **certs.tar.gz** (the file generated in Step #2) with the following command: "**tar xvf certs.tar.gz -C /**".
8. In the SSH console, execute the following copy command: "**cp /opt/avaya/pmgr/.cert/PlatformCertFile.pem /etc/nginx/cert.pem**".
9. In the Meetings Management UI, navigate to the **Configuration** tab of the distributed AAWG, check and make sure that the NTP and DNS are well configured. If they are not, input the correct NTP and DNS and then click "Apply".
10. In the Meetings Management UI, when the node is available and an alarm for applying license is showing, navigate to **Devices** > **User Portals** and apply a new license for this AAWG node.
11. Update the Meetings Management advanced parameter **com.avaya.iview.esg.seednode.ip** to the correct IP address (the IP address of the first AAWG added into Meetings Management).

12. Normally, Meetings Management will start the AAWG installation automatically once the above steps are completed. The whole installation process will continue for about 10 minutes. When the installation has completed, repeat the above procedures for the subsequent nodes.
13. In the Meetings Management UI, navigate to **Settings** > **Devices** > **AAWG / User Portal** and then click "Apply".

Migration for Distributed ECS (H.323 Gatekeeper)

Prerequisites:

- Before the migration, make sure the ECS server is working fine, and no alarms are displayed on the Meetings Management dashboard.
- Make note of the current IP address and FQDN used for all ECS nodes. The IP address and the FQDN used for each newly deployed ECS should be the same as is used for the existing ECS server.

Create a VM backup/snapshot, and make sure the target host has **ESXi 7.0.3 and above**.

Procedure:

1. SSH to the old VM with "pmgradmin" user then switch to "root" user and manually back up all the certificates into a zip file named **certs.tar.gz** using the following commands:
   - "**tar czvf certs.tar.gz /opt/avaya/pmgr/. cert"**
   - **"chmod 644 certs.tar.gz"**
2. Copy the cert file **certs.tar.gz** out of the server (with sFTP / winSCP).
3. Shutdown the old VM.
4. Deploy a new VM and configure the network settings (IP address, subnet mask, default GW, DNS Server and NTP settings) to be the same as were used for the old ECS server.
5. Power on the new VM.
6. In the Meetings Management UI, when the ECS Server is online and an alarm for applying for a license is showing, navigate to **Devices** > **H.323 Gatekeepers** and apply for a new license for this ECS.
7. SSH to the new VM with "pmgradmin" user then switch to "root" user.
8. Copy the cert file **certs.tar.gz** (the file generated in Step #1) into the new VM (with sFTP / winSCP), then extract it with following commands:
   - "**tar xvf certs.tar.gz -C /**"
   - "**/opt/avaya/ECS/external-scripts/update-certificate 1 3 /opt/avaya/pmgr/.cert/PlatformCertFile.pem /opt/avaya/pmgr/.cert/PlatformCAFile.pem**"
9. In the Meetings Management UI, navigate to **Devices** > **H.323 Gatekeepers**, then select the ECS > **Configuration** > Input "**NTP Server**" > uncheck "**Secure Connection**" > click "**Apply**".
10. Once the ECS server has no alarms and its status is green, go to its Configuration tab > check "**Secure Connection**" (also firstly click "**Test Connection**") > click "**Apply**".

Migration for Distributed UCCS

Prerequisites:

- Before the migration, make sure the UCCS server is working fine, and no alarms are displayed on the Meetings Management dashboard.
- Make note of the current IP address and FQDN used for all UCCS nodes. The IP address and the FQDN used for each newly deployed UCCS should be the same as is used for the existing UCCS server.
- Create a VM backup/snapshot, and make sure the target host has **ESXi 7.0.3 and above**.

Procedure:

1. SSH to the old VM with "pmgradmin" user then switch to "root" user and manually back up all the certificates into a zip file named **certs.tar.gz** using the following commands:
   - "**tar czvf certs.tar.gz /opt/avaya/pmgr/.cert"**
   - **"chmod 644 certs.tar.gz"**
2. Copy the cert file **certs.tar.gz** out of the server (with sFTP / winSCP).
3. Shutdown the old VM.
4. Deploy a new VM and configure the network settings (IP address, subnet mask, default GW, DNS Server and NTP settings) to be the same as were used for the old UCCS server.
5. Power on the new VM.
6. In the Meetings Management UI, when the UCCS server is online and an alarm for applying license is showing, navigate to **Devices** > **UCCS Servers** and apply a new license for this UCCS.
7. SSH to the new VM with "pmgradmin" user then switch to "root" user,
8. Copy the cert file **certs.tar.gz** (the file generated at Step #1) into the new VM (with sFTP / winSCP), then extract it with following commands:
   - "**tar xvf certs.tar.gz -C /**"
   - "**/opt/avaya/uws/external-scripts/update-certificate 1 3 /opt/avaya/pmgr/.cert/PlatformCertFile.pem /opt/avaya/pmgr/.cert/PlatformCAFile.pem**"
9. Then in the SSH console, execute the following copy command:
   "**cp /opt/avaya/pmgr/.cert/PlatformCertFile.pem /etc/nginx/cert.pem"**
10. In the Meetings Management UI, navigate to **Settings** > **Maintenance** > **Log** > Change "**Log Level**" to a different value > Click "Apply". Wait for about 5 minutes and then change the log level back if needed.

Migration for Media Server

Prerequisites:

- Before the migration, ensure the Media Server is working fine and no alarms are displayed on the Meetings Management dashboard.
- Make note of the current IP address and FQDN used for the Media Server. The IP address and the FQDN used for each newly deployed Media Server should be the same as is used for the existing Media Server.
- Create a VM backup/snapshot, and make sure the target host has **ESXi 7.0.3 and above**.

Procedure:

1. SSH to the old VM with "pmgradmin" user then switch to "root" user and manually back up all the certificates into a zip file named **certs.tar.gz** using the following commands:
   - "**tar czvf certs.tar.gz /opt/avaya/pmgr/.cert**"
   - "**chmod 644 certs.tar.gz**"
2. Copy the cert file **certs.tar.gz** out of the server (using sFTP / winSCP).
3. In the Meetings Management UI, navigate to **Devices** > **Media Servers**, then select the Media Server > **Manage** > **Retrieve Configuration File** > **Ok** to back-up the configuration (**note this step is only needed for Media Server with Full Video mode**).
4. Write down the Public/Service FQDN, Public URL branch, NTP and DNS settings.
5. Shutdown the old VM.
6. Deploy a new VM and configure the network settings (IP address, subnet mask, default GW, DNS Server and NTP settings) to be the same as were used for the old Media Server.
7. Power on the new VM.
8. Wait about 10 min after the server starts until all installation scripts are completed.
9. SSH to the new VM with "pmgradmin" user then switch to "root" user. Extract the cert file **certs.tar.gz** (the file generated in Step #1) using the following commands:
   a. If the Media Server is working in High-Capacity Audio mode, then you need to check if AAMS has

completed the initialization by running following command:

- "service avaya.mediaserver status"
- Repeat the command until it shows "**Active: Active (Running)**", then proceed with the procedure.

b. Copy the cert file **certs.tar.gz** (the file generated in Step #1) into the new VM (using sFTP / winSCP), then extract it using the following commands:

- "**tar xvf certs.tar.gz -C /**"
- "**/opt/avaya/WCS/external-scripts/update-certificate 1 3 /opt/avaya/pmgr/.cert/PlatformCertFile.pem /opt/avaya/pmgr/.cert/PlatformCAFile.pem**"
- "**/opt/avaya/aams/external-scripts/update-certificate 1 3 /opt/avaya/pmgr/.cert/PlatformCertFile.pem /opt/avaya/pmgr/.cert/PlatformCAFile.pem**"
- "**reboot**"

c. Make a backup of the following files, put them in a safe place like /tmp or /root or /home/pmgradmin:
/opt/avaya/WCS/data/java.security.fips
/opt/avaya/WCS/data/java.policy.fips

10. In the Meetings Management UI, when the Media Server is available and an alarm for applying license is showing, navigate to **Devices** > **Media Servers** and apply a new license for this Media Server.
    a. If an 'admin' password was set in the Management Server, different from the one set on the new OVA, an alarm message "The username and password for this device does not match the one defined in Avaya Meetings Management" will appear. To recover, the admin should navigate to the Media Server's "Access" tab and click "Change Password".
11. Verify that the Public/Service FQDN, Public URL branch, NTP and DNS Servers were restored correctly - if not, manually update them according to the capture from Step #4 (device will be restarted automatically).
12. When the Media Server is connected without any alarms displayed, navigate to **Devices** > **Media Servers**, then select the Media Server > **Manage** > **Update Configuration File**, select the latest file to update, then click **Ok** to restore the configuration (**note this step is only needed for Media Server with Full Video mode**).
13. New for 9.1.14 AEMS/WCS: SSH to the new VM with "pmgradmin" user then switch to "root" user.
    a. Copy the files **java.security.fips** and **java.policy.fips** from the temporary location back to original location
    /opt/avaya/WCS/data/java.security.fips
    /opt/avaya/WCS/data/java.policy.fips
    b. Reboot.
14. Wait a few minutes for the Media Server to return to a connected state. If a "The web collaboration service is not available" alarm is displayed, disable/enable the **"Secure Connection"** to clear this alarm.
    a. Go to the Media Server's configuration tab, **uncheck** the **"Secure Connection"** box and click **Apply**. After that, the device will be restarted automatically. Wait a few minutes for the Media Server to return to a connected state.
    b. Go to the Media Server's configuration tab, **check** the **"Secure Connection"** box and click **Apply**. After that, the device will be restarted automatically. Wait a few minutes for the Media Server to return to a connected state.

Migration for Meetings Management

Prerequisites:

- Before the migration, make sure ALL other components of the deployment have been migrated completely.

- Make note of the current IP address, subnet mask, default GW and FQDN used for the Management server. The IP address, subnet mask, default GW and FQDN used for each newly deployed Management server should be the same as is used for the existing Management server.

- Create a VM backup/snapshot, and make sure the target host has **ESXi 7.0.3 and above**.

Procedure:

1. Backup Meetings Management database and configuration files from Meetings Management admin UI by following standard backup procedures.
2. If there are customized audio prompts or brandings applied to the current Meetings Management, these will need to be backed up using the following manual procedures.
    a. SSH to the current Meetings Management server with "pmgradmin" user, then switch to "root" and run the following commands:

        - "**tar czvf customdata.tar.gz /opt/avaya/iview/tomcat/webapps/iview/resources/prompts/new_language/ /opt/avaya/iview/tomcat/webapps/iview/resources/prompts/customized/ /opt/avaya/iview/tomcat/webapps/iview/resources/branding**"
        - **"chmod 644 customdata.tar.gz**"

    b. Copy the **customdata.tar.gz** out of the server (using sFTP/WinSCP).
3. Shutdown the Meetings Management server.
4. Deploy the new VM(s) and configure the network settings (IP address, subnet mask, default GW, DNS Server and NTP settings) to be the same as were used for the old Management server.
5. Input new license to activate the new Meetings Management server.
6. For all-in-one deployments with AAWG included in the Management Server installation, wait until the local AAWG is successfully installed by checking the status from **Settings** > **System Preferences** > **Local Services**.
7. SSH to the new VM with "pmgradmin" user, then switch to "root" user. Extract the **customdata.tar.gz** file (the file generated in Step #2) using the following command:
    - "**tar xvf customdata.tar.gz -C /**"
    - "**reboot"**
8. Switch to Fedramp (or JITC) if the original deployment is Fedramp or JITC.
9. Setup redundancy if the original deployment is a redundancy deployment.
10. Restore the original backup file into the new master Meetings Management following standard restoring procedures.