Avaya Meetings® Media Server for Meetings® Server R9.1 FP15 (9.1.15.0.5)

Release Notes

Avaya Meetings® Media Server
Version 9.1.15.0.5
for Meetings® Server R9.1 FP15

May 2025

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

http://support.avaya.com

Document changes

Date	Description
18-4-2025	First Release of the document
17-9-2025	Content Updated

Introduction

This document provides late-breaking information to supplement **Avaya Meetings® Media Server** 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/P1778/avaya-meetings-media-server/9.1.x.

Note: Prior to Release 9.1 FP11, this product is called Avaya Equinox® Media Server.

Installation

Product compatibility

At the time of this publication, Avaya Meetings Media Server 9.1.15.0.5 for Meetings® Server R9.1 FP15 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 C	Version
Avaya Meetings Management Bundle	9.1.15.0.6 Bundle 9.1.15.0.9 (Management) 9.1.0.40 (GK) 2.2.0.12 (SIP B2BUA) 9.1.15.0.3 (UCCS) 10.2.0.0.30(Portal/AAWG) 9.1.14.1.10 (PMGR)
Avaya Meetings Media Server Bundle	9.1.15.0.5 Bundle 9.1.15.0.108 (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:	3.39.0.137 3.39.0.137 3.39.0.137 3.39.0.137
ASBCE	FIPS Fedramp Deployments – 8.0.1.0-10-17555 Commercial Deployments – 8.1.3.0-31-21052
AAWG for TE Deployments	10.2.0.0.30
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

WebRTC Web Client compatibility

WebRTC calls must be routed through the Avaya WebRTC Gateway before reaching the Meetings Media Server.

This significantly improves the system stability and the video quality of the WebRTC calls.

- For OTT deployments: Use the Avaya Meetings Management configuration UI:

  Verify and ensure that the Advanced Setting "**com.avaya.aawg.aemsWebrtcCapability**" is set to "**false**".

- For TE deployments: Refer to "Configuring WebRTC media adaptation" in Administering the Avaya Aura® Web Gateway.

Installation Overview

Avaya Meetings Media Server 9.1.15 is available as a Virtualized Software OVA.

The OVA is a virtualization format with the Linux Red Hat 8.10 operating system and can be deployed 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 OVA's is permitted and recommended. See the Avaya Solutions Platform 130 Series iDRAC9 Best Practices.

Required patches

No patches are required for the 9.1.15 version.

However once the above version is deployed and the Media Server is registered with Meetings Management, the Media Server must be upgraded with Security Update package SSP-015-29.

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 Media Server

GDPR

For the Meetings Media Server, Meetings Recording Gateway, and Meetings H.323 Edge, a properly upgraded system will be fully GDPR compliant.

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

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

Once the Installation procedure has been completed and the Media Server is properly registered with Meetings Management the versions of the installed components can be checked in the "Software version" field of the Meetings Management web interface: Devices -> Media Servers.

Migration to Avaya Meetings Media Server 9.1 FP15

Meetings Media Server 9.1 FP15 employs an upgraded Linux OS version – RHEL 8.10. For this reason, upgrading of older Media Server deployments to 9.1 FP15 is not possible. Media Server 9.1 FP15 requires full OVA deployment.

A special Migration Procedure from Media Server 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 Media Server 9.1.14 SP1 to 9.1.15:

- This process is only supported for migrating from Meetings Media Server 9.1.14 SP1 (Bundle 9.1.14.1.5 / MCU 9.1.14.1.104) for TE / OTT. If your current environment is 9.1.14 GA or older, first use the relevant RN to upgrade to the 9.1.14 SP1 Release.
- 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 Media Server 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 B: How to migrate devices into new VM Servers for Avaya Meetings Server solution.

Full Deployment of Avaya Meetings Media Server 9.1 FP15

Full deployment of a Meetings Media Server 9.1 FP15 Virtual Machine uses the 9.1 FP15 OVA

- Extract the MediaServer_9_1_15_0_5.ova file from PLDS archive MeetingsMediaServer_9_1_15_0_OVA.zip (PLDS Download ID **EQMS0000915**) and then use it to deploy the Meetings Media Server Virtual Machine. Attempting to install archives downloaded from PLDS directly will result in an error.
- After the deployment of the OVA no additional installation actions are required for the Media Server.

Full Deployment of Avaya Meetings Media Server 9.1 FP14

Full deployment of a Meetings Media Server 9.1 FP14 Virtual Machine uses the 9.1 FP14 OVA**.**

- Extract the MediaServer_9_1_14_0_6.ova file from PLDS archive MeetingsMediaServer_9_1_14_0_OVA.zip (PLDS Download ID EQMS0000914) and then use it to deploy the Meetings Media Server Virtual Machine. Attempting to install archives downloaded from PLDS directly will result in an error.
- After the deployment of the OVA no additional installation actions are required for the Media Server.

Upgrading to Avaya Meetings Media Server 9.1 FP13

The Meetings Media Server version 9.1 FP13 (9.1.13.0.13) upgrade package supports upgrading from Meetings Media Server 9.1 FP12 releases [9.1.12 Log4j Security Update (Bundle 9.1.12.0.9 / WCS 1.2.7.9.4), 9.1.12 (9.1.12.0.9)] and 9.1 FP11 releases [9.1.11 Log4j Security Update (Bundle 9.1.11.0.23 / WCS 1.2.7.4.9), 9.1.11 SP1 (9.1.11.0.23), 9.1.11 (9.1.11.0.20)] via the Meetings Management (iView) UI.

If your current environment is 9.0, 9.0.x, 9.1 to 9.1.10.x, first use the relevant RN to upgrade to one of the above versions.

The upgrade is performed using the contents of 2 archives downloaded from PLDS:

1. Security Update: **SecurityUpdate_9-1_CVE-24-0.zip** update file is included in the Meetings Management 9.1 FP13 archive **MeetingsMgmt_9_1_13_0.zip** (PLDS Download ID EQMNG000032).
2. Media Server: **MeetingsMediaServer_9_1_13_0.zip** archive (PLDS Download ID EQMS0000027) contains the

MediaServer_9_1_13_0_13.zip.

Both files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required upgrade order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Meetings Management server has been upgraded to version 9.1 FP13 (9.1.13.0.25) before you start the upgrade of the Media Server.
3. Ensure that your Meetings Media Server is running one of the following versions: 9.1.12 Log4j Security Update (Bundle 9.1.12.0.9 / WCS 1.2.7.9.4), 9.1.12 (9.1.12.0.9), 9.1.11 Log4j Security Update (Bundle 9.1.11.0.23 / WCS 1.2.7.4.9), 9.1.11 SP1 (9.1.11.0.23), 9.1.11 (9.1.11.0.20).
4. Upgrade the Media Server platform security using the Platform Security Update file SecurityUpdate_9-1_CVE-24-0.zip. This file is included in the Meetings Management 9.1 FP13 archive MeetingsMgmt_9_1_13_0.zip.
5. Upgrade the Media Server application software using the MediaServer_9_1_13_0_13.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Meetings Management Server User Interface.

Full Deployment of Avaya Meetings Media Server 9.1 FP13

Full deployment of a Meetings Media Server 9.1 FP13 Virtual Machine uses the 9.1 FP13 OVA.

- Extract the MediaServer_9_1_13_0_13.ova file from PLDS archive MeetingsMediaServer_9_1_13_0_OVA.zip (PLDS Download ID EQMS0000912) and then use it to deploy the Meetings Media Server Virtual Machine. Attempting to install archives downloaded from PLDS directly will result in an error.
- After the deployment of the OVA no additional installation actions are required for the Media Server.

Upgrading to Avaya Meetings Media Server 9.1 FP12

The Meetings Media Server version 9.1 FP12 (9.1.12.0.9) upgrade package supports upgrading from 9.1 FP11 SP1 (9.1.11.0.23), 9.1 FP11 (9.1.11.0.20) and 9.1 FP10 (9.1.10.0.9) via the Meetings Management (iView) UI.

If your current environment is 9.0, 9.0.x, 9.1 to 9.1.9.1, first use the relevant RN to upgrade to one of the above versions.

The upgrade is performed using the contents of 2 archives downloaded from PLDS:

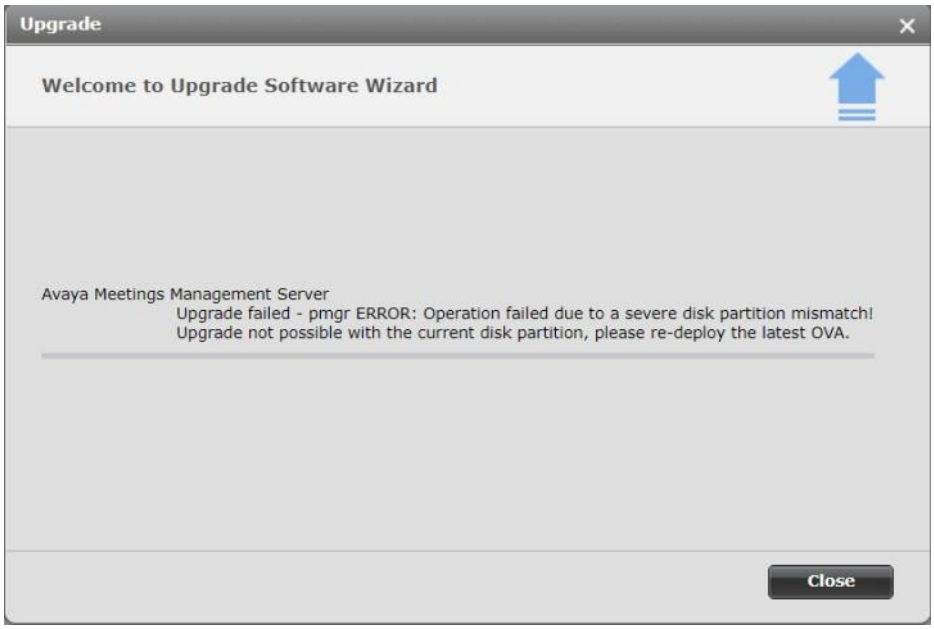
1. Security Update: SecurityUpdate_9-1_CVE-21-1.zip update file is included in the Meetings Management 9.1 FP12 archive MeetingsMgmt_9_1_12_0.zip.
2. Media Server: MeetingsMediaServer_9_1_12_0.zip archive contains the MediaServer_9_1_12_0_41.zip. Both files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required upgrade order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Meetings Management Server has been upgraded to version 9.1 FP12 (9.1.12.0.41) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version 9.1 FP11 SP1 (9.1.11.0.23), 9.1 FP11 (9.1.11.0.20) or 9.1 FP10 (9.1.10.0.9).
4. Upgrade the Media Server platform security using the Platform Security Update file SecurityUpdate_9-1_CVE-21-1.zip. This file is included in the Meetings Management 9.1 FP12 archive MeetingsMgmt_9_1_12_0.zip.
5. Upgrade the Media Server application software using the MediaServer_9_1_12_0_41.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Meetings Management Server User Interface.

Important Notes:

1. Starting from 9.1 FP11, the CVE upgrade with this release ***must*** come first, before the application upgrade.
2. The CVE installation script will check the size of the free space on the boot partition, and if there is more than **100M ('df -h' command)** of **free space**, it will continue to execute.
    - If there is less, the script will automatically attempt to clean up any old kernels.
    - If it fails to clean or there is not enough space, a failure message will be sent, and presented on the Management UI, requesting the admin to re-deploy the new OVA.



    This will happen with older systems that were upgraded from **9.0.x**, where the boot partition on RH 6.7 was even smaller (**~150M**).

3. In case **re-deployment is needed**, there is a procedure to back up the data and restore it onto the new OVA.
    - There are limitations on what can be restored, for example the admin will have to obtain new license keys.
    - Certificates can be saved and restored, given that the IP/FQDN remains the same. If not, it should be handled as a new device.
    - Re-deployment sequence:
        - Use “df -h” command to check the size of the free spaces on the boot partition. If the free space is less than 100M, the component will likely need redeployment.
        - If both Media Server and Management (iView) server require you to re-deploy the OVA, **first migrate the Media Server**, and only then migrate the Management (iView) server.
        - If the Media Server requires you to re-deploy the OVA, but the Management (iView) server does not, **first upgrade the Management (iView) server** as usual, and only then migrate the Media Server.
        - If the Media Server does not require re-deployment, but the Management (iView) server does, **first migrate the Management (iView) server,** and only then continue upgrading the Media server following the above detailed order.
        - For detailed procedures on How to migrate devices into new VM servers, see Appendix B: How to migrate devices into new VM Servers for Avaya Meetings Server solution.

Full Deployment of Avaya Meetings Media Server 9.1 FP12

Full deployment of a Meetings Media Server 9.1 FP12 Virtual Machine uses the 9.1 FP12 OVA.

- Extract the MediaServer_9_1_12_0_9.ova file from PLDS archive MeetingsMediaServer_9_1_12_0_OVA.zip, and then use it to deploy the Meetings Media Server Virtual Machine.
- Attempting to install archives downloaded from PLDS directly will result in an error.
- After the deployment of the OVA no additional installation actions are required for the Media Server.

Upgrading to Avaya Meetings Media Server 9.1 FP11

The Meetings Media Server version 9.1 FP11 (9.1.11.0.20) upgrade package supports upgrading from 9.1 FP10 (9.1.10.0.9) and 9.1 FP9 SP1 (9.1.9.1.12) via the Meetings Management (iView) UI.

If your current environment is 9.0, 9.0.x, 9.1 to 9.1.9.1, first use the relevant RN to upgrade to one of the above versions.

The upgrade is performed using the contents of 2 archives downloaded from PLDS:

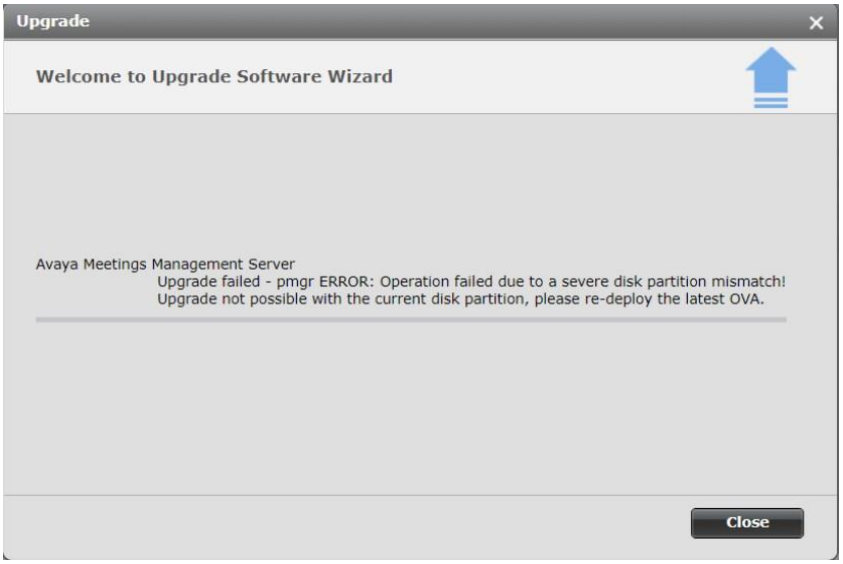
1. Security Update: SecurityUpdate_9-1_CVE-18-2.zip update file is included in the Meetings Management 9.1 FP11 archive MeetingsMgmt_9_1_11_0.zip.
2. Media Server: MeetingsMediaServer_9_1_11_0.zip archive contains the MediaServer_9_1_11_0_20.zip. Both files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required upgrade order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Meetings Management Server has been upgraded to version 9.1 FP11 (9.1.11.0.69) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version 9.1 FP10 (9.1.10.0.9) or 9.1 FP9 SP1 (9.1.9.1.12).
4. Upgrade the Media Server platform security using the Platform Security Update file SecurityUpdate_9-1_CVE-18-2.zip. This file is included in the Meetings Management 9.1 FP11 archive MeetingsMgmt_9_1_11_0.zip.
5. Upgrade the Media Server application software using the MediaServer_9_1_11_0_20.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Meetings Management Server User Interface.

Important Notes:

1. Unlike previous upgrades, the CVE upgrade with this release ***must*** come first, before the application upgrade.
2. The CVE installation script will check the size of the free space on the boot partition, and if there is more than **100M ('df -h' command)** of **free space**, it will continue to execute.
   - If there is less, the script will automatically attempt to clean up any old kernels.
   - If it fails to clean or there is not enough space, a failure message will be sent, and presented on the Management UI, requesting the admin to re-deploy the new OVA.



This might happen with older systems that were upgraded from **9.0.x**, where the boot partition on RH 6.7 was even smaller (**~150M**).

3. In case **re-deployment is needed**, there is a procedure to back up the data and restore it to the new OVA.

• There are limitations on what can be restored, for example the admin will have to obtain new license keys.

• Certificates can be saved and restored, given that the IP/FQDN remains the same. If not, it should be handled as new device.

• Re-deployment sequence:

• Use “df -h” command to check the size of the free spaces on the boot partition. If the free space is less than 100M, the component will likely need redeployment.

• If both Media Server and Management (iView) server require you to re-deploy the OVA, **first migrate the Media Server**, and only then migrate the Management (iView) server.

• If the Media Server requires you to re-deploy the OVA, but the Management (iView) server does not, **first upgrade the Management (iView) server** as usual, and only then migrate the Media Server.

• If the Media Server does not require re-deployment, but the Management (iView) server does, **first migrate the Management (iView) server**, and only then continue upgrading the Media server following the above detailed order.

• For detailed procedures on How to migrate devices into new VM servers, see Appendix B: How to migrate devices into new VM Servers for Avaya Meetings Server solution.

Full Deployment of Avaya Meetings Media Server 9.1 FP11

Full deployment of a Meetings Media Server 9.1 FP11 Virtual Machine uses the 9.1 FP11 OVA.

• Extract the MediaServer_9_1_11_0_21.ova file from PLDS archive MeetingsMediaServer_9_1_11_0_OVA.zip, and then use it to deploy the Meetings Media Server Virtual

Machine.

• Attempting to install archives downloaded from PLDS directly will result in an error.

• After the deployment of the OVA no additional install actions are required for the Media Server

Upgrading to Equinox Media Server 9.1 FP10

The Equinox Media Server version 9.1 FP10 (9.1.10.0.9) upgrade package supports upgrading from 9.1 FP9 (9.1.9.0.8) and 9.1 FP9 SP1 (9.1.9.1.12) via the Equinox Management (iView) UI.

If your current environment is 9.0, 9.0.x, 9.1 to 9.1.8, first use the relevant RN to upgrade to one of the above versions.

Install security patches by using SecurityUpdate_9-1_CVE-14-0.zip after upgrading the Media Server to version 9.1.10.0.9. The upgrade is performed using the contents of 2 archives downloaded from PLDS:

1. Media Server: EquinoxMediaServer_9_1_10_0.zip archive contains the MediaServer_9_1_10_0_9.zip upgrade file.
2. Security Update: SecurityUpdate_9-1_CVE-14-0.zip update file is included in the Equinox Management 9.1 FP10 archive EquinoxMgmt_9_1_10_0.zip.

Both files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required upgrade order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Equinox Management Server has been upgraded to version 9.1 FP10 (9.1.10.0.47) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version 9.1 FP9 SP1 (9.1.9.1.12) or 9.1 FP9 (9.1.9.0.8).
4. Upgrade the Media Server application software using the MediaServer_9_1_10_0_9.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Equinox Management Server User Interface.
5. Upgrade the Media Server platform security using the Platform Security Update file SecurityUpdate_9-1_CVE-14-0.zip. This file is included in the Equinox Management 9.1 FP10 archive EquinoxMgmt_9_1_10_0.zip.

NOTE: WARNING!

The procedure to move from non-Secure to Secure Connection is as follows:

1. Test the TLS connection
2. Wait for 5 min.
3. Click the “Apply” button to switch to Secured Connection

Full Deployment of Equinox Media Server 9.1 FP10

Full deployment of an Equinox Media Server 9.1 FP10 Virtual Machine uses the 9.1 FP10 OVA.

- Extract the MediaServer_9_1_10_0_9.ova file from PLDS archive EquinoxMediaServer_9_1_10_0_OVA.zip, and then use it to deploy the Equinox Media Server Virtual Machine.
  Attempting to install archives downloaded from PLDS directly will result in an error.
- After the deployment of the OVA no additional install actions are required for the Media Server.

Upgrading to Equinox Media Server 9.1 FP9 SP1

The Equinox Media Server version 9.1 FP9 SP1 (9.1.9.1.12) upgrade package supports upgrading from 9.1 FP8 (9.1.8.1.5) and 9.1 FP9 (9.1.9.0.8) via the Equinox Management (iView) UI.

If your current environment is 9.0, 9.0.1 or 9.0.2, first upgrade to 9.1 GA (9.1.0.8) and then to one of the above versions.

Install security patches by using SecurityUpdate_9-1_CVE-11-0.zip after upgrading the Media Server to version 9.1.9.1.12. The upgrade is performed using the contents of 2 archives downloaded from PLDS:

1. Media Server: EquinoxMediaServer_9_1_9_1.zip archive contains the MediaServer_9_1_9_1_12.zip upgrade file.
2. Security Update: SecurityUpdate_9-1_CVE-11-0.zip update file is included in the Equinox Management 9.1.9 SP1 archive EquinoxMgmt_9_1_9_1.zip.

Both files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required upgrade order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Equinox Management Server has been upgraded to version 9.1.9 SP1 (9.1.9.1.59) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version 9.1 FP9 (9.1.9.0.8) or R9.1 FP8 (9.1.8.1.5).
4. Upgrade the Media Server application software using the MediaServer_9_1_9_1_12.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Equinox Management Server User Interface.
5. Upgrade the Media Server platform security using the Platform Security Update file SecurityUpdate_9-1_CVE-11-0.zip. This file is included in the Equinox Management 9.1.9 SP1 archive EquinoxMgmt_9_1_9_1.zip.

NOTE: WARNING!

The procedure to move from non-Secure to Secure Connection is as follows:

1. Test the TLS connection
2. Wait for 5 min.
3. Click the “Apply” button to switch to Secured Connection

Full Deployment of Equinox Media Server 9.1 FP9 SP1

Full deployment of an Equinox Media Server 9.1 FP9 SP1 Virtual Machine uses the 9.1 FP9 SP1 OVA.

- Extract the MediaServer_9_1_9_1_12.ova file from PLDS archive EquinoxMediaServer_9_1_9_1_12_OVA.zip, and then use it to deploy the Equinox Media Server Virtual Machine.
  Attempting to install archives downloaded from PLDS directly will result in an error.
- After the deployment of the OVA no additional install actions are required for the Media Server

Upgrading to Equinox Media Server 9.1 FP9

The Equinox Media Server version 9.1 FP9 (9.1.9.0.8) upgrade package supports upgrading from 9.1 FP5 (9.1.0.23) and 9.1 FP8 (9.1.8.1.5) via the Equinox Management (iView) UI.

If your current environment is 9.0, 9.0.1 or 9.0.2, first upgrade to 9.1 GA (9.1.0.8) and then to one of the above versions.

Install security patches by using SecurityUpdate_9-1_CVE-9-1-1.zip after upgrading the Media Server to version 9.1.9.0.8. The upgrade is performed using the contents of 2 archives downloaded from PLDS:

1. Media Server: EquinoxMediaServer_9_1_9_0.zip archive contains the MediaServer_9_1_9_0_8.zip upgrade file.
2. Security Update: SecurityUpdate_9-1_CVE-9-1-1.zip update file is included in the Equinox Management 9.1 FP9 archive EquinoxMgmt_9_1_9_0.zip.

Both files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required upgrade order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Equinox Management Server has been upgraded to version 9.1 FP9 (9.1.9.0.26) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version 9.1 FP5 (9.1.0.23) or 9.1 FP8 (9.1.8.1.5).
4. Upgrade the Media Server application software using the MediaServer_9_1_9_0_8.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Equinox Management Server User Interface.
5. Upgrade the Media Server platform security using the Platform Security Update file SecurityUpdate_9-1_CVE-9-1-1.zip. This file is included in the Equinox Management 9.1 FP9 archive EquinoxMgmt_9_1_9_0.zip.

NOTE: WARNING!

The procedure to move from non-Secure to Secure Connection is as follows:

1. Test the TLS connection
2. Wait for 5 min.
3. Click the “Apply” button to switch to Secured Connection

Full Deployment of Equinox Media Server 9.1 FP9

Full deployment of an Equinox Media Server 9.1 FP9 Virtual Machine uses the 9.1 FP9 OVA.

- Extract the MediaServer_9_1_9_0_8.ova file from PLDS archive EquinoxMediaServer_9_1_9_0_OVA.zip and then use it to deploy the Equinox Media Server Virtual Machine.
  Attempting to install archives downloaded from PLDS directly will result in an error.
- After the deployment of the OVA no additional installation actions are required for the Media Server.

Upgrading to Equinox Media Server 9.1 FP8

The Equinox Media Server version 9.1 FP8 (9.1.8.1.5) upgrade package supports upgrading from 9.1 GA (9.1.0.8), 9.1 FP5 (9.1.0.23) or the earlier 9.1.8.8.3 build for 9.1 FP8 via the Equinox Management (iView) UI.

If your current environment is 9.0, 9.0.1 or 9.0.2, first upgrade to 9.1 GA.

Install security patches by using SecurityUpdate_9-1_CVE-8.zip after upgrading the Media Server to version 9.1.8.1.5. The upgrade is performed using the contents of 2 archives downloaded from PLDS:

1. Media Server: EquinoxMediaServer_9_1_8_1.zip archive contains the MediaServer_9_1_8_1_5.zip upgrade file.
2. Security Update: SecurityUpdate_9-1_CVE-8.zip update file is included in the Equinox Management 9.1 FP8 archive EquinoxMgmt_9_1_8_118.zip.

Both files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required upgrade order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Equinox Management Server has been upgraded to version 9.1 FP8 (9.1.8.118) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version R9.1 FP5 (9.1.0.23) or the earlier 9.1.8.8 build for R9.1 FP8.
4. Upgrade the Media Server application software using the MediaServer_9_1_8_1_5.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Equinox Management Server User Interface.
5. Upgrade the Media Server platform security using the Platform Security Update file SecurityUpdate_9-1-0_CVE 8.zip. This file is included in the Equinox Management 9.1 FP8 archive EquinoxMgmt_9_1_8_118.zip.

NOTE: WARNING!

The procedure to move from non-Secure to Secure Connection is as follows:

1. Test the TLS connection
2. Wait for 5 min.
3. Click the “Apply” button to switch to Secured Connection

Full Deployment of Equinox Media Server 9.1 FP8

Full deployment of an Equinox Media Server 9.1 FP8 Virtual Machine uses the 9.1 FP8 OVA.

- Extract the MediaServer_9_1_8_1.ova file from PLDS archive EquinoxMediaServer_9_1_8_1_OVA.zip and then use it to deploy the Equinox Media Server Virtual Machine.
  Attempting to install archives downloaded from PLDS directly will result in an error.
- After the deployment of the OVA no additional installation actions are required for the Media Server.

Upgrading to Equinox Media Server 9.1 FP5

The Equinox Media Server version 9.1 FP5 (9.1.0.23) upgrade package supports upgrading from 9.1 GA (9.1.0.8), 9.1 SP4 (9.1.0.17.1) and from 9.1 SP4 / Update-2 (9.1.0.17.5) via the Equinox Management (iView) UI.

If your current environment is 9.0, 9.0.1 or 9.0.2, first upgrade to 9.1 GA.

Install security patches by using SecuriyUpdate_9-1-0_CVE-6.zip after upgrading the Media Server to version 9.1.0.23.

The upgrade is performed using the contents of 2 archives downloaded from PLDS:

1. Media Server: EquinoxMediaServer_9_1_0_23.zip archive contains the MediaServer_9_1_0_23.zip upgrade file.
2. Security Update: SecurityUpdate_9-1-0_CVE-6.zip update file is included in the Equinox Management 9.1 FP5 archive EquinoxMgmt_9_1_5_55.zip.

Both files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required installation order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Equinox Management Server has been upgraded to version 9.1 FP5 (9.1.5.55) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version 9.1 SP4 (9.1.0.17.1) or 9.1 SP4 Update-2 (9.1.0.17.5).
4. Upgrade the Media Server application software using the MediaServer_9_1_0_23.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Equinox Management Server User Interface.
5. Upgrade the Media Server platform security using the Platform Security Update package SecuriyUpdate_9-1-0_CVE-6.zip. This file is included in the Equinox Management 9.1 FP5 archive EquinoxMgmt_9_1_5_55.zip.

- Note**:** there is no need to reinstall the SecurityUpdate_9-1-0_CVE-6.zip if upgrading from Media Server 9.1 SP4 where the SecurityUpdate_9-1-0_CVE-6.zip should have been installed.

Full Deployment of Equinox Media Server 9.1 FP5

Full deployment of an Equinox Media Server 9.1 FP5 Virtual Machine uses the 9.1 FP5 OVA.

- Extract the MediaServer_9_1_0_23.ova file from PLDS archive EquinoxMediaServer_9_1_0_23_OVA.zip and then use it to deploy the Equinox Media Server Virtual Machine.
  Attempting to install archives downloaded from PLDS directly will result in an error.
- After the deployment of the OVA no additional installation actions are required for the Media Server.

Upgrade from 9.1 SP3 to 9.1 SP4

The upgrade is performed using the content of an archive downloaded from PLDS:

- Media Server: EquinoxMediaServer_9_1_0_17_1.zip archive contains the MediaServer_9_1_0_17_1.zip upgrade file.

This file needs to be extracted from the archive downloaded from PLDS and installed according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required upgrade order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Equinox Management Server has been upgraded to version 9.1 SP4 (9.1.0.16.29) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version 9.1 SP3 (9.1.0.16.1) and that SecuriyUpdate_9-1-0_CVE-4 has been applied during the 9.1. SP3 upgrade.
4. Upgrade the Media Server application software using the MediaServer_9_1_0_17_1.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Equinox Management Server User Interface.

NOTE: The "SecuriyUpdate_9-1-0_CVE-4" must have been already applied during the 9.1 SP3 upgrade.

Upgrade from 9.1 SP1 to 9.1 SP3

Install security patches by using SecurityUpdate_9-1-0_CVE-4.zip after upgrading the Media Server to v9.1.0.16.1. The upgrade is performed using the contents of 2 archives downloaded from PLDS:

1. Media Server: EquinoxMediaServer_9_1_0_16_1.zip archive contains the MediaServer_9_1_0_16_1.zip upgrade file.
2. Security Update: SecuriyUpdate_9-1-0_CVE-4.zip update file is included in the Equinox Management 9.1 SP3 archive EquinoxMgmt_9_1_0_16_13.zip.

Both files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required installation order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Equinox Management Server has been upgraded to version 9.1 SP3 (9.1.0.16.13) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version 9.1 SP1 (9.1.0.12.1).
4. Upgrade the Media Server application software using the MediaServer_9_1_0_16_1.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Equinox Management Server User Interface.
5. Upgrade the Media Server platform security using the Platform Security Update package SecuriyUpdate_9-1-0_CVE-4.zip.This file is included in the Equinox Management 9.1 SP3 archive EquinoxMgmt_9_1_0_16_13.zip.

NOTE: When upgrading to "SecuriyUpdate_9-1-0_CVE-4" the upgrade may fail.

The error can appear if the upgraded system was not updated already to the previous package (n-1), and both the current (n) and the previous (n-1) contains Kernel updates. This is a result of the boot partition being small, and can only contain single Kernel upgrade file. The unused Kernel upgrade files present in the boot partition are deleted only after wake-up which happens right after the reset at end of security updates process. Normal maintenance should apply security updates one by one, and if this is skipped, the workaround is to apply the latest security update once more.

Upgrade from 9.1 to 9.1SP1

Install security patches by using SecuriyUpdate_9-1-0_CVE-2_0.zip after upgrading the Media Server to v9.1.0.12.1

During upgrade of Equinox version prior to 9.1 SP1 please make sure you also install fonts_upgrade_package.zip from 9.1.0.12.1 upgrade package on the Media Server to avoid an issue with rendering some non-Latin languages (e.g. Chinese, Japanese, Indian, Korean, Arabic, Hebrew, etc.) during Whiteboard sharing.

The upgrade is performed using the contents of 2 archives downloaded from PLDS:

1. Media Server: EquinoxMediaServer_9_1_0_12_1.zip archive contains the MediaServer_9_1_0_12_1.zip upgrade file and the fonts_upgrade_package.zip upgrade file.
2. Security Update: SecuriyUpdate_9-1-0_CVE-2_0.zip update file is included in the Equinox Management 9.1 SP1 archive EquinoxMgmt_9_1_0_12_10.zip.

These files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required installation order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Equinox Management Server has been upgraded to version 9.1 SP1 (9.1.0.12.10) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version 9.1 SP1 (9.1.0.8).
4. Upgrade the Media Server application software using the MediaServer_9_1_0_12_1.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Equinox Management Server User Interface.
5. Upgrade the Media Server platform security using the Platform Security Update package SecuriyUpdate_9-1-0_CVE-2_0.zip. This file is included in the Equinox Management 9.1 SP1 archive EquinoxMgmt_9_1_0_12_10.zip.
6. Upgrade the fonts using the fonts_upgrade_package.zip file.

Upgrade from 9.0.2 to 9.1

The Avaya Equinox Media Server upgrade to Release 9.1 (9.1.0.8) must be performed on a Media Server unit running Release 9.0.2 GA (9.0.2.5.4). The Media Server R9.1 is based on RedHat (RH) Linux 7.3 Operating System while the Media Server R9.0.2 is based on RH Linux 6.7 Operating System. The process of the Media Server platform upgrade from Release 9.0.2 to R9.1 includes a Linux OS Upgrade from RH 6.7 to RH 7.3.

If your Media Server currently runs a software version earlier than version 9.0.2 GA you must upgrade the Media Server to 9.0.2 first and only then upgrade it to 9.1. Refer to the “Avaya Equinox Media Server for Equinox Conferencing Solution 9.0.2 FP (9.0.2.5)” Release Notes for important information related to the Upgrade to 9.0.2.

The upgrade is performed using the contents of 2 archives downloaded from PLDS:

1. Media Server: EquinoxMediaServer_9_1_0_8.zip archive contains the MediaServer_9_1_0_8.zip upgrade file.
2. Equinox Management: OS_Upgrade_7_3_170927.zip and SecuriyUpdate_9-1-0_CVE-1_5.zip upgrade files are included in the Equinox Management 9.1 archive EquinoxMgmt_9_1_0_8_4.zip.

These files need to be extracted from the archives downloaded from PLDS and installed separately according to the installation order specified below. Attempting to install archives downloaded from PLDS directly will result in an error.

The required installation order is as follows:

1. Create an image snapshot of the Media Server as a backup. Use your company approved procedure for creating the image.
2. Ensure that the Equinox Management Server has been upgraded to version 9.1 (9.1.0.8.4) before you start the upgrade of the Media Server.
3. Ensure that your Media Server is running version 9.0.2 (9.0.2.5).

4. Upgrade the Media Server Operating System from RH 6.7.to RH 7.3 using the OS_Upgrade_7_3_170927.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Equinox Management Server User Interface. This file is included in the Equinox Management 9.1 archive EquinoxMgmt_9_1_0_8_4.zip. The OS upgrade may take up to 60 minutes.
5. Upgrade the Media Server application software using the MediaServer_9_1_0_8.zip upgrade file. Employ the standard upgrade procedure for Media Servers via the Equinox Management Server User Interface.
6. Upgrade the Media Server platform security using the Platform Security Update package SecuriyUpdate_9-1-0_CVE-1_5.zip. This file is included in the Equinox Management 9.1 archive EquinoxMgmt_9_1_0_8_4.zip.

For information about patches and product updates, see the Avaya Technical Support Web site https://support.avaya.com.

Troubleshooting the installation

For information about troubleshooting the installation, see the Avaya Technical Support Web site https://support.avaya.com.

Restoring software to previous version

If snapshots were made of an entire previous solution deployment, those could be restored to revert to a previous version.

For the detailed procedure for backing up Avaya Meetings Media Server and restoring from backup, please see the Administering Avaya Meetings Media Server guide, chapter 6: Data management.

What's new

The following table lists the enhancements and modifications in the Avaya Meetings Media Server (previously known as Equinox Media Server) 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.

Avaya Meetings Server 9.1 FP15

The Avaya Meetings Media Server 9.1.15.0.5 is a part of the Meetings Solution 9.1.15 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	Meeting Server 9.1.15 is packaged with RHEL 8.10 OS
Harman Integration:	Avaya Meetings Server 9.1 FP15 introduces integration with Harman Media Suite (HMS) to manage recording operations for meetings hosted on the server. HMS fully replaces the Avaya Streaming and Recording (AESR) solution, eliminating the need for ACRG and providing native support for recording within the Meetings Server environment. 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.

Avaya Meetings Server 9.1 FP14

The Avaya Meetings Media Server 9.1.14.0.6 is a feature pack. The base operating system has been upgraded from RHEL 7.6 to RHEL 8.4. This software release implements multiple security vulnerability and system stability improvements.

Avaya Meetings Server 9.1 FP13

The Avaya Equinox Media Server 9.1.13.0.13 is a feature pack. This software release implements multiple security vulnerabilities and system stability improvements.

Enhancement / Modification	Description
FedRAMP compliance support	Meeting Media Server 9.1.13 is verified to operate correctly in a FedRAMP configuration
Increased upload speed for better presentation quality	The bandwidth limit for presentations can now be configured to a higher value, up to 800 Kbps (in the Meetings Management Meeting Policies setting page).
Viewing disk encryption status and CVE version	You can check if the disk encryption or remote key server is enabled for your Avaya Meetings Media Server. The CVE version is now also displayed in the Software Version field.
Updated waiting room background audio prompt	The updated audio prompt is played for Workplace Client and WebRTC Client participants. This audio replaces WaitingRoomBackgroundNoStar.wav. The updated text of the audio prompt is "The meeting has not yet started. You will automatically be placed in the meeting when the moderator joins. If you are the moderator, please use the graphical user interface to go to the meeting controls menu and select become moderator". This is to prompt the Avaya Workplace mobile user to use the graphical user interface instead of using DTMF, as that use case is not supported when the user is connecting with Avaya Workplace.

Avaya Meetings Server 9.1 FP12

The Avaya Meetings Media Server 9.1.12.0.9 is a feature pack. This software release implements multiple security vulnerability and system stability improvements.

A new flex profile was added to the OVA which allows you to better utilize the host system in the case where the standard profiles might underutilize the available capacity. See the Avaya Meetings Server 9.1.12 Offer Definition and Deploying Avaya Meetings Server 9.1 for further details.

Avaya Meetings Server 9.1 FP11

The Avaya Meetings Media Server 9.1.11.0.20 is a feature pack. The base operating system has been upgraded from RHEL 7.3 to RHEL 7.6. This software release implements multiple security vulnerability and system stability improvements.

Additionally, support for OVA deployment on VMWare ESXi 7.0 has been added. Avaya Meetings Media Server 9.1.11.0.20 OVA can now be deployed on VMware 6.7 or 7.0 versions. Furthermore, the OVA can now be deployed directly via the ESXi web client, as well as using vSphere web client for vCenter.

Equinox Conferencing Solution 9.1 FP10

The Avaya Equinox Media Server 9.1.10.0.9 is a feature pack, but no new major features are introduced. This software release implements multiple security vulnerability and system stability improvements.

Equinox Conferencing Solution 9.1 FP9 SP1

The Avaya Equinox Media Server 9.1.9.1.12 is a service pack, so no new major features are introduced. This software release implements multiple security vulnerability and system stability improvements.

Additionally, Equinox Conferencing solution FP9 SP1 provides full GDPR data privacy compliancy with secure processing (encryption) and retention of Personal Data. For the AEMS component the GDPR related change lets you set the Log Retention duration.

Equinox Conferencing Solution 9.1 FP9

Enhancement / Modification	Description
VMWare Support	Added support for OVA deployment on VMWare ESXi 6.7. Avaya Equinox Media Server 9.1.9.0.8 OVA can now be deployed on VMware 6.0, 6.5 or 6.7 versions. **Note:** the OVA should only be deployed using vSphere web client for vCenter, and not directly via a host's web interface.
AVP Support	Added support for OVA deployment on AVP versions 8.1 and 8.1.1. The Avaya Equinox Media Server 9.1 FP9 OVA can now be deployed on Avaya Solutions Platform Servers running AVP versions 8.0, 8.1 and 8.1.1.
Security Enhancements	Linux SSH Admin user was removed.

Note:

1. Discontinued manufacturer support for Scopia® Lync Gateway / Client:
   https://downloads.avaya.com/css/P8/documents/101051991
2. Discontinued manufacturer support for the Scopia® Elite 5xxx MCU software:
   https://downloads.avaya.com/css/P8/documents/101046658

Equinox Conferencing Solution 9.1 FP8

The Avaya Equinox Media Server 9.1.8.1.5 is a service pack part of the Equinox Conferencing Solution Feature Pack. This software release implements multiple security vulnerability and system stability improvements.

Additionally, support for OVA deployment on AVP versions 8.0 has been added. The Avaya Equinox Media Server 9.1 FP8 OVA can now be deployed on Avaya Common Servers running AVP versions 7.1, 7.1.2, 7.1.3 and 8.0.

Equinox Conferencing Solution 9.1 FP5

The Avaya Equinox Media Server 9.1.0.22 is a service pack part of the Equinox Conferencing Solution Feature Pack. This software release implements multiple security vulnerability and system stability improvements.

Additionally, support for OVA deployment on AVP versions 7.1.3 has been added. The Avaya Equinox Media Server 9.1 FP5 OVA can now be deployed on Avaya Common Servers running AVP versions 7.0, 7.1, 7.1.2, and 7.1.3.

Equinox Conferencing Solution 9.1 SP4

The Avaya Equinox Media Server 9.1.0.17 is a service pack, so no new major features are introduced.

Equinox Conferencing Solution 9.1 SP3

The Avaya Equinox Media Server 9.1.0.16.1 is a service pack, so no new major features are introduced.

The Equinox 9.1SP3 release introduces a new option in OTT to force the Equinox Media Server webRTC calls to go through the Equinox Conferencing WebRTC gateway. This is to improve packet loss handling. Equinox Conferencing WebRTC gateway supports re-transmission resulting in improved video quality.

- For Equinox Conferencing (OTT) deployments
    - Configuration is done through Equinox Management configuration UI
    - By default, this behavior is not enabled
    - Feature can be enabled by setting the “com.avaya.aawg.forceMediaAdaption” advanced parameter. Value needs to be set to “true”.
    - com.avaya.aawg.forceMediaAdaption=true
    - Feature can be disabled by setting the parameter value to “false”.

Equinox Conferencing Solution 9.1 SP1

Enhancement / Modification	Description
1080p60/720p60	Added the support for 60fps on AVP 7.1.2 and ESXi 6.0 servers. Details in chapter “1080p60/720p60 video resolution”.

Equinox Conferencing Solution 9.1

Enhancement / Modification	Description
AES256	Added the support for AES256 encryption in SIP for the media stream. (GRIP 17200)
Lecturer on slave	Lecture mode works also from slave MCU with some limitations (GRIP 16030)
Russian language	Added the Russian language in video display messages (GRIP 14416)

Call Statistics	Statistics of the call information available at Equinox Management (GRIP 17972)
Lecturer Audio	Lecturer can be audio only participant in video call
Audio Announcements customization	The audio prompts announcements can be customized per each tenant (GRIP 16272)
User Audio language	User can specify its own preferred language by login in user portal
Opus Codec	Opus audio codec offered to capable endpoints (advanced command needed to enable)
AWS	Amazon Web Service support
WCS slider	Web Collaboration Service slider feature
MSS enabled	In High-capacity mode the Multi Stream Switched Video is available for Equinox client 3.3 and XT series endpoints.

Resolved Issues

Avaya Meetings Server 9.1 FP15

ID	Visible symptoms
1-22662136362	Green Banner appears in the Video Overlay when a System Notification (IMCI) is shown.
1-22104365477	CVEs have been identified while Media Server is running latest 9.1.14 Security Update SSP-012
1-18888114142	P3S3 - Green screen appears on portal and IXWP
1-22133518632	Avaya Media Server reboots when Workplace Client joins with audio a Meeting after IVR and attempts to open video

Avaya Meetings Media Server v9.1.14.0.6 for Meetings Server 9.1 FP14

ID	Visible symptoms
RVELITE-14133	Users cannot join a Meeting using a dial-up number via IVR – the IVR session does not start. Users can still join via URL or using the Join function of a Workplace Client.
RVELITE-14156	Users fail to join Meeting due to lack of audio resources. In some rare cases on a loaded Media Server the resources used for audio calls might not be released properly when a call is disconnected which might gradually lead to lack of audio resources.
1-18888114142	Unacceptable video quality due to high packet loss on the MCU side. Encountered when EP-s and infrastructure are configured for MTU size higher than 1360 which is a default limitation on the Media Server.
1-19058515050	I Users cannot join Meeting - 503 Service Unavailable notification is reported. The reason is that in some rare cases audio resources are not released correctly when calls are terminated on the AAWG.

1-18922330094	The VM Snapshot option is blocked on the Management and Media Server VM-s when a Conferencing Solution 9.1.13 OVA is deployed.
1-17854258899	The audio level is low in Meetings where the G.711 audio codec is used.
1-18141381314	Authentication failure when users attempt to login to Media Server, Recording GW etc. with EASG (Challenge/Response).
1-17820237052	Unexpected display "Meeting is (not) encrypted". Meeting reported unexpectedly as non-encrypted when dialing out to a client.

Avaya Meetings Server 9.1 FP13

Avaya Meetings Media Server v9.1.13.0.13 for Meetings Server 9.1 FP13

ID	Visible symptoms
	Protection for log4j vulnerabilities – all known issues reported at the time of the release (see PSN005938u for vulnerabilities details)
RHSA-2021:2725 RHSA-2021:2845 RHSA-2021:3028 RHSA-2021:3296 RHSA-2021:3325 RHSA-2021:3327 RHSA-2021:3336 RHSA-2021:3438 RHSA-2021:3798 RHSA-2021:3801 RHSA-2021:3810 RHSA-2021:3889 RHSA-2021:4033 RHSA-2021:4777 RHSA-2021:4782 RHSA-2021:4785 RHSA-2021:4788 RHSA-2021:4904 RHSA-2022:0063 RHSA-2022:0064 RHSA-2022:0274 RHSA-2022:0306 RHSA-2022:0473	Security vulnerability improvements
1-17431802263 1-17855700310 1-17858727340 1-17925496617	Media Server Reboot issues

1-18540143541 1-17431802263	
1-17436669362	H.323 endpoint cannot receive content sharing.
1-17400781260	Issues with no-video when escalating from P2P calls to Merged Meeting. Not related to Payload 112
1-17903569682	Some Media Servers are missing services and don't take traffic any more
1-18083938540	EASG password challenge issue
1-18104871782	‘Mute All Participants’ not working for some users

Avaya Meetings Server 9.1 FP12

Avaya Meetings Media Server v9.1.12.0.9 for Meetings Server 9.1 FP12

ID	Visible symptoms
RHSA-2021:0671 RHSA-2021:0699 RHSA-2021:0742 RHSA-2021:0808 RHSA-2021:0856 RHSA-2021:1071 RHSA-2021:1145 RHSA-2021:1298 RHSA-2021:1384 RHSA-2021:1389 RHSA-2021:1469 RHSA-2021:2147 RHSA-2021:2305 RHSA-2021:2314 RHSA-2021:2357 1-17448498852 1-17469115612	Security vulnerability improvements
1-16091221499	Open+PIN messages are played for any codec change
1-16498974314	Unable to deploy AEMS using 48 cores or higher on AWS Cloud
1-16963786842	Participants in Meetings Conference hear scratchy noise
1-17004361143	Massive frozen images from participants in video layout
1-17036683770	Active Speaker not moved to the main Active Speaker Frame
1-17135962709	No audio from external phone connection into virtual room / One Way Audio
1-17140857810	Corrupted video from Polycom RealPresence - Semi-opaque Strip over video
1-17142557364	Gallery Layout offered to MacOS Workplace client
1-17151233924	AEMS: FATAL Mutex Unlock failure messages flooding the MCU logs
1-17162547510	Meeting Welcome Slide shows Meeting Hebrew name in reverse for text longer than 50 characters

1-17168424782 1-17238104992 1-17368230333 1-17306984318	Media Server Reboot issues
1-17176845087	Presentation is not working from H.239 to WCS capable endpoints
1-17408482690	AEMG unable to communicate with AEMS (Admin-Manager interface), AEMS restart

Avaya Meetings Server 9.1 FP11

Avaya Meetings Media Server v9.1.11.0.20 for Meetings Server 9.1 FP11

The base operating system for 9.1.11.0 has changed from RHEL (RedHat Enterprise Linux) version 7.3 to 7.6.

RedHat Service Announcements

ID	Visible symptoms
RHSA-2019:2079 RHSA-2020:1021 RHSA-2020:1512 RHSA-2020:2081 RHSA-2020:2082 RHSA-2020:2344 RHSA-2020:2414 RHSA-2020:2432 RHSA-2020:2642 RHSA-2020:2663 RHSA-2020:2664 RHSA-2020:2894 RHSA-2020:2968 RHSA-2020:3217 RHSA-2020:3220 RHSA-2020:3848 RHSA-2020:3861 RHSA-2020:3864 RHSA-2020:3876 RHSA-2020:3878 RHSA-2020:3901 RHSA-2020:3902 RHSA-2020:3908 RHSA-2020:3911	Security vulnerability improvements

RHSA-2020:3915 RHSA-2020:3916 RHSA-2020:3952 RHSA-2020:3971 RHSA-2020:3978 RHSA-2020:3996 RHSA-2020:4003 RHSA-2020:4005 RHSA-2020:4007 RHSA-2020:4011 RHSA-2020:4032 RHSA-2020:4041 RHSA-2020:4060 RHSA-2020:4072 RHSA-2020:4076 RHSA-2020:4276 RHSA-2020:4350 RHSA-2020:4907 RHSA-2020:4908 RHSA-2020:5002 RHSA-2020:5009 RHSA-2020:5011 RHSA-2020:5023 RHSA-2020:5083 RHSA-2020:5437 RHSA-2020:5443 RHSA-2020:5566 RHSA-2021:0153 RHSA-2021:0221 RHSA-2021:0336 RHSA-2021:0339 RHSA-2021:0343 RHSA-2021:0348 RHSA-2020:3733 RHSA-2020:5280	
1-16090305223 1-16130396998	Text or icons from user in different conference
1-15976259012	Presentation delay
1-16141045241	Phantom Participants
1-15964912870	Audio Prompt interruption
1-16172986132	H323 endpoint not receiving presentation
1-16161541657	Crash due to improperly handled SDP attribute
1-16054532145	Failure to restore save configuration

1-16160005089	Robotic noise due to older Opus version, update Opus libraries
1-16235773055	AEMS fails to identify CU360 as Avaya EP
1-16218265746	Participant shown as active speaker after leaving conference
1-16244176580	Crash, insufficient memory allocated, increased allocated size
1-16172986132	Presenting within video channel when presentation channel expected
1-16303992022	AEMS was restarted with 'Automatic Reboot Scheduled: Video DSP Maintenance Planned' message. Root cause was buffer leak.
1-16313458362	FATAL MCU Received reboot request: reason MpLost
1-16302818170	PartNotFound Appearing occasionally as Label on Users
1-16172986132 1-16319575387	LifeSize connecting to Equinox Conference causes strange video and other issues
1-16091221499	MCU sends SDP with all media=inactive
1-15919184994	Cannot have 16 parties in an ad-hoc Equinox Meeting
1-16091221499	MCU unable to detect RFC2833 DTMF
1-16899116392	AEMS restarts due to DSP issue
1-16908857919	Participant's name was absent in the video layout
1-16937469766	Media Server restart after particular DTMF sequence
1-16933550022	(Audio) Calls Rejected by the Media Server
1-16941304024	Actual Call BW is higher than allowed by configuration
1-16930874389	AEMS rebooted few times after upgrade to 9.1.10
1-16948511565	Media servers rebooting after recent upgrade to 9.1.10
1-16959660406	Wrong display on DeskPhone - P-Asserted issue
1-16911547042	FATAL messages found in MCU while investigating the report
1-16961909902	Hebrew participant names in the IX or Web client video sub-frame text overlay appears reversed
1-16996454842	User can see Layout of 21 while the Service is limited to Layout of 16
1-16941304024	Actual Call BW is higher than allowed by configuration, second part
1-17039526064	AEMS restarts after applying 9.1.10 Patch 11 - MVP exception
1-17052781381	No presentation in broadcast (black square instead of slides)
1-17009897368	AEMS Restarted unexpectedly 3 Times in an hour
1-17005720156	AEMS Crash 2020-11-18
1-17039526064	AEMS restarts after applying 9.1.10 Patch 11 - DSP crash
1-17028004878	AEMS22 DSP crash and restart 2020-12-03 09:11
1-16983734667	iView showing zeroes when Presentation is in progress
1-17123856241	Workplace Client does not show the Welcome Slide and shows black video

Equinox Conferencing Solution 9.1 FP10

Avaya Equinox Media Server v9.1.10.0.9 for Equinox Solution 9.1 FP10

ID	Visible symptoms
135041 - RHSA-2020:1180 135044 - RHSA-2020:1021 135046 - RHSA-2020:1138 135047 - RHSA-2020:1080 135048 - RHSA-2020:1176 135052 - RHSA-2020:1000 135053 - RHSA-2020:1181 135059 - RHSA-2020:1131 135060 - RHSA-2020:1135 135062 - RHSA-2020:1113 135066 - RHSA-2020:1011 135069 - RHSA-2020:1061 135070 - RHSA-2020:1022 135073 - RHSA-2020:1020 135077 - RHSA-2020:1050 135080 - RHSA-2020:1016	Security vulnerability improvements
1-116090305233	AEMS does not correctly recognize and enables slides for Avaya Communicator / Equinox client when using Avaya CM
1-16109348146	Multiple AEMS servers restarts – CPU affinity issue on upgrade & handling SRTCP unencrypted packets
1-16109348146	AEMS Crash due to duplicate handlers – timing issue
1-16097303637	AEMS crash more issues due to proper adapter handlers
1-16090284083	AEMS crash due to web collaboration adapter handler
1-16077785861	Audio Muting issue when cascading AEMS calls (large conferences)
1-16084399168	Incorrect resources reporting between AEMS and AEMG leads to failing calls
1-16077785861	Problems and Destruction of meetings with a large numbers participants
1-16082440553	AEMS Server Crashes – decrypting unencrypted data
1-160684XXXX	AEMS MVP crash – corrupted memory fixed with proper mutex
1-16065845804	AEMS MVP crash in Video FEC processing
1-14924611730	AEMS ControlError messaged reported due to empty media SDP params
1-16010024032	AEMS Unexpected restart and then failed to create ad hoc calls
1-15937331288	Dropped terminal auto re-connects but not visible on WebRTC or IX Workplace participants list
1-15985179529	Unable to Deploy Equinox OVAs with ESXi 6.7 Web Client
1-15982593858	AEMS restarted itself when conference was is in progress – memory timing issue

1-15837560661	Problems when connecting H323 stations to IX Meeting
1-15975141043	Wrong display for AEMS port capacity
1-15970428540	AEMS disconnects from Equinox Management
1-15909355342	AEMS Reboot Unexpectedly – adapter related fix
1-15924543586	Polycom RealPresence Mobile app receives black screen from Equinox Media Server when H264 HP is used.
1-15926014452	AEMS DSP Video Processing Crash with bad islice
1-15878043174	AEMS disconnected from AEMG - logs were stuck till rebooted
1-15751798506	AEMG unable to manage or perform administrative functions
1-15721917094	Security scanning of Equinox devices triggers the alarm "Failed to connect to the device's Admin-Manage interface"

Equinox Conferencing Solution 9.1 FP9 SP1

Avaya Equinox Media Server v9.1.9.1.12 for Equinox Solution 9.1 FP9 SP1

ID	Visible symptoms
1-14986258181 1-15019281399 1-15095813774 1-15095813732 1-15717006385 1-15731990992 1-15732012173 1-15759713202 1-15789409358 1-15789341598 1-14986244699 1-14986251736	Security vulnerability improvements
1-15730609829	Equinox client did not receive video during meeting
1-15714900922	MCU restarted due to decoder crash
1-14925163762	MCU was halting showing power down
1-15038645381	Taking 8 seconds for desk-phones to hear waiting room music
1-15051639093	AEMS 9.1.8 Server Restarted Unexpectedly
1-15739730392	Added Participant Join Meeting But Dropped Immediately
1-14923911153	Ultra-high configuration reporting wrong capacity
1-14999699073	Cascading does not work on High Audio Mode.
1-15026892788	Multiple AEMS system crashed
1-15711812709	Hearing cracking noise when joining as moderator
1-14978148572	Improper Automatic Reboot Scheduled: Video DSP Maintenance Planned
1-14786219401	Autodial not working
1-15781518850	Dialing from Desk-phone results in Prompt cut after 1 sec

Equinox Conferencing Solution 9.1 FP9

Avaya Equinox Media Server v9.1.9.0.8 for Equinox Solution 9.1 FP9

ID	Visible symptoms
1-14639076217	Black main video for all parties until AEMS is restarted, because of tremendous packet loss
1-14771919933	DTMF in ISDN audio is not working
1-13814193327	Documentation: Reservation set to 0 (PodFX install)

Equinox Conferencing Solution 9.1 FP8

Avaya Equinox Media Server v9.1.8.1.5 for Equinox Solution 9.1 FP8

ID	Visible symptoms
1-14786690622 1-14598813182 1-14598894871 1-14512420541	Security vulnerability improvements
1-14761320422	AEMS may crash when WebRTC clients connect
1-14710956764	CU-360 cannot join VMR call
1-14694913917 1-14767761988 1-14626452453	Participants in a Meeting do not receive video, only audio
1-14551504132 1-14603702168 1-14639076217	AEMS may experience high internal packet loss causing unit stability issues and restarts. Meeting participants may experience video quality or black video problems and call disconnects
1-14597360766 1-14677923700 1-14753439968 1-14914367518	Callers could not connect to meetings due to AEMS resource allocation problems
1-14615374059 1-14919748573	A caller entering an Audio/Video meeting might have a one-way audio
1-14583883589 1-14093412311	AEMS restarted unexpectedly due to incorrect handling of STUN negotiation
1-14586724829	AEMS enforced scheduled restart due to DSP problems
1-14049990637 1-14546517093	AEMS restarted unexpectedly
1-14128164042	A meeting Moderator dialing in may see a “Mute” icon in the video overlay indicating that his audio is muted while the Moderator’s audio is not muted.
1-13915196299 1-14029226809	XT Endpoints might not receive H.239 content when Equinox Clients present using WCS
1-14689756412 1-14689773742	AESR Recording Presentation problems: Black presentation received by AESR when recording
1-14524939562	AESR Recording Presentation problems: Black or cropped presentation.
1-14549862075	AESR Recording Presentation problems: Unexpected Presentation layout in a recorded meeting
1-14547024471	Meeting recording does not start
1-14044250300 1-14531235191	WebRTC Client does not receive video after its camera has been blocked and unblocked
1-14665107436	Excessive amount of printouts in the MCU Logs

Equinox Conferencing Solution 9.1 FP5

Avaya Equinox Media Server v9.1.0.22 for Equinox Solution 9.1FP5

ID for MCU	Visible symptoms
1-14053582417	Video calls failing, requiring restart to recover.
1-14040104439	AEMS 9.1.0.22.2 has occasional reboots.

ID for AAMS	Visible symptoms
AMS-5900	OpenSSL security update.
AMS-5530	MariaDB security update.
AMS-5697	SDP negotiation did not handle stereo formulation correctly.
AMS-5657	Stale SIP TCP connection undetected
AMS-5588	amsupgrade/backup restore creates anonymous account
AMS-6244	ICE SDP mid attribute support for Firefox
AMS-5985	Do not disable VAD when joined to multiple conferences.
AMS-5889	Occasional duplicate DTMF digits detected.

ID for WCS	Visible symptoms
WCS-2388	WCS is hanging and rejecting the calls. WCGW meetings load factor increased after one failed attempt to enable slider for meeting.
1-13915196299	Frequently XT endpoint does not receive H.239 content when Equinox clients present using WCS.

Equinox Conferencing Solution 9.1 SP4

Avaya Equinox Media Server v9.1.0.17 for Equinox Solution 9.1SP4

ID	Visible symptoms
1-140132861888	System stability improvements
1-139235147888	DSP maintenance error in webRTC connection
1-138938704667	No video from Polycom in H.323

Equinox Conferencing Solution 9.1 SP3

Avaya Equinox Media Server v9.1.0.16.1 for Equinox Solution 9.1SP3

ID	Visible symptoms
1-13551234779 1-13729140830 1-13337348471 1-13778214508 1-13886283315 1-13859358401 1-13842419032 1-13816047319 1-13856334641 1-13874111771	System stability improvements
1-13525892802	DSP maintenance error
1-13712272589	Wrong parameter in Media-Line (m-line) not compatible with SBCE
1-13533868731	Missing Media-Line (m-line) SBCE required
1-13680171330	Timing issue with analog phones joining the meeting
1-13464941142	Sometimes the waiting room welcome announce continues to be played despite the moderator joined the meeting
1-13511079472	Improved presentation quality in H.263
1-13766238782	Detection of H.245 outband DTMFs from Polycom, added an advanced command "addDTMFsInSimAltCaps" to add DTMFs cap for Polycom devices
1-13680171330	Analog Phone not connecting to PIN protected meeting with waiting room

Equinox Conferencing Solution 9.1 SP1

Avaya Equinox Media Server v9.1.0.12 for Equinox Solution 9.1SP1

ID	Visible symptoms
1-13441506048	No audio announcement heard after becoming Moderator

1-1347630786 2	Problem in webRTC with certificate and secured DTLS media
1-1343593511 0	Equinox Client guest user failed to enter a conference

Equinox Conferencing Solution 9.1

Avaya Equinox Media Server v9.1.0.6 for Equinox Solution 9.1

ID	Visible symptoms
1-1307830249 0	Customized logo not preserved after upgrade. Web Collaboration to video (H.239/BFCP) GW whiteboard Pen/Marker not visualized.

Known Issues and Workarounds

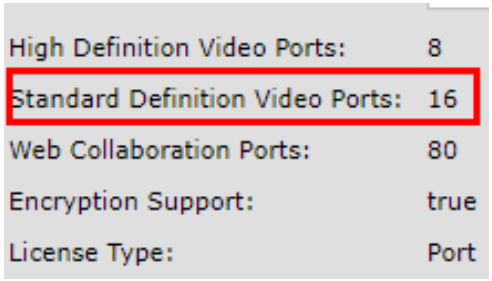
Avaya Meetings Media Server 9.1 FP15

ID	Visible Symptoms
ECONF-5621	No contact is shown in the Contact or Terminal when searching.

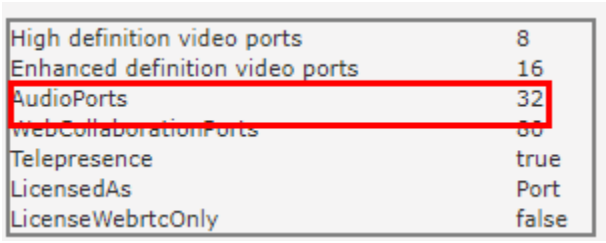
Avaya Meetings Media Server 9.1 FP11

DTMF from the Polycom X50 client does not work. The X50 sends DTMF signals in-band contrary to what was negotiated, and is not supported by the MCU.

- Inconsistency between reported licensed audio/video ports between the iView and MCU. The correct number supported is 16.
  MCU license on iView:



MCU license on the MCU:



Avaya Equinox Media Server v9.1.8.1.5 for Equinox Conferencing Solution v9.1 FP8

The procedure to move from non-Secure to Secure Connection is as follows:

1. Test the TLS connection
2. Wait for 5 min.
3. Click the “Apply” button to switch to Secured Connection

Avaya Equinox Media Server v9.1.0.12 for Equinox Conferencing Solution 9.1 SP1

ID	Visible symptoms	Workaround
	MSS: maximum number of video MSS calls limited to max 200 on a single meeting.	-

Avaya Equinox Media Server v9.1.0.6 for Equinox Conferencing Solution 9.1

ID	Visible symptoms	Workaround
	Fail OS upgrade	Before performing OS upgrade (9.0.2 + CVE3 -> 9.1), take snapshot.
	Upgrade fails	Can’t upgrade directly from 9.0/9.0.1 to 9.1, must upgrade first to 9.0.2, and also CVE3 before starting the process
	Please note	Upgrade of media server contains PMGR.
	Please note	OVA 9.1 contains CVEs fixes
	CVE fixes	In case of upgrade to 9.1 (and not new OVA deploy), please upgrade CVEs as well (SecuriyUpdate_9-1-0_CVE-1_5.zip)
	After mid-call operations from Equinox clients or WebRTC clients which involve closing/opening video channel from media server towards client, NSS/TOL status is not saved	

ID	Visible symptoms	Workaround
	After pause/un-pause action from WebRTC client – no video is displayed for client	
		AES256 is supported for sip calls. In order to allow it, you should activate it by using the following hidden advanced command: “enableAes256” with value: 1
	Presentation issues for some of the participants that do not support Web collaboration technology.	When moving between a non-whiteboard presentation (e.g. full screen sharing, application sharing) and a whiteboard presentation, stop the presentation and start it again.
	FECC (Far End Camera Control) is not supported when trying to control participants that are connected in encrypted mode	-
	When deploying Equinox media server and Equinox management server on AWS (using	

	conversion from OVA to AMI), SSH won't be available from external network. One can still access the system from the internal network via SSH	
	In conference based on MCU service when AMS and MCU are cascaded (only audio & webcollab), Equinox Audio only+webcollab which is connected to AMS sends partial presentation, non-webcollab Endpoints connected to MCU can't see presentation.	Moving the partial presentation frame or resizing it makes the partial presentation to be displayed as expected.
	VMware ESXi 6.0 and 6.5 deploy	Deploy Media Server application OVA Version 9.1.0 on servers with ESXi 6.0 and 6.5 should be done only via vCenter. After deploy is done, is needed to press on "check compliance" under "VM Storage Policies" section in order to have the power-on button available.
	MSS calls: maximum number of video MSS calls limited to max 150.	-

Documentation Note

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 Meetings 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 Global Services Support:

1. Log in to the Avaya Support Web site https://support.avaya.com.
2. Contact Avaya Global Services 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, see the Escalation Contacts listings on the Avaya Web site.

Contact Support Tasks

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

Appendix A: Installing Avaya Common Servers (CSR) with Avaya Appliance Virtualization Platform (AVP)

Please note: Only the standard AVP hypervisor license is installed automatically following EULA acceptance on initial AVP SSH login a script must be executed for the enhanced AVP hypervisor license to be installed.

Downloading documentation

About this task

Avaya Common Servers (CSR) are delivered with Appliance Virtualization Platform (AVP) hypervisor pre-installed. A script must be executed for the enhanced AVP hypervisor license to be installed. Avaya Common Servers utilize OEM hardware from HP or Dell.

Use this procedure to find and download documents on HP or Dell servers that you are using in your deployment. The documentation includes information on the servers and procedures for installing them in racks.

Procedure

1. Open a browser and go to https://support.avaya.com/downloads.
2. Enter `Common Servers` in the **Enter Your Product Here** field, and select the server version from the **Choose Release** dropdown.
3. Download the documents that you need.

Initial AVP host configuration

About this task

Note:

AVP is pre-installed on Common Servers with In-band Management (applications and host management are accessed through a single port). If you require Out of Band Management, enable this feature as explained in the guide for *Migrating and Installing Avaya Appliance Virtualization Platform*; you should not reinstall the AVP.

Note:

Ultra High-capacity Common Servers include an additional license to enable AVP to use more than 32 vCPUs for a single OVA. A script must be executed for the enhanced AVP hypervisor license to be installed. For Ultra High servers, you must connect to the host via SSH using a client such as PuTTY in order to accept the agreement and fully enable the host.

Note:

It is mandatory to install Utility Services as the first VM in an AVP environment (before Equinox Management and Equinox Media Server). It is sufficient to install this in Services Port Only mode. When installing Utility Services in an Equinox Conferencing OTT/standalone deployment, configure the WebLM, CM and SMGR IP addresses to 0.0.0.0 if those components are not present in the environment.

The enhanced license is not Pre-Deployed as part of Pre-Staging, a script to apply the enhanced AVP hypervisor license is Pre-Staged.

- AVP 7.0 / 7.0.1: AVP must NOT be re-imaged else the Pre-Staged enhanced AVP hypervisor license script will be overwritten.
- AVP 7.1.2 and greater**:** The enhanced AVP hypervisor license script is included with the AVP image.

Warning:

If the AVP software requires reinstallation, make sure to use AVP 7.1.2 or greater, which includes the enhanced AVP hypervisor license script in the AVP image.

Reinstallation of AVP 7.0 or 7.0.1 will not allow applying the enhanced AVP hypervisor license, due to the required Pre-Staged script being overwritten.

Note:

SSH is enabled by default until the EULA license is accepted. Once accepted, SSH is automatically disabled after 24 hours. You need to connect to the host using SSH and accept the EULA before deploying any applications on the host.

Procedure

1. Connect a laptop to port 2 of the AVP host. Configure the laptop with the following:
   - IP address: 192.168.13.5
   - Subnet mask: 255.255.255.248
2. Add host to the Solution Deployment Manager (SDM).
3. (Optional) Enable SSH on host via SDM (if more than 24 hours has elapsed since initial power on). 4. Start an SSH session, log in to 192.168.13.6.
   The username varies depending on the AVP version. For AVP release 7.0.1, it is `root`; for AVP release 7.1, it is `admin`. The temporary setup password is `Avaya123$` (for AVP 7.0 / 7.0.1) `AVaya@01` (for AVP 7.1.2) . Once you log in, you are prompted to change this immediately. (The system is not operational until the setup password has been changed.)
5. Read and accept EULA.
6. (Required for Ultra High servers only) Execute the **enable_enhanced_AVP script** by entering the following on the AVP command line:
   - AVP 7.0 / 7.0.1: `/vmfs/volumes/server-local-disk/enable_enhanced_AVP`
   - AVP 7.1.2: `/opt/avaya/bin/enable_enhanced_AVP`
7. (Required for Ultra High servers only) Read and accept EULA.
8. (Required for Ultra High servers only) The script states **AVP enhanced mode successfully enabled** when completed.
9. (Optional for Ultra High servers only) To confirm successful enablement of AVP enhanced mode, execute the following command on the AVP command line:
   - AVP 7.0 / 7.0.1:
     ```
     ~ # vim-cmd vimsvc/license --show | grep "VMware vSphere"
                        name: VMware vSphere 5 Standard
     ```
   - AVP 7.1.2:
     ```
     ~ # vim-cmd vimsvc/license --show | grep "VMware vSphere"
                        name: VMware vSphere 6 Standard for Embedded OEMs
     ```

AVP license types

AVP 7.x: AVP Hypervisor Enhanced license required for the Equinox Media Server

- Required for Equinox Media Server where >32 vCPUs required.
- For AVP 7.0 / 7.0.1: Execute the following script after deployment to apply the enhanced hypervisor license: `/vmfs/volumes/server-local-disk/enable_enhanced_AVP`

NOTE: Accept the EULA to allow the enhanced hypervisor license to be applied.

AVP 7.1.2: Execute the following script after deployment to apply the enhanced hypervisor license:

```
/opt/avaya/bin/enable_enhanced_AVP
```

NOTE: Accept the EULA to allow the enhanced hypervisor license to be applied. An AVP host WebLM license for "VALUE_AVP_XL_SRVR" (this is the Equinox server type) must also be installed on a WebLM Server.

AVP 7.1.2 onwards: AVP Host WebLM license (30-day grace period)

Required for all AVP hosts and specific to the particular server type being used. In the case of the Equinox Media Server, a "VALUE_AVP_XL_SRVR" server type AVP host license is required to be installed on the associated WebLM Server.

See the following AVP document for further details on obtaining and installing an AVP host license: Migrating and Installing Avaya Aura® Appliance Virtualization Platform

Chapter 7: Installing and configuring Appliance Virtualization Platform licensing

Deploying the Solution Deployment Manager client

About this task

To manage the system and deploy OVAs, you need to install the Solution Deployment Manager (SDM) client on a PC. The SDM application requires a PC running 64–bit Windows 7 OS.

Before you begin

Download the SDM user guide from https://downloads.avaya.com/css/P8/documents/101023857 The guide also explains how to access the AVP host for a fresh installation. The AVP host is shipped with default IP and login.

Procedure

1. Download the SDM client application from the Avaya PLDS.
   The SDM version must match the AVP version (for example, 7.1 for both).
2. Install the SDM application.
3. In the **SDM Client Dashboard**, select the **VM Management** page.
4. In the **Location Management page**, create a location for your hosts' cluster by selecting **Location > New**.
   a. Add a name for the location.
   b. Leave the optional fields empty.
5. In the **Host Management** page, enter the AVP host name, FQDN or IP, user name, and password.
6. Open the SDM client, and select the host for the OVA you want to install. This opens a page showing the host details. Select **Next**.
7. Add the OVA file you need to deploy: full pathname (for example, C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts\EquinoxMediaServer_8_5_0_23_5.ova) and select **Submit**.
8. Enter the virtual machine name and configure the network properties: default gateway, public IP address, public netmask. Select **Deploy**.
9. In the EULA acceptance page, select **Accept**.

Appendix B: 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.tart.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 showingnavigate 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 > User Portal / Web Gateway** 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 license is showing, navigate to **Devices** > **H.323 Gatekeepers** and apply 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:

- 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"**
- Copy the cert file **certs.tar.gz** out of the server (using sFTP / winSCP).
- 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**).
- Write down the Public/Service FQDN, Public URL branch, NTP and DNS settings.
- Shutdown the old VM.
- 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.
- Power on the new VM.
- Wait about 10 min after the server started until all installation scripts are completed.
- 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
- 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.
- 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".
- 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).
- 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**).

• SSH to the new VM with "pmgradmin" user then switch to "root" user.

- 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
- Reboot.

• 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.

• 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.

• 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:

• Backup Meetings Management database and configuration files from Meetings Management admin UI by following standard backup procedures.

• 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).

• Shutdown the Meetings Management server.

• Deploy the new VM(s) and configure the network settings (IP address, subnet mask, default GW) to be the same as were used for the old Management server.

• Input new license to activate the new Meetings Management server.

• 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**.

• 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”

• Switch to Fedramp (or JTIC) if the original deployment is Fedramp or JITC.

• Setup redundancy if the original deployment is a redundancy deployment.

• Restore the original backup file into the new master Meetings Management following standard restoring procedures.