Avaya Aura® Solution for Midsize Enterprise 6.2.2.1 with Avaya Aura® 6.2 Feature Pack 4 September 2016 Updates

Release Notes

Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer
Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site:
http://www.avaya.com/support

License
USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.
Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)
Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (For example,., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:
http://support.avaya.com/ThirdPartyLicense/

Preventing toll fraud
"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention
If you suspect that you are being victimized by toll fraud and you need technical
assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:
http://www.avaya.com/support

Providing Telecommunications Security
Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.
Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that can be accessed by this
Avaya product (that is, "networked equipment").
An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who might be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.
Such intrusions might be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:
- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there might be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it might result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security
The final responsibility for securing both this system and its networked equipment rests with you — Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:
- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers must carefully program and configure:
- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities
Customers might experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance
Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment is the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. might void the user's authority to operate this equipment.

Federal Communications Commission Statement
Part 15:

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

European Union Declarations of Conformity

Avaya Inc. declares that the equipment specified in this document bearing the “CE” (*Conformity Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).
Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the Avaya Support Web site:
http://www.avaya.com/support

Trademarks

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:
http://www.avaya.com/support

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:
http://www.avaya.com/support

Contents

General Information

The Avaya Aura® Solution for Midsize Enterprise Release 6.2.2.1 template delivers the following applications for use as Virtual Machines (VM) running on System Platform 6.3.0.

- Avaya Aura® Application Enablement Services 6.3.0
- Avaya Aura® Communication Manager 6.3.0
- Avaya Aura® Communication Manager Messaging 6.3.100
- Avaya Aura® Presence Services 6.2.0
- Avaya Aura® Session Manager 6.3.2
- Avaya Aura® System Manager 6.3.2
- Avaya Aura® Utility Services 6.3.0

These Release Notes also detail applying the Avaya Aura® 6.2 Feature Pack 4 (FP4) update for applicable ME applications, following deployment of the Avaya Aura® Solution for Midsize Enterprise 6.2.2.1 template.

In addition to these Release Notes, refer to each of the specific Release Notes for each of the applications for additional fixes, known issues and workarounds. These are available on support.avaya.com:

1. Go to the Avaya Support site at http://support.avaya.com.
2. Click **Products**. The **Enter Product Name** box is displayed.
3. Type the product name in the box, and when it appears below, select it.
4. **Choose Release** version from the pull-down menu.
5. Under **USER GUIDES & TOP DOCUMENTS**, select View All>
6. In the left pane, select **Release Notes & Software Update Notes**.

Third-party components

Certain portions of the product ("Open Source Components") are licensed under open source license agreements that require Avaya to make the source code for such Open Source Components available in source code format to its licensees, or that require Avaya to disclose the license terms for such Open Source Components. For a period of three years from your date of purchase of a product containing any of the software listed below from Avaya Inc., any Avaya affiliate or an authorized Avaya reseller, we will provide upon request a complete machine readable copy of the source code for such Open Source Component on a medium customarily used for software interchange for a charge no more than our cost of physically performing source distribution. To get access to the source code, you may contact Avaya at (408) 577-7666. Alternatively, you may download the source code from the following link: https://plds.avaya.com. Information regarding other Open Source Components is available on: https://support.avaya.com/Copyright. To access a copy of the license text for the other Open Source Components, see the following:

- Avaya Aura® Application Enablement Services (AES):
  - CLI: /licenses directory
  - GUI: Navigate to Help -> About AE Services
- Avaya Aura® Communication Manager:
  - Disk 1 of the software media: /Licenses directory
  - GUI: Login to System Management Interface (SMI)
- Avaya Aura® Presence Services: /opt/Avaya/Presence/install/3p_rpms/Licenses directory
- Avaya Aura® Session Manager: /Licenses directory
- Avaya Aura® System Manager:
  - CLI: /Licenses directory
  - GUI: Navigate to Settings -> About -> Third Party Terms for CentOS
- Avaya Aura® System Platform:
  - Dom0 CLI: /licenses directory
- Avaya Aura® Utility Services: /Licenses directory
- Installation Wizard:
  - post-install.tar: /Licenses directory
  - pre-install.war: /Licenses directory
- Services VM including Secure Access Link (SAL)
  - CLI:
    - /LICENSE directory
    - /opt/avaya/SAL/gateway/LICENSE/ directory

The Open Source Components are provided "AS IS". ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR THE CONTRIBUTORS OF THE OPEN SOURCE COMPONENTS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Avaya provides a limited warranty on the Product that incorporates the Open Source Components. Refer to your customer sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for the Product, while under warranty, is available through the following web site: http://www.avaya.com/support

Installs and Upgrades

The following upgrade, configuration and interoperability notes apply specifically to Avaya Aura® Solution for Midsize Enterprise release 6.2.2.1.

The Avaya Aura® Solution for Midsize Enterprise 6.2.2.1 software template includes the application versions listed previously and can be used for new installs and upgrades from:

- Avaya Aura® Solution for Midsize Enterprise 6.2
- Avaya Aura® Solution for Midsize Enterprise 6.1
- Midsize Business Template 5.2.1.

Template	Build #	System Platform	New Server	New Licensing	Upgrade Procedure Type	Reference Document
MBT 5.2.1	12	6.0.3.10.3 to 6.3	Yes – to ME spec. HP DL360 G7 or HP DL360p G8	Yes	Migration	Upgrading Avaya Aura® Midsize Business Template to Avaya Aura® Solution for Midsize Enterprise
ME 6.1.0	2580	6.0.3.10.3 to 6.3	Yes – to ME spec. HP DL360 G7 or HP DL360p G8	Yes	Migration	Upgrading Avaya Aura® Solution for Midsize Enterprise
ME 6.1.0	2580	6.0.3.10.3 to 6.3	No – Re-use ME spec. HP DL360 G7	No	Template Upgrade	Upgrading Avaya Aura® Solution for Midsize Enterprise
ME 6.2.0	3105	6.2.1.3.9 to 6.3	No – Re-use ME spec. HP DL360 G7	No	Template Upgrade	Upgrading Avaya Aura® Solution for Midsize Enterprise

Note:

- No license credit will be given for existing licenses for upgrades from Midsize Business Template 5.2.1
- Upgrades are not supported from Collaboration Server 6.1.
- S8800 Servers running Collaboration Server 6.1 cannot be upgraded to Midsize Enterprise 6.2.2.1.
- Midsize Enterprise 6.2.2.1 is only supported on the Avaya Common Servers HP DL360 G7 and HP DL360p G8 (with FP4).

Avaya Aura® Solution for Midsize Enterprise 6.2.2.1 template is available on DVD, material code 700510831, and as three ISO image downloads from PLDS.

Software Download Description	File Name	PLDS Download ID
Avaya Aura® Solution for Midsize Enterprise 6.2.2.1 ISO Image 1 of 3	Midsize_Ent-6.2.2.1.2120-1.iso	CMME0000175
Avaya Aura® Solution for Midsize Enterprise 6.2.2.1 ISO Image 2 of 3	Midsize_Ent-6.2.2.1.2120-2.iso	CMME0000176
Avaya Aura® Solution for Midsize Enterprise 6.2.2.1 ISO Image 3 of 3	Midsize_Ent-6.2.2.1.2120-3.iso	CMME0000177
Midsize Enterprise 6.2.2.1 Standalone Installation Wizard	SP_Pre-Installation_Wizard_7527.exe	CMME0000093
Avaya Aura® System Platform 6.4 Installation and Upgrade ISO	vsp-6.4.0.0.17006.iso	CMME0000225
Third Party Software Source Code for System Platform 6.4	vsp-src-6.4.0.0.17006.iso	CMME0000241

New Installs:

The Avaya Aura® Solution for Midsize Enterprise (ME) release 6.2.2.1 template is Pre-Staged on the server by a distribution partner, ready to be configured with customer-specific values.

After deployment, make sure that the latest approved updates are applied according to these Release Notes and the Product Compatibility Matrix available on http://support.avaya.com.

For new installation and configuration, please refer to the following documents, available on http://support.avaya.com

- *Implementing Avaya Aura® Solution for Midsize Enterprise*
- *Avaya Aura® Solution for Midsize Enterprise 6.2.2.1 with Avaya Aura® 6.2 Feature Pack 4 September 2016 Updates Intelligent Workbook*

Upgrades:

For upgrades, please refer to the following document available on http://support.avaya.com

- *Upgrading Avaya Aura® Solution for Midsize Enterprise*

1. **Install latest patches.**

For upgrades, as per Product Compatibility Matrix, install latest available patches to ME 6.1 or ME 6.2 before upgrading. The Product Compatibility Matrix and patches can be found on http://support.avaya.com. Please refer to specific application documentation for applying patches and / or Service Packs.

Access Product Compatibility Matrix Procedure

a. Access the Avaya support website at http://support.avaya.com.
b. Scroll down to the bottom of the page and locate the **Tools** menu.
c. Click on the **Product Compatibility Matrix** link.
d. Select the letter "**S**" and click on **Solution for Midsize Enterprise (Avaya Aura®)**
e. Select the applicable **Avaya Aura® Solution for Midsize Enterprise (ME)** release.
f. Scroll down the screen and click on **Select Primary Component**
g. Repeat the following for each application in turn:
   - g.i. Select an application by clicking on its box.
   - g.ii. Select latest date.
   - g.iii. Note the applicable updates for the application.

2. **Before starting an Upgrade, check the RAID Battery/Capacitor status:**

If the RAID battery/capacitor in the HP server is failing, a write-cache issue may cause the installation to fail. To check the status of the RAID battery/capacitor, perform the following:

- Log into Domain-0 of the machine and switch user to root
- Execute the following command:
  - raid_status -v
- From the command output, verify the following lines:
  - Controller Status: OK
  - Cache Status: OK
  - Accelerator Ratio: 25% Read / 75% Write
  - Battery/Capacitor Count: 1
  - Battery/Capacitor Status: OK
- If the output is different, replace the RAID battery/capacitor before proceeding with the installation / upgrade.
  - Refer to the applicable HP Server Maintenance and Service Guide for details of how to replace the RAID battery/capacitor.

3. **Upgrade Avaya Aura® System Platform (SP) and Services VM (SVM) first.**

Note, re-login to the System Platform web console needs to happen within 4 hrs of an SVM upgrade to prevent auto rollback of SVM.

4. **Before upgrading from ME 6.1 or ME 6.2, refer to Avaya Aura® System Manager (SMGR) PSN004553u.**

If the certificates are renewed from the System Manager (SMGR) web console or auto-renewed on System Manager, any subsequent upgrade attempt from ME 6.1 (SMGR 6.1.x) or ME 6.2 (SMGR 6.2.x) to ME 6.2.2.1 (SMGR 6.3.0) release will fail.

Workaround is detailed in the following PSN available on http://support.avaya.com:

> PSN004553u: Upgrade from System Manager 6.1.x and 6.2.x to 6.3.0 fails if upgrade is performed through System Platform.

5. **Check Status of Avaya Aura® System Manager (SMGR) Certificates.**

Before applying SMGR updates, ensure that SMGR certificates are valid and renew if necessary.

- Log into Primary System Manager Web console.
- Navigate to **Services □ Inventory**.
- Select **Manage Elements**
- Select the **System Manager** element and click on **More Actions**
- Select **Configure Identity Certificates** from the drop down list.
- Verify the validity period for all certificates.

Refer to the following PSN for further details, available on http://support.avaya.com:

> PSN003661u: Renewal of expired or about to expire certificates of Avaya Aura® System Manager.

6. **Check the Avaya Aura® System Manager (SMGR) Enrollment Password.**

When upgrading from ME 6.1/6.2, verify that the SMGR Enrollment Password is not expired and that this matches what was used in the original installation (Refer to the Troubleshooting section of the **Implementing Avaya Aura® Solution for Midsize Enterprise** guide for full details). This is necessary as the SMGR clients (SM and Presence Services) will need to re-enroll as part of their upgrade. In the SMGR Web Interface:

- Navigate to **Security □ Certificates □ Enrollment Password**
- Choose at least **8 hours** from the **Password expires in:** drop down menu

- Enter the **Enrollment Password** in the **Password:** field.
- Click **Commit**

7. **After ME 6.2.2.1 template upgrade, note the following before upgrading Presence Services 6.2.0.**

Further details are available in the Avaya Aura® Presence Services (PS) 6.2.7 Release Notes available on http://support.avaya.com

- **Ensure that Avaya Aura® Presence Services (PS) only has one entry in Avaya Aura® System Manager (SMGR) Manage Elements page before applying the PS 6.2.7 update.**
    - Open up the SMGR GUI
        - From the System Platform web console **Manage** page, click on the SMGR "wrench" / "spanner"
    - Login as **admin**
    - Select **Inventory** under the **Services** menu
    - Select **Manage Elements**
    - Remove any additional PS entries
        - Select tick box for entry to remove
        - Click **Delete** button
        - Confirm deletion, click **Delete** button

- **Ensure that the Avaya Aura® Presence Services (PS) Migration Tool is run before applying the PS 6.2.7 update.**
    - Refer to the Avaya Aura® Presence Services (PS) 6.2.7 Release Notes for further details, available on http://support.avaya.com.

8. **After ME 6.2.2.1 template upgrade, update the CMM Version.**

Following upgrade from ME 6.1 or ME 6.2, update the CMM Version in SMGR Manage Elements:

- Open up the SMGR GUI
    - From the System Platform web console Manage page, click on the SMGR "wrench" / "spanner"
- Login as **admin**
- Select **Inventory** under **Services** menu
- Select **Manage Elements**
- Select applicable **Messaging** entry using tick box and click on **Edit**
- Select **Attributes**
- Change **Version** to **6.3**
- Click on **Commit**

9. **If upgrading from ME 6.1 or ME 6.2 to ME 6.2.2.1, note the following:** Starting in CM Release 6.3.111.0, The Avaya Aura® Communication Manager updated the SNMP stack/engine to use Net-SNMP.

   The G3-MIB was retired and replaced with two new MIBs:

   - The AVAYA-AURA-CM-MIB
   - AVAYA-AURA-CMALARM-MIB.

   For further details, refer to the following PSN available on http://support.avaya.com:

   PSN020171u: CM is updating SNMP functionality to Net-SNMP.

10. **If upgrading from ME 6.2.2.0 to ME 6.2.2.1, note the following:**

    - Only the CM and SMGR VMs will be updated. All other VMs will remain untouched with all their respective Service Packs applied.
    - After the upgrade has completed, all applicable Service / Feature Packs will need to be re-applied for these VMs.

High Availability (HA) Upgrades:

Please refer to *Upgrading Avaya Aura® Solution for Midsize Enterprise* document for full details for performing upgrades to ME HA configured systems.

Below is a high level overview of the steps involved for upgrading an ME HA deployment.

- From the Primary Server, stop HA
- From the Primary Server, remove HA
- For both Primary and Secondary Servers, upgrade System Platform and apply any System Platform updates as necessary
- From the Primary Server, upgrade the ME template as normal for a non-HA system
- From the Primary Server, install all patches for the individual VMs as necessary
- From the Primary Server, create HA
- From the Primary Server, start HA

Note, if the ME HA system is in a failed over state when HA is removed, when re-enabled the HA Primary and Secondary Servers will be switched from the original deployment. This will require new licenses to be issued to account for the change of the associated MAC address.

Apply Avaya Aura® 6.2 Feature Pack 4 (AA 6.2 FP4) September 2016 Updates:

The AA 6.2 FP4 updates include support for the HP Proliant® DL360p G8 variant Avaya Common Server. ME 6.2.2.1 with AA 6.2 FP4 updates is supported on the following server types:

- Common Server R2 (CSR2), Material Code 303560: HP Proliant® DL360p G8
- Common Server R1 (CSR1), Material Code 263762: HP Proliant® DL360 G7

The following table details the AA 6.2 FP4 September 2016 Updates per application and the order in which they should be applied. These updates are cumulative.

Please refer to the following documents, available on http://support.avaya.com, for details of how to apply patches and / or Service Packs.

- *Implementing Avaya Aura® Solution for Midsize Enterprise*
- *Avaya Aura® Solution for Midsize Enterprise 6.2.2.1 with Avaya Aura® 6.2 Feature Pack 4 September 2016 Updates Intelligent Workbook*

WARNING:

1. Ensure a full backup of the ME system has been made before starting this update process.

2. All updates for all applications must be applied.

3. Apply the updates as ordered in the table.

4. Refer to the applicable individual application documentation available on http://support.avaya.com (Release Notes, PCNs and / or PSNs) for each of the updates for specific instructions before attempting to apply these.

#	Application	ME 6.2.2.1 Version	AA 6.2 FP4 June 2015	AA 6.2 FP4 September 2016	Update Filename	PLDS Download ID
1	Avaya Aura® System Platform	6.3.7	6.3.7[1]	6.4.0[2]	vsp-6.4.0.0.17006.iso[3] (Platform Upgrade)	CMME0000225

#	Application	ME 6.2.2.1 Version	AA 6.2 FP4 June 2015	AA 6.2 FP4 September 2016	Update Filename	PLDS Download ID
2	Services VM (SAL Gateway)	2.0.0	3.0.0[1]	3.0.0	Services_VM-3.0.0.0.11.iso[4] (template)	CMME0000102
				3.0.1	ServicesVM-3.0.1-2.zip	CMME0000226
3	Avaya Aura® System Manager (SMGR)	6.3.2	6.3.14[1]	6.3.18[6]	smgr-patch-plugin-updater-1.0.bin[5]	CMME0000137
					System_Manager_6.3.18_r5505487.bin	CMME0000239
4	Avaya Aura® Session Manager (SM)	6.3.2	6.3.14[1]	6.3.18	asm-installer-6.3.18.0.631804.iso	CMME0000238
5	Avaya Aura® Presence Services (PS)	6.2.0	6.2.6[1]	6.2.7	PS-6.2.0.2-182.zip[7]	CMME0000124
					PS-6.2.1.99-201.zip[8]	CMME0000125
					PS-6.2.7.0-58.zip	CMME0000219
					PS-6.2.7.1-58.zip	CMME0000220
					PS-6.2.7.2-58.zip	CMME0000235
					PS-6.2.7.3-58.zip	CMME0000236
					PS-6.2.7.4-58.zip	CMME0000237
6	Avaya Aura® Communication Manager (CM)	6.3.100	6.3.111[1]	6.3.115	03.0.141.0-23276.tar	CMME0000231
7	Avaya Aura® Application Enablement	6.3.0	6.3.3[1]	6.3.3	aesvcs-6.3.3.0.10-1-featurepack.zip	CMME0000144

#	Application	ME 6.2.2.1 Version	AA 6.2 FP4 June 2015	AA 6.2 FP4 September 2016	Update Filename	PLDS Download ID
	Services (AES)				2014.06.18-LSU-Patch-RHEL5U10.bin	CMME0000146
					633_LSUPatch6_1.bin	CMME0000228
					633_SuperPatch_7.zip[9]	CMME0000242

Note(s):

[1]: Pre-Staged ME 6.2.2.1 Solutions on Common Server R2 (CSR2) will include AA 6.2 FP4 June 2015 versions.

[2]: **WARNING**: All default passwords must be changed before attempting to install this version of System Platform.

Upgrading to this version will fail if root's password is root01, admin's password is admin01, cust's password is cust01 or ldap's password is root01. To avoid this issue, ALL these passwords must be changed before upgrade as shown below:

- Change cust's password:
  - Log onto SP Management Console as admin
  - Navigate to **User Administrator □ Local Management**
  - Select cust to Edit
  - Enter new password
  - Save.
- Change admin's password:
  - Log onto SP Management Console as admin
  - Navigate to **User Administrator □ Change Password**
  - Enter old and new password
  - Save
- Change ldap's password:
  - Log onto SP Management Console as admin
  - Navigate to **User Administrator □ Change LDAP Password**
  - Enter new password
  - Save
- Change root's password on Domain-0:

    - Log onto Domain-0 as root
    - Execute ‘passwd’ to change root’s password
        - Note, you don’t have to change root’s password on CDOM as SP copies dom0’s /etc/shadow to cdom every 5 minutes.

[3]: Use this System Platform .iso installation file to create a DVD. This DVD can then be used to perform a Fresh Install of System Platform or perform a Platform Upgrade of System Platform.

- **Fresh Install**
  WARNING: this will remove all content on the server.
    - Insert DVD in the ME server CD/DVD drive.
    - Boot the server for a fresh install of the underlying operating system and System Platform.
- **Platform Upgrade**
  WARNING: System Platform will reboot as part of this process.
    - The DVD can be used to upgrade an earlier version of System Platform R6.x running on a server.
        - Insert DVD in the ME server CD/DVD drive.
        - Login to System Platform web console as admin user.
        - Navigate to **Server Management □ Platform Upgrade**
        - Select **SP CD/DVD** in the **Upgrade Platform From:** menu
        - Click the **Search** button.
        - Select **VSP.ovf** template.
        - Click the **Select** button.
        - Click the **Upgrade** button.
        - Click the **OK** button when warning prompt appears (pop-up).
        - When the web console login screen re-appears, login as admin.
        - Accept License Agreement (if this is first login after SP install / upgrade).
        - Click the **Commit** button.

[4]: The Services VM can be deployed in two sizes, which one to use is dependent on the server type:

- Services_VM_Medium.ovf: Applicable to CSR2 server types.
- Services_VM_Small.ovf: Applicable to CSR1 server types.

[5]: This executable should be run before attempting to deploy the Avaya Aura® System Manager 6.3.18 update.

- Copy file to **/home/admin** of **CDom** using **admin** account
  - e.g. use SCP client
- Login to **CDom** as **admin**
- Switch user to root: **su root**
- Make the file executable for root: **chmod 700 smgr-patch-plugin-updater-1.0.bin**
- Execute the file: **./smgr-patch-plugin-updater-1.0.bin**

[6]: After install of the SMGR 6.3.18 update, CBC ciphers must be re-enabled. These are required by the ME Post Installation Wizard, e.g. for NPCs. Execute the enableCbcCiphers.sh script on SMGR to enable the CBC ciphers:

- Login to the SMGR CLI as user admin.
- Make the **enableCbcCiphers.sh** script executable:
  - **chmod 750 /opt/vsp/enableCbcCiphers.sh**
- Execute the **enableCbcCiphers.sh** script and enable CBC ciphers:
  - **/opt/vsp/enableCbcCiphers.sh on**

    Setting supported Ciphers to aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc

[7]: This patch is ONLY required when directly upgrading Avaya Aura® Presence Services (PS) on Avaya Aura® Solution for Midsize Enterprise (ME) 6.2.2.1 systems from PS 6.2.0 to PS 6.2.7.

[8]: This patch is ONLY required when directly upgrading Avaya Aura® Presence Services (PS) on Avaya Aura® Solution for Midsize Enterprise (ME) 6.2.2.1 systems from PS 6.2.1 to PS 6.2.7.

[9]: This AES Super Patch should be installed after the Linux Security Update Patch 6.1 (633_LSUPatch6_1.bin).

Apply Application Patches / Service Packs:

After updating ME 6.2.2.1 with the AA 6.2 FP4 releases, apply the following patches / Service Packs.

WARNING:

Refer to the applicable individual application documentation (Release Notes, PCNs and / or PSNs) for each of the updates for specific instructions before attempting to apply these.

Note:

Refer to the *Avaya Aura® Solution for Midsize Enterprise 6.2.2.1 with Avaya Aura® 6.2 Feature Pack 4 September 2016 Updates Intelligent Workbook* for additional details of how to apply updates for each application.

Application	June 2015 Version	September 2016 Version	Update Filename	PLDS Download ID
Services VM	3.0.x		svm_sanity_1.0.1.bsx[2]	CMME0000214
Avaya Aura® Application Enablement Services (AES)	6.x		aesvcs_bash_patch.bin	CMME0000197
			AES6.x-tzdata-2016f-1.0.bin	CMME0000227
Avaya Aura® Communication Manager updates	6.3 KSP4[1]	6.3 KSP6	KERNEL-2.6.18-409.AV1.tar	CMME0000232
	6.3 SSP6[1]	6.3 SSP7	PLAT-rhel5.3-3020.tar	CMME0000217
Avaya Aura® Communication Manager Messaging update SP7 update	6.3.5	6.3.7	CMM-03.0.141.0-0700.tar	CMME0000234
Avaya Aura® Utility Services SP14 update	6.3.10[1]	6.3.14	util_patch_6.3.14.0.20.zip[3][4]	CMME0000240
			util_patch_6.3.0.9.20.zip[5]	CMME0000224
Avaya Aura® Utility Services 6.3 Service Packs 1 and 2 do not uninstall cleanly. See Note **[5]**.	6.3.x		util_patch_6.3.0.4.20.zip[3]	CMME0000120

Note(s):

[1]: Pre-Staged ME 6.2.2.1 Solutions on Common Server R2 (CSR2) will include these AA 6.2 FP4 June 2015 updates.

[2]: The Services VM **svm_sanity_1.0.1.bsx** patch MUST be installed on the Services VM ASAP after applying the System Platform 6.4 update.

Refer to **Services-VM Sanity Patch (svm_sanity_1.0.1) – Release Notes** for further details.

[3]: Utility Services 6.3 Service Packs 1 and 2 do not uninstall cleanly, breaking future application of patches/Service Packs. See PSN027002u for further details and resolution.

[4]: Deactivate and remove any existing Utility Services Service Pack prior to installing a new Service Pack.

[5]: Reinstatement of CBC ciphers support for SSH. Required by the Post Installation Wizard, e.g. for NPCs.

Survivable Remotes:

The compatible Avaya Aura® Communication Manager (CM) Survivable Remote template is version 6.3.0.0.2105. Survivable Remotes need to be upgraded to this version.

When using Avaya Aura® Midsize Enterprise (ME) template 6.2.2.1 to upgrade from previous ME releases, Survivable Remote servers using Communication Manager LSP to back up ME main server(s) will no longer update or synchronize translations with the main server until all servers are upgraded. There will be no additional ME template for LSP/BSM upgrades, so all main and survivable remote server upgrades should be completed in as short an interval as possible.

The following rules apply for upgrades that include LSP/BSM sites:

- ME+LSP configuration
  - Follow CM upgrade rules: LSP first, ME second.
- ME+LSP/BSM configuration
  - Follow SM upgrade rules: ME first, LSP/BSM second.
  - Refer to PSN100152 and apply patch if applicable.

Application	Version	Update Filename	PLDS Download ID
Avaya Aura® Communication Manager Survivable Remote template	6.3.100	6.3.0.0.2105.iso	CMME0000187
	6.3.115	03.0.141.0-23276.tar	CMME0000231

Application	Version	Update Filename	PLDS Download ID
Avaya Aura® Communication Manager updates	6.3 KSP6	KERNEL-2.6.18-409.AV1.tar	CMME0000232
	6.3 SSP7	PLAT-rhel5.3-3020.tar	CMME0000217
Avaya Aura® Session Manager update	6.3.18	asm-installer-6.3.18.0.631804.iso[1]	CMME0000238
Branch Session Manager 6.3.2 Customer Account Reset Patch. See Note [1].	6.3.2	asm-patch-6.3.2.1.632006.sh[1]	SM000000052
Avaya Aura® Utility Services, SP14 update	6.3.14	util_patch_6.3.14.0.20.zip[2][3]	CMME0000240
		util_patch_6.3.0.9.20.zip[4]	CMME0000224
Avaya Aura® Utility Services 6.3 Service Packs 1 and 2 do not uninstall cleanly. See Note **[3]**.	6.3.x	util_patch_6.3.0.4.20.zip[2]	CMME0000120

Note(s):

[1]: Branch Session Manager 6.3 Customer Account password is reset to initial value when upgrading. See PSN100152 for further details and resolution.

[2]: Utility Services 6.3 Service Packs 1 and 2 do not uninstall cleanly, breaking future application of patches/Service Packs. See PSN027002u for further details and resolution.

[3]: Deactivate and remove any existing Utility Services Service Pack prior to installing new Service Pack.

[4]: Reinstatement of CBC ciphers support for SSH. Required for Post Installation Wizard, e.g. for NPCs.

Network Parameter Changes (NPC):

- **High Availability (HA) Solutions:**
  - For any Network Parameter changes (NPC), HA must be turned off.
  - CDom IP address that is used when deploying the HA Standby Server must not be re-used. It is used again if / when HA is turned off.
- **Hostname changes:**

- System Platform Network Configuration page allows for hostnames with leading digits (as per RFC 1123) whilst the ME Pre-Install Wizard only allows this for AES. Setting PS, SM and SMGR with hostnames that have a leading digit will cause breakage whereby SMGR does not support RFC 1123. To ensure hostname support across all ME applications, it's advisable to adhere to RFC 952 for what characters are allowed for hostnames.

Known Issues, Patches and Workarounds

Refer to the following sections for details of known issues and apply the workaround where applicable.

- Installations
- Upgrades and Updates
- Network Parameter Changes
- Backup and Restore
- Serviceability
- Operation
- High Availability (HA)
- Survivable Remotes
- Endpoints

Installations

1. **Extended privileges assigned to CM customer login if dadmin used.**
   If dadmin is not used for the CM customer account, the customer account will have a reduced set of privileges.
   - **Workaround**
     - Use dadmin for the CM customer account to ensure an extended set of privileges are applied.
2. **ME Post Installation wizard can timeout when the SMGR Post Deployment file is being downloaded.**
   This issue can be caused by a slow network connection.
   - **Workaround**
     - Download all the ME template files locally to the /vsp-template/Midsize_Ent directory and then upgrade directly from the System Platform server.
3. **Issues importing Installation Wizard generated System Manager RTSElements.xml and users.xml files.**
   - **For System Manager Manage Elements, importing RTSElements.xml after applying either of the Presence

Services 6.2.4, 6.2.5, 6.2.6 or 6.2.7 updates causes "Failed Records: 1" to be displayed and import stops.

    - Presence Services 6.2.4, 6.2.5, 6.2.6 or 6.2.7 creates its own entry in System Manager Manage Elements such that the Presence Services record contained in the RTSElements.xml file is no longer required.

- **ME Pre-Staged configuration values are not updated for System Manager configuration following customer deployment. If an ABIT file has been used, this causes the import of the users.xml file into System Manager to fail for Pre-Staged ME systems.**
    - The problems caused by this are specific to SIP endpoints, configured within an ME Installation Wizard generated users.xml file, where an ABIT file was loaded during installation. Issues are caused by a mismatch of System Manager configuration data that is defined during Pre-Staging and the customer specific values defined at the 'Configure' stage, i.e. certain values remain defined with the Pre-Staged values.
- **Workaround**
    - Open up the SMGR GUI
        - From the System Platform web console Manage page, click on the SMGR "wrench" / "spanner"
    - Login as **admin.**
    - In the **Services** column, click on **Inventory**
        - Select **Manage Elements.**
        - Select **Import** from the **More Actions** drop-down list.
        - Click the **Browse** button next to the **Select File** box and locate the file **RTSElements.xml** (contained in the SMGR xml files zipfile).
        - In the **Configuration** section, click the **Continue processing other records** radio button for **Select Error Configuration:**
        - In the **Schedule** section,
            - Click the **Run immediately** radio button for **Schedule Job:**
            - Click the **Import** button
        - In the **Import List** section, confirm that the import succeeds by clicking the tick box for the respective scheduled job and click the **View** button. The **Import Status** screen shows the status of the import. Check that the import of the **RTSElements.xml** file is **SUCCESSFUL**:

        - **Element Records**: 5
        - **Failed Records**: 1
    - Click **Manage Elements** to return.
    - Note, temporarily 2 Session Manager entries will be listed. The one with the ip address for Node name will be removed after the audit process runs.
- Wait for Communication Manager (CM) synchronization to complete
    - Navigate to **Inventory -> Synchronization -> Communication System**
    - Refresh and check **Sync Status** for CM until it shows **Completed.**
- In the **Elements** column, click on **Routing**
    - Select **Regular Expressions**
    - Select the messaging **Pattern** and click the **Edit** button.
    - Update **Pattern** SIP domain for messaging from **mysipdomain.com** to match the applied customer specific SIP domain value.
    - Click on **Commit**.
- In the **Elements** column, click on **Routing**
    - Select **SIP Entities.**
    - Select Session Manager entry and click the **Edit** button.
    - Update **Name** for Session Manager from **sm1** to match the applied customer specific value, i.e. hostname of Session Manager.
    - Click on **Commit**.
- In the **Elements** column, click on **Session Manager**
    - Navigate to **Application Configuration -> Applications**
    - Select the CM system as defined during the 'Configure' stage from the **CM System for SIP Entity** drop-down list.
    - Click on **Commit**.
- In the **Elements** column, click on **Session Manager**
    - Navigate to **Application Configuration-> Application Sequences**
    - Select the **cm1** entry and click the **Edit** button.
    - Update the **Name** for the **Application Sequence** from **cm1** to match the applied customer specific value, i.e. hostname of CM.
    - Click on **Commit**.
- The users.xml file can now be imported.

4. **Avaya® Bulk Import Tool for Station Administration (ABIT.xls) issues.**
    - Error when Set Type set to a SIP type, e.g. 9630SIP, for cell 13B
        - **Workaround**
            - This issue can be overcome by preceding 9630SIP with a single quotation mark ('): '9630SIP
    - Problems with the display of the buttons **Input, Check** and **Output**.
        - **Workaround**
            - Try re-loading the ABIT.xls file.
5. **AES incorrectly defined as a SIP Entity in System Manager.** Following deployment of an ME 6.2.2 system, AES is incorrectly configured as a SIP Entity in System Manager. AES is not supported as a SIP Entity to ASM directly.
    - **Workaround**
        - Open up the SMGR GUI
            - From the System Platform web console Manage page, click on the SMGR "wrench" / "spanner"
        - Login as **admin**
        - In the **Elements** column, click on **Routing**
            - Select **SIP Entities**
            - Select **aes** entry and click the **Delete** button.
            - Click the **Delete** button to confirm
6. **For Pre-Staged ME systems, AES cust and root passwords remain set with default values following 'Configuration'.** Change the cust and root passwords manually via the AES CLI.
    - **Workaround**
        - SSH to AES and login as admin
        - Switch user to root: **su - root**
        - Change default password of root: **passwd**
        - Change default password of cust: **passwd cust**
7. **Avaya Aura® Presence Services (PS) installation can fail for fresh installations of Avaya Aura® Solution for Midsize Enterprise (ME)** If the hostname for PS contains uppercase characters this can cause the PS installer to fail. This is fixed for PS 6.2.2 and later releases.
    - **Workaround**
        - For fresh installations of ME, avoid assigning a hostname to PS that contains uppercase characters.
        - If a hostname with uppercase characters for PS is required:

        - Perform the fresh installation using a PS hostname with lowercase characters.
        - After installation is complete, use the Avaya Aura® System Platform Network Configuration page and change the PS hostname to one with uppercase characters.

Upgrades and Updates

8. **After Upgrade of ME 6.1 template to ME 6.2.2 template, SM Application state may remain in "Partial" state.**
    - **Workaround**
        - If this occurs, login to SM and execute statapp. If mgmt is DOWN, ensure the SMGR Enrollment Password is valid and then re-run initTM on SM CLI as root.
9. **DRS status page shows double entries of Presence 6.1 and Presence 6.2 for presence after upgrade ME from 6.1 to 6.2.2.**
    - **Workaround**
        - Delete the Presence 6.1 instance
            - Open up the SMGR GUI
                - From the System Platform web console Manage page, click on the SMGR "wrench" / "spanner"
            - Login as **admin**
            - Select **Replication** under **Services** menu
            - Select **psreplica_6.1** (tick box)
            - Click **View Replica Nodes** button
            - Select PS instance that is showing **Ready for Repair**
            - Click on the **Remove** button
10. **After upgrading SVM, the SVM Application State can show "Partial".**
    - **Workaround**
        - Application State is "Partial"
            - Restart the snmpAgent service.
                - SSH to SVM and login as admin.
                - Switch user to root: **su - root**
                - Execute the following command: **service snmpAgent restart**
11. **When applying Avaya Aura® Communication Manager (CM) update, Avaya Aura® System Platform (SP) may report a timeout failure.**
    A **Failed to install patch** error can sometimes occur due to a timeout failure when applying a CM update. However, this does not prevent the update from being deployed.

- o **Workaround**
    - After receiving the timeout error, navigate to the SP web console **Server Management -> Patch Management -> Manage** page.
    - Continue to click the **Refresh** button at the bottom of the page until the applicable CM update displays **Active Status** under the **cm** section.

12. **The installation of Avaya Aura® System Manager updates can fail with the error “lost connection” displayed by the Avaya Aura® System Platform web console.**
    - o **Workaround**
        - Before attempting to install Avaya Aura® System Manager updates, run the **smgr-patch-plugin-updater-1.0.bin** executable on System Platform CDom.
            - Copy file to **/home/admin** of **CDom** using **admin** account, e.g. use SCP client.
            - Login to **CDom** as **admin**
            - Switch user to root: **su root**
            - Make the file executable for root: **chmod 700 smgr-patch-plugin-updater-1.0.bin**
            - Execute the file: **./smgr-patch-plugin-updater-1.0.bin**
13. **Attempts to apply the AES 6.3.3.0.10-1 Service Pack after removing the AES 6.3.3.0.10-0 Service Pack can fail. System Platform web console indicates successful install but patch Status not Active.**
    - o **Workaround**
        - Refer to PSN027014u available on http://support.avaya.com
14. **When upgrading from ME 6.1, Avaya Aura® Presence Services Migration Tool fails.**

    Avaya Aura® Presence Services Attributes data is missing.
    - o **Workaround**
        - Login to the **Avaya Aura® System Platform** web console as user **admin**.
        - Navigate to **Virtual Machine Management Manage**
        - Open up the SMGR GUI
            - From the System Platform web console Manage page, click on the **smgr** “wrench” / “spanner”
        - Login as **admin**
        - In the **Services** column, click on **Inventory**.
        - Click on **Mange Elements** in the left hand menu.
        - Select the **Presence Services** entry and click **Edit**.

- Select the **Attributes** tab and ensure the following values are defined:
    - **Group:** cluster1
    - **jsmId:** jsm-1.presence
    - **Server Type:** primary
- Click the **Commit** button.

Avaya Aura® Presence Services SIP Entity Type set to Other.

The **SIP Entity** for **Presence Services** must be set to **Type: Presence Services**.

- **Workaround**

    Delete and re-add the **Presence Services SIP Entity** with **Type: Presence Services.**

    - Login to the **Avaya Aura® System Platform** web console as user **admin**.
    - Navigate to **Virtual Machine Management □ Manage**
    - Open up the SMGR GUI
        - From the System Platform web console Manage page, click on the **smgr** “wrench” / “spanner”
    - Login as **admin**
    - In the **Elements** column, click on **Routing**
    - Click on **SIP Entities** in the left hand menu.

    Capture Configuration Data.

    - Select the **Presence Services** entry and click **Edit**.
    - Note the defined values:
        - Name:
        - FQDN or IP address:
        - Location:
        - Time Zone:
        - SIP Timer B/F (in seconds):
        - Entity Links:
            - Name
            - SIP Entity 1
                - Protocol
                - Port
            - SIP Entity 2
                - Port
            - Connection Policy
    - Click the **Cancel** button.

    Delete the Presence Services entry.

    - Select the **Presence Services** entry and click **Delete**.
    - Click the **Delete** button to confirm.

        Re-add Presence Services SIP Entity.

        - Click the **New** button.
        - Configure values according to the previously captured data but set **Type:** to **Presence Services**.
        - Click the **Add** button for **Entity Links** and configure according to the previously captured configuration data.
        - Click the **Commit** button.

15. **Avaya Aura® System Manager (SMGR) SIP Entity Monitoring page does not show the Monitored SIP Entities and phones unable to register after applying Avaya Aura® Session Manager update.**
    - **Workaround**

      Reboot Avaya Aura® Session Manager (SM)

      - Login to the **Avaya Aura® System Platform** web console as user **admin**.
      - Navigate to **Virtual Machine Management □ Manage**
      - Click on the **sm** link under the **Name** column.
      - Click the **Reboot** button.
      - Click **OK** to continue.
      - Wait for **SM** to complete rebooting.
        - **State:** Running
        - **Application State:** Running
      - If after SM reboot problem persists, execute **initTM** command on SM.
        - Login to SM CLI using customer account.
        - Run the following command on SM CLI: **initTM**

<u>**Network Parameter Changes**</u>

16. **For Network Parameter Changes following ME 6.2.2.1 template deployment, wait at least 45 minutes for all changes to be applied.**
    - **Workaround**
      - Currently, System Platform behaves as follows when applying Network Parameter Changes. Further changes should not be made until System Manager has completed its updates. As such, wait at least 45 minutes to ensure that all changes have been applied before attempting any further changes via the System Platform web console.
        - CDom and System Manager included in Network Parameter Changes (NPC):

        - SP displays screen indicating that it will return in 5 minutes. If not, then manually enter IP address in browser (Note, indicates the new CDom IP address). SP returns in approx. 5 minutes but System Manager is still processing the NPC.
    - No change to CDom but System Manager included in Network Parameter Changes (NPC):
        - SP stays on Network Configuration page and states “Processing your request, please wait”. However, SP menu is still accessible to the user potentially allowing other admin tasks to be initiated before the Network Parameter Changes have completed.

  Note, SP "Install/Upgrade Log" not updated in real time, seemingly only after changes have been completed.

17. **Hostnames with leading digits are not supported.**
    System Platform Network Configuration page allows for hostnames with leading digits whilst the ME Pre-Install Wizard only allows this for AES. Setting PS, SM and SMGR with hostnames that have a leading digit causes breakage. SMGR does not support RFC 1123.
    - **Workaround**
        - Do not apply hostnames with leading digits for any of the ME applications other than AES.
18. **WebLM IP address is not updated after changing IP address of System Manager on ME.**
    If the IP address of System Manager is changed via the System Platform Network Configuration page, the WebLM IP address does not get updated.
    - **Workaround**
        - Login to the System Platform web console.
        - Navigate to **Server Management -> System Configuration**
        - In the **Web LM Address:** section, update **Host:** IP address to match the System Manager IP address.
        - Click **Save**
19. **Avaya Aura® Presence Services (PS) “Name” in Avaya Aura® System Manager (SMGR) Manage Elements will not match hostname after PS Network Parameter Changes (NPCs) are applied if PS hostname updated.**
    - **Workaround**
        - Apply the NPCs that include change of PS hostname.

        - Once the NPCs have completed, update the **Presence Services** “Name” in SMGR Manage Elements page.
            - Open up the SMGR GUI
                - From the System Platform web console Manage page, click on the SMGR “wrench” / “spanner”
            - Login as **admin.**
            - In the **Services** column, click on **Inventory.**
            - Select **Manage Elements.**
            - Select the **Presence Services** entry.
            - Click on the **Edit** button.
            - Change “Name” to match the applied “short” PS hostname.
            - Click on the **Commit** button.

20. **Avaya Aura® Presence Services (PS) Replication fails if just Avaya Aura® System Manager (SMGR) IP address changed without also changing its hostname.**
    - **Workaround**
        - Login to the PS CLI as cust: **ssh <PS IP address>**
        - Switch user to root: **su - root**
        - Edit the **/etc/hosts** file and update the SMGR entry to match its new IP address.
        - Stop the PS application: **/opt/Avaya/Presence/presence/bin/stop.sh**
        - Execute the following command to display the state of the PS processes and wait for their state to change to “Not monitored”: **monit summary**
        - Start the PS application: **/opt/Avaya/Presence/presence/bin/start.sh**
        - Execute the following command to display the state of the PS processes and wait for the state to change to “Running”: **monit summary**
            - Note, some PS processes take time before reporting state as **“**Running”.
21. **Original Presence Services (PS) entry will remain in Avaya Aura® System Manager (SMGR) Manage Elements if, before the NPC, the system already has provisioned PS enabled users.**

    When a system already has provisioned PS enabled users before executing an NPC, the original PS entry will remain in SMGR Manage Elements.
    - **Workaround**
        - After the NPC, re-provision impacted users to the new PS entry.

        - On SMGR navigate to **Routing -> SIP Entities**.
        - Select the **Presence Services** entry and click the **Edit** button.
        - Change **Name** to match the new **Presence Services** entry in the **Manage Elements** page.
        - Click on the **Commit** button.
        - Navigate to **User Management**.
        - For each user that has PS enabled:
            - Under **Presence Profile**, change the **System** entry to the new PS entry.
            - Click on the **Commit & Continue** button.

22. **Avaya Aura® System Manager (SMGR) SIP Entity Monitoring page does not show the Monitored SIP Entities and phones unable to register after Network Parameter Change(s).**
    - **Workaround**

      Reboot Avaya Aura® Session Manager (SM)
        - Login to the **Avaya Aura® System Platform** web console as user **admin**.
        - Navigate to **Virtual Machine Management □ Manage**
        - Click on the **sm** link under the **Name** column.
        - Click the **Reboot** button.
        - Click **OK** to continue.
        - Wait for **SM** to complete rebooting.
            - **State:** Running
            - **Application State:** Running

Backup and Restore

23. **In ME 6.2.2.1, restore can sometimes appear hung with status "Wait for Tomcat to restart".**
    - If whilst performing a restore operation on System Platform the restore log gets to the “Wait for Tomcat to restart” step and does not finish, the restore at this point is complete and other tasks can be performed.
    - This can be confirmed by checking the backup.log on CDom:
        - SSH to CDom and login as admin
        - Change directory: **cd /vspdata/backup/**
        - View the end of the backup log: **tail backup.log**
        - Check that the last entry is:
            - **RESTORE ****** Succeeded ******

Serviceability

24. **Avaya Aura® Presence Services (PS) not accessible via the Services Port using Port Forwarding.**
    - **Workaround**
        - Access PS via the console on Domain-0
            - Login to Domain-0 and su to root
            - Enter the following command to access the Presence Services console: **xm console presence_va**
            - Login to Presence Services as root
            - Add the following static route: **route add -net 192.11.13.4 netmask 255.255.255.252 gw dom0.vsp**
            - **NOTE:**
                - This won't persist a reboot. For the static route to persist a reboot, the following needs to be added to file **/etc/sysconfig/network-scripts/route-eth0**

                  192.11.13.4/30 via 135.9.146.23 dev eth0

25. **Avaya Aura® Utility Services 6.3 Service Packs 1 and 2 do not uninstall cleanly.**
    This breaks future application of patches/Service Packs.
    - **Workaround**
        - See PSN100152 for resolution.

Operation

26. **Avaya Aura® Session Manager (SM) fails to boot if date / time is set back in the past**
    If the date / time of Avaya Aura® System Platform is changed back in the past, Avaya Aura® Session Manager will fail to boot due to the file system check.
    - **Workaround**
        - Contact Avaya Technical Support for remedial action which requires root privileges.
27. **Editing the Presence Services Element entry in Avaya Aura® System Manager (SMGR) Manage Elements page fails.**
    The following error occurs when attempting to **Commit** changes to the **Presence Services** entry in SMGR **Manage Elements**: Some internal error has occurred in the service. Please contact the support team.
    - **Workaround**

        - Delete the **Presence Services** entry from SMGR **Manage Elements**.
        - Add **Presence Services** entry to SMGR **Manage Elements** with the required changes.

<u>High Availability (HA)</u>

28. **HA is supported only for network with subnet /24.**
    - **Workaround**
        - The Primary and Secondary Servers should be in same network with subnet mask 255.255.255.0.
29. **Following failover, the Avaya Aura® System Platform Console Domain (CDom) may reboot several times and the web console may run slowly.**
    Other VMs are not impacted by this issue, only CDom.
    - **Workaround**
        - Currently there is no workaround.
30. **Following failover, calls to Avaya Aura® Communication Manager Messaging voicemail may fail.**
    - **Workaround**
        - Check that **MessageCore** is **IN SERVICE**
            - Login to the Avaya Aura® Communication Manager (CM) System Management Interface (SMI).
            - Select **Administration □ Messaging** from the menu bar.
            - Navigate to **Server Information □ System Status** from the left-hand column.
            - Check the status of **MessageCore** and **LDAP processes**. Status should be as follows:
                - **MessageCore IN SERVICE**
                - **LDAP internal server (slapd): UP**
                - **LDAP front end server (Ldapfe): UP**
                - **LDAP Corporate LAN server (Ldapcorp): UP**
        - If **MessageCore** is not **IN SERVICE** or **LDAP processes** are not **UP**, **Stop** and **Start Messaging**.
            - **Stop Messaging**
                - Navigate to **Utilities □ Stop Messaging**
                - Click the **Stop** button.
                - Wait for the **Stop of Messaging completed.** pop-up to be displayed and click the **OK** button.
            - **Start Messaging**
                - Navigate to **Utilities □ Start Messaging**

        - Wait for the **Start of Messaging completed.** pop-up to be displayed and click the **OK** button.

Survivable Remotes

31. **Branch Session Manager Customer access login is not properly being retained when the Branch Session Manager templates are being upgraded to Release 6.3.2 (CM Survivable Remote template 6.3.0.0.2105).**
    Following upgrade, the BSM customer account password is set to the value entered when the previous template was initially installed on the system as opposed to retaining the current value.
    - **Workaround**
        - Use the customer account password from when the Branch Session Manager (BSM) template was initially installed and / or refer to PSN100152: Branch Session Manager 6.3 Customer Account password is reset to initial value when upgrading.

NOTE: Review the latest individual Release Notes, PCNs and PSNs for each of the ME Applications and Endpoints for specific known issues.

Technical Support

Support for Avaya Aura® Solution for Midsize Enterprise is available through Avaya Technical Support.

If you encounter trouble with Avaya Aura® Solution for Midsize Enterprise:

1. Retry the action. Follow the instructions in written or online documentation carefully.
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.
4. If you continue to have a problem, contact Avaya Technical Support by:
    - Logging on to the Avaya Technical Support Web site at http://support.avaya.com.
    - Calling or faxing Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site. You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

      Note: If you have difficulty reaching Avaya Technical Support at the above URL or e-mail address, please go to http://www.avaya.com for more information. When you request technical support, provide the following information:

        - Configuration settings, including Midsize Enterprise configuration and browser settings.
        - Usage scenario, including all steps required to reproduce the issue.
        - Copies of all logs related to the issue.
        - All other information that you gathered when you attempted to resolve the issue.

Tip: 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.

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