Avaya Multimedia Messaging Release 3.5.1

General Availability Release Notes

Issue 1.0
21 August 2019

Table of Contents

Change History

Date	Description
8/21/2019	General Availability for Avaya Multimedia Messaging 3.5.1

Introduction

This document provides information to supplement Avaya Multimedia Messaging 3.5.1 software and documentation. For updated documentation, product support notices, and service pack information, go to the Avaya Support site at http://support.avaya.com.

Please refer to the latest Avaya Aura® 8.0.0.x Release Notes for information specific to the Avaya Aura® feature and service packs.

Installation

Product Release Matrix

The following table lists the release build numbers of the Avaya Multimedia Messaging server.

Client/Server	Release Build Number
Avaya Multimedia Messaging	3.5.1.0.23

What's New?

Avaya Multimedia Messaging provides Avaya Equinox Clients a powerful tool to interact with other users over IM and efficiently handle multiple IM conversations with individuals or groups. Avaya Multimedia Messaging offers users more effective handling of IM between a user's desktop and mobile devices, support for more meaningful workflows for team messaging, and ability to quickly and easily record and send rich multimedia messages for more effective communications. The following services are new when using AMM with Avaya Aura® Equinox 3.5:

- Notifications to iOS Equinox clients via Apple Push Notification Service
  - Notifications of new messages can now be delivered to Equinox clients on the iOS platform via the Apple Push Notification Service, or APNs. This requires an Equinox client with a minimum version of 3.4.5.
  - For 3.5.1, the feature has an enhanced administration user interface and the feature was moved to General Availability.
- The tomcat version has been changed from 8.0.24 to 8.0.53 to address vulnerability issues.

Important Notes

- While AMM interop with OpenFire has been validated, there are issues with AMM/Cisco Jabber interop that will require subsequent fixes.

Fixes

Key	Summary	Found in Release	Fix Version/s
SVVM-8615	CFD: Old tomcat version 8.0.24 used in AMM (VPV)	3.5.0	3.5.1
SVVM-8616	CFD: Information Disclosure in Bad Request from AMM (VPV)	3.5.0	3.5.1

Product documentation

The following customer documentation is available for Avaya Equinox Clients in Release 3.5.1.

- *Avaya Multimedia Messaging Reference Configuration:* This document describes Avaya Multimedia Messaging network, architecture, suggested deployment topologies, system capacities and product interoperability. This document also describes the functional limitation of specific configurations.
- *Deploying Avaya Multimedia Messaging:* This document describes planning, initial setup, and configuration for Avaya Multimedia Messaging. It also provides information about known troubleshooting issues related to deployment.
- *Administering Avaya Multimedia Messaging*: This document describes ongoing administration, management, and maintenance tasks for Avaya Multimedia Messaging. Use this document after deploying Avaya Multimedia Messaging. For more information about deployment, see *Deploying Avaya Multimedia Messaging*.

Product compatibility

For the latest and most accurate compatibility information go to: https://support.avaya.com/CompatibilityMatrix/Index.aspx.

The following table lists the minimum and recommended release lineups of the Avaya products that the Equinox Clients require:

Product	Minimum Release*	Recommended Release*
Avaya Aura® System Manager (SMGR)	7.0.1 (FP)	8.0.0.0
Avaya Aura® Session Manager (SM)	7.0.1	8.0.0.0
Avaya Aura® Communication Manager (CM)	6.3.8.0	8.0.0 SP1
Avaya Aura® Presence Services (PS)	7.1.2	8.0.0.0
Avaya Aura® Conferencing	8.0.6.0	8.0 SP9
Avaya Breeze	3.4.0.1	3.5.0.0
Avaya Session Border Controller for Enterprise	6.3.0.0	7.2.2.0
Avaya one-X® Client Enablement Services	6.2.6.0	7.0.1.0
Avaya Equinox Conferencing	9.0.2.0	9.1.8
Avaya Media Server	7.7.1.0	8.0.0
Avaya Aura Device Services	7.0.1.0	8.0.0.0
Avaya Aura Web Gateway	3.1.0.0	3.6.0.0

* Or later service pack.

Product Release Line-Up

The following table lists the release build numbers of the Avaya Equinox clients and required infrastructure servers.

Client/Server	Release Build Number	Date Available
Avaya Equinox for Windows	3.6.0.153	23 Jul 2019
Avaya Equinox for MacOS	3.6.0.153	23 Jul 2019
Avaya Equinox for Android	3.6.0.134	23 Jul 2019
Avaya Equinox for iOS	3.6.0.133	23 Jul 2019
Avaya Multimedia Messaging	3.5.1.0.23	21 Aug 2019
Avaya Aura® Device Services	8.0.0.0.268	23 Jul 2019
Avaya Aura® Web Gateway	3.6.0.0.148	15 Jun 2019

Supported Hardware and Software Versions

Refer to the Planning and Configuration section in the “Deploying Avaya Multimedia Messaging” documentation.

Software Distribution and Installation for Avaya Multimedia Messaging 3.5.1.0.23

Build Download Details

The following software files are required:

- amm-3.5.0.0.263_OVF10.ova
- amm-3.5.0.0.263_OVF10.ova.sha256sum.txt
- amm-3.5.1.0.23.bin
- amm-3.5.1.0.23.bin.sha256sum.txt
- amm-3.5.0.0.263_OVF10-aws-001.ova
- OS Patch (requires at least version 3.3.0.0.4)
    - ucapp-system-3.4.0.1.10.tgz
    - ucapp-system-3.4.0.1.10.tgz.sha256sum.txt

AMM 3.5.1 Installation Instructions

AMM 3.5.1 requires a RHEL 7.3 environment.

For OVA deployments this should use the AMM 3.5 build 263 OVA (amm-3.5.0.0.263_OVF10.ova). The 3.5.1 binary installer (amm-3.5.1.0.23.bin) should then be copied to the system and executed in lieu of the 3.5.0.0.263 binary installer. It is not necessary to execute the 3.5.0.0.263.bin installer.

Upgrade from AMM 3.4 or 3.5.0

For upgrade from 3.4 or 3.5.0, please follow the instructions in AMM deployment guide.

Fresh install

Please follow the installation instructions available in the *Deploying Avaya Multimedia Messaging* documentation using the AMM 3.5 build 263 OVA and amm-3.5.1.0.23.bin. For software only installation, a RHEL 7.3 environment as specified in the deployment document.

Known Issues

ID	Summary
SVVM-8461	AMM initiated multi-user chat failing with Cisco Jabber
SVVM-8467	XMPP conference, AMM users fail to connect to conference when originator is in INTERNAL Directory
SVVM-8379	ServiceException 500 : An error was encountered while processing message data retrieved from the data store
SVVM-8380	Unknown status on performance page after trying to generate data - 4 plus hours to generate data
SVVM-8404	Multiple errors seen during restore of media giving impression of failure

SVVM-8580	118583 - RHEL 7 : glusterfs (RHSA-2018:3432) (tcp)

System layer updates

Updated command "sys smcvemgt" with new "mds" option to manage the MDS (Microarchitectural Data Sampling) mitigation. See the following CVEs for more on MDS.

https://access.redhat.com/security/cve/cve-2018-12130
https://access.redhat.com/security/cve/cve-2018-12126
https://access.redhat.com/security/cve/cve-2018-12127
https://access.redhat.com/security/cve/cve-2019-11091

Updated system layer update tool to version 2.2. This version has the following enhancements.

- If an application (e.g., AMM) is installed, the system update is blocked if the system clock is not synchronized in NTP. This avoids failures in starting the application back up after the system layer update has completed.

- Fixes a bug with updating the system update meta data in the cases where the application does not initialize properly at the end fo the system update.

Mid-July 2019 RHEL security update.

bind-9.9.4-74.el7_6.1.x86_64
bind-libs-9.9.4-74.el7_6.1.x86_64
bind-libs-lite-9.9.4-74.el7_6.1.x86_64
bind-license-9.9.4-74.el7_6.1.noarch
bind-utils-9.9.4-74.el7_6.1.x86_64
https://access.redhat.com/security/cve/cve-2018-5742
https://access.redhat.com/security/cve/cve-2018-5743

java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6.x86_64
https://access.redhat.com/security/cve/cve-2018-3639
https://access.redhat.com/security/cve/cve-2018-2952
https://access.redhat.com/security/cve/cve-2018-3136
https://access.redhat.com/security/cve/cve-2018-3139
https://access.redhat.com/security/cve/cve-2018-3149
https://access.redhat.com/security/cve/cve-2018-3169
https://access.redhat.com/security/cve/cve-2018-3180
https://access.redhat.com/security/cve/cve-2018-3183
https://access.redhat.com/security/cve/cve-2018-3214
https://access.redhat.com/security/cve/cve-2019-2422

https://access.redhat.com/security/cve/cve-2019-2602
https://access.redhat.com/security/cve/cve-2019-2684
https://access.redhat.com/security/cve/cve-2019-2698

kernel-3.10.0-957.21.3.el7.x86_64
kernel-tools-3.10.0-957.21.3.el7.x86_64
kernel-tools-libs-3.10.0-957.21.3.el7.x86_64
python-perf-3.10.0-957.21.3.el7.x86_64
https://access.redhat.com/security/cve/cve-2018-18397
https://access.redhat.com/security/cve/cve-2018-18559
https://access.redhat.com/security/cve/cve-2018-9568
https://access.redhat.com/security/cve/cve-2018-17972
https://access.redhat.com/security/cve/cve-2018-18445
https://access.redhat.com/security/cve/cve-2019-6974
https://access.redhat.com/security/cve/cve-2019-7221
https://access.redhat.com/security/cve/cve-2018-12126
https://access.redhat.com/security/cve/cve-2018-12127
https://access.redhat.com/security/cve/cve-2018-12130
https://access.redhat.com/security/cve/cve-2019-11091
https://access.redhat.com/security/cve/cve-2019-11477
https://access.redhat.com/security/cve/cve-2019-11478
https://access.redhat.com/security/cve/cve-2019-11479

libgudev1-219-62.el7_6.5.x86_64
https://access.redhat.com/security/cve/cve-2018-15688
https://access.redhat.com/security/cve/cve-2018-16864
https://access.redhat.com/security/cve/cve-2018-16865
https://access.redhat.com/security/cve/cve-2019-3815
https://access.redhat.com/security/cve/cve-2019-6454

libssh2-1.4.3-12.el7_6.2.x86_64
https://access.redhat.com/security/cve/cve-2019-3855
https://access.redhat.com/security/cve/cve-2019-3856
https://access.redhat.com/security/cve/cve-2019-3857
https://access.redhat.com/security/cve/cve-2019-3863

openssl-1.0.2k-16.el7_6.1.x86_64
openssl-libs-1.0.2k-16.el7_6.1.i686
openssl-libs-1.0.2k-16.el7_6.1.x86_64
https://access.redhat.com/security/cve/cve-2018-5407

perl-5.16.3-294.el7_6.x86_64
perl-libs-5.16.3-294.el7_6.x86_64
perl-macros-5.16.3-294.el7_6.x86_64
perl-Pod-Escapes-1.04-294.el7_6.noarch
https://access.redhat.com/security/cve/cve-2018-18311

polkit-0.112-18.el7_6.1.x86_64
https://access.redhat.com/security/cve/cve-2019-6133

python-2.7.5-80.el7_6.x86_64
python-libs-2.7.5-80.el7_6.x86_64

https://access.redhat.com/security/cve/cve-2019-9636
https://access.redhat.com/security/cve/cve-2019-10160

systemd-219-62.el7_6.5.x86_64
systemd-libs-219-62.el7_6.5.x86_64
systemd-sysv-219-62.el7_6.5.x86_64
https://access.redhat.com/security/cve/cve-2018-15688
https://access.redhat.com/security/cve/cve-2018-16864
https://access.redhat.com/security/cve/cve-2018-16865
https://access.redhat.com/security/cve/cve-2019-3815
https://access.redhat.com/security/cve/cve-2019-6454
https://access.redhat.com/security/cve/cve-2018-15688
https://access.redhat.com/security/cve/cve-2018-16864
https://access.redhat.com/security/cve/cve-2018-16865
https://access.redhat.com/security/cve/cve-2019-3815
https://access.redhat.com/security/cve/cve-2019-6454
https://access.redhat.com/security/cve/cve-2018-15688
https://access.redhat.com/security/cve/cve-2018-16864
https://access.redhat.com/security/cve/cve-2018-16865
https://access.redhat.com/security/cve/cve-2019-3815
https://access.redhat.com/security/cve/cve-2019-6454

vim-minimal-7.4.160-6.el7_6.x86_64
https://access.redhat.com/security/cve/cve-2019-12735

wget-1.14-18.el7_6.1.x86_64
https://access.redhat.com/security/cve/cve-2019-5953

Updated the following RPMs to resolve a bug fix related to CVE https://access.redhat.com/security/cve/cve-2017-5715.

dracut-033-554.el7.x86_64
dracut-config-rescue-033-554.el7.x86_64
dracut-fips-033-554.el7.x86_64
dracut-network-033-554.el7.x86_64

Updated the following RPMs to resolve RPM dependencies.

copy-jdk-configs-3.3-10.el7_5.noarch.rpm

cryptsetup-2.0.3-3.el7.x86_64.rpm
cryptsetup-libs-2.0.3-3.el7.x86_64.rpm
dbus-1.10.24-13.el7_6.x86_64.rpm
dbus-libs-1.10.24-13.el7_6.x86_64.rpm

Added the following RPMs to resolve new RPM dependencies.

atk-2.28.1-1.el7.x86_64.rpm
avahi-libs-0.6.31-19.el7.x86_64.rpm
cairo-1.15.12-3.el7.x86_64.rpm
cups-libs-1.6.3-35.el7.x86_64.rpm
fribidi-1.0.2-1.el7.x86_64.rpm
gdk-pixbuf2-2.36.12-3.el7.x86_64.rpm
graphite2-1.3.10-1.el7_3.x86_64.rpm
gtk2-2.24.31-1.el7.x86_64.rpm
gtk-update-icon-cache-3.22.30-3.el7.x86_64.rpm
harfbuzz-1.7.5-2.el7.x86_64.rpm
jasper-libs-1.900.1-33.el7.x86_64.rpm
jbigkit-libs-2.0-11.el7.x86_64.rpm
libglvnd-1.0.1-0.8.git5baa1e5.el7.x86_64.rpm
libglvnd-egl-1.0.1-0.8.git5baa1e5.el7.x86_64.rpm
libglvnd-glx-1.0.1-0.8.git5baa1e5.el7.x86_64.rpm
libtiff-4.0.3-27.el7_3.x86_64.rpm
libwayland-client-1.15.0-1.el7.x86_64.rpm
libwayland-server-1.15.0-1.el7.x86_64.rpm
libXcursor-1.1.15-1.el7.x86_64.rpm
libXdamage-1.1.4-4.1.el7.x86_64.rpm
libXfixes-5.0.3-1.el7.x86_64.rpm
libXft-2.3.2-2.el7.x86_64.rpm
libXinerama-1.1.3-2.1.el7.x86_64.rpm
libXrandr-1.5.1-2.el7.x86_64.rpm
libXxf86vm-1.1.4-1.el7.x86_64.rpm
lz4-1.7.5-2.el7.x86_64.rpm
mesa-libEGL-18.0.5-4.el7_6.x86_64.rpm
mesa-libgbm-18.0.5-4.el7_6.x86_64.rpm
mesa-libGL-18.0.5-4.el7_6.x86_64.rpm
mesa-libglapi-18.0.5-4.el7_6.x86_64.rpm
pango-1.42.4-2.el7_6.x86_64.rpm
pixman-0.34.0-1.el7.x86_64.rpm
python-ply-3.4-11.el7.noarch.rpm

Work-arounds

XMPP conference, AMM users fail to connect to conference when originator is in INTERNAL Directory (SVVM-8467)

Domains for external XMPP interop need to be configured to be external.