Avaya Aura® 6.2 Feature Pack 4

System Manager 6.3.8 Release Notes

Issue: 1.0
June 2014

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"**Documentation**" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products.

Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). 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 to Avaya customers and other parties through the Avaya Support website: http://www.avaya.com/support

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, http://support.avaya.com/Licenseinfo ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR ANAUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA R ESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERSTO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System

License. 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 you. “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.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Business Partner would like to install 2 of the same type of vAppliances, then two vAppliances of that type must be ordered.

Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. “Instance” means one unique copy of the Software. For example, if the end user customer or Business Partner would like to install 2 instances of the same type of Products, then 2 Products of that type must be ordered.

Third-party components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/ThirdPartyLicense/. You agree to the Third Party Terms for any such Third Party Components.

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 Toll 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 website: http://www.avaya.com/support.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, Avaya Aura® System Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.
All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading documents

For the most current versions of documentation, see the Avaya Support website:

http://www.avaya.com/support

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Table of Contents

What’s new

This Release Notes document provides information about new features, installation downloads, and the supported documentation of Avaya Aura® System Manager 6.3.8 on System Platform and VMware. This document also contains information about known issues and the possible workarounds.

This document provides information about System Manager 6.3.8 Software, Data Migration Utility, System Manager 6.3.0 VE OVA and System Manager 6.3.0 System Platform ISO Image.

Note: Contact Avaya Technical Support for the following information:

- Installing System Manager 6.3.8 on System Platform.
- Upgrading to System Manager 6.3.8 on System Platform.
- Installing System Manager 6.3.8 on VMware in Virtualized Environment.
- Upgrading to System Manager 6.3.8 VMware in Virtualized Environment.

Avaya delivers System Manager 6.3.8 in the form of a bin file. You must apply the System Manager 6.3.8 bin file on the System Manager 6.3.x release.

Some product changes are documented as Product Support Notice (PSN). The PSN number defines the related document.

To read a PSN online:

1. Open the Web browser, and navigate to http://support.avaya.com
2. On the main menu, click **Documents**.
3. In the **Enter Your Product Here** field, type System Manager or select **Avaya Aura® System Manager** from the list.
4. Select 6.3.x from the **Choose Release** dropdown.
5. Click **Enter**.
6. In the Content Type pane, select **Product Support Notices**.
7. To open a specific PSN, click the PSN title link.

Enhancements delivered to System Manager 6.3.8:

Enhancement	Keywords
Following are supported for Upgrade feature in System Manager • Support for Communication Manager 5.2.1 to 6.3.6 on different hardware. • Support for System Platform based Communication Manager upgrade (6.0,6.1,6.2) to System Platform based Communication manager 6.3.6	Upgrade
Following are enhancements done in Manage Element for Upgrade feature in System Manager • **Access Profiles**: Access profiles can be Viewed/created/modified/deleted from Services/Inventory/Manage Element page while Creating/Editing Application System. The access profiles can of type URI/SSH/SNMP. • **Device Type:** If device type is present for an Application System it can be selected and assigned on Services/Inventory/Manage Element page while Creating/Editing Elements. • You can create SNMP type access Profile instead of SNMP Attribute Section. • Access Profiles is introduced instead of Access Point section	Manage Element Enhancements for Upgrade
Following are enhancements done in Discovery for Upgrade feature in System Manager • **Subnet Configurations:** Subnet configurations can be Viewed/created/modified/deleted from Services/Inventory/Subnet Configuration screen. • **Element Access Configuration**: Access Configurations for element type can be	Discovery enhancements for Upgrade

Viewed /created/modified/deleted at Services/Inventory/Element Type Access screen. Different element types support different type of protocols for access. The supported protocols will be displayed whenever element type is chosen. • **Global SNMP Configuration:** SNMP configurations can be Viewed/created/modified/deleted from Services / Configurations / Settings / SMGR / Global SNMP Configuration • **Discovery Profile Creations**: Discovery profiles can be Viewed/created/modified/deleted from Services/Inventory/Manage Elements – Discovery Tab. Discovery profile creation involves selection of subnet, element type and global SNMP profiles. All these three configurations are displayed in tabular format and selection is allowed on them • **Discovery**: Discovery can be triggered to run immediately or schedule for later time on Services/Inventory/Manage Elements – Discovery Tab. Select required discovery profile and click on discover now or schedule discovery tab. The status of discovery will be shown on discovery tab as model pop up. Once process completed this pop up gets auto closed. This pop up also indicated the number of elements discovered.	
System Manager Command Line Interface (CLI) session timeout value has been set to 10 minutes.	Security Hardening
A message will be displayed while accessing System Manager Command Line Interface (CLI) if a kernel update requires a reboot of the virtual machine.	Security Hardening
Support for enterprise licensing with cross combinations of VE and non-VE servers in the network. The following combinations are supported: • System Manager WebLM as master WebLM with Standalone WebLM as local WebLM (any mix of VE and non-VE) • Standalone WebLM as master WebLM with Standalone WebLM as local WebLM (any mix of VE and non-VE) • System Manager WebLM as local WebLM is not supported in any deployment	Licensing (WebLM)
A EULA is prompted during System Manager bin file installation on VMware	EULA prompt
You can change Login Name using Bulk user Import using XML and excel	User Bulk Import
You can change Login Name using user management Web Service	User Management Web Service
Data Migration used for Upgrading System Manager runs as background process.	Data Migration
Support for manual Avaya XMPP handle creation - Presence domain selection support in Communication profile for XMPP handle.	User Management
Support Morocco DST Change for System Manager on VMware	Morocco Time zone Support for System Manager on VMware
Support for generating SHA-2 based certificates - With this feature, System Manager supports generation of certificates by using SHA2 as the signing algorithm. The signing algorithm used by the System Manager Certificate Authority (CA) will be updated from SHA1 to SHA2. All new certificates will be signed using this algorithm.	Certificate Management
Support for generating 2048-bit certificates - With this feature, System Manager supports generation of certificates by using 2048 as the default key size. All new certificates will use 2048 as the default key size unless explicitly overridden by the requesting client.	Certificate Management
Support for license over-install checks for non-capacity features: WebLM provides a warning to the administrator installing a new license file when a non-capacity feature present in the existing license file is not present in the new license file being installed. The administrator shall be prompted to confirm or cancel the license file installation. If the administrator selects continue, then WebLM would proceed with the license file over-installation. WebLM will also log the event. The log shall include details of	WebLM

the license installation, user name of the person installing the license, and whether the warning was confirmed or cancelled.	
Support for User preferences: Customized Shortcuts; Add Shortcuts; Edit Shortcuts; Store User Shortcuts; Persist User Shortcuts Support for Quick Navigator: Allows users to enter a string of characters that will match to any valid link on the System Manager UI page navigation. Administrators Links pages will open within System Manager tabs.	System Manager Web Console
Support for viewing scheduled Sequential Job Tasks on Scheduler Web console.	View scheduled Sequential Job Tasks
Support for granular user bulk export – options for selecting communication profiles and contacts attributes for a user export.	User Bulk Export
Following are supported in Excel based User Bulk Import and export: • Support for Collaboration Environment communication profile for user import/export using Excel. • Support for Station Endpoint Communication profile complete set of attributes in user import • Support for User provisioning rule • Support for additional user core attribute like preferred language and others • Support of updating login name • Support for additional communication profiles like CallPilot and Presence. • Support for multiple communication profile sets	User Bulk Import using Excel
Following are supported • Support for Network Region Map • Support for Profile settings and favorite buttons • Support for Communication Manager List/Display Reports(part of Integrated Management Transition)	Communication Manager Element Manager

Deploying the feature pack

Must read

1. **Avaya Aura SMGR 6.3.8 DVD details:**
   - Avaya Aura SMGR 6.3.8 software DVD pack contains 2 DVDs
   - The DVD Artwork mentions the numbers as DVD 1 of 2 and DVD 2 of 2 for respective DVDs.
   - DVD 1 of 2 is the 1st DVD that must be installed and it contains following Software - Avaya Aura System Manager 6.3.0 - Software Update Revision No: 6.3.0.8.923
   - DVD 2 of 2 is the 2nd DVD that must be installed after 1st DVD is installed and it contains following Software (Avaya Aura System Manager 6.3.8 - Software Update Revision No: 6.3.8.5.2376)

   Note
   - If you have installed release earlier than System Manager 6.3.0 , install DVD 1of 2 first and then DVD 2 of 2
   - If you already have installed System Manager Release 6.3.0, directly install DVD 2 of 2.

2. **Upgrade sequence**

   System Manager on System Platform

   You must follow the following sequence for upgrading System Manager Software on System Platform: (1) upgrade System Platform (2) upgrade System Manager and (3) upgrade Elements. For additional information on the installation, follow instructions from the Installation note in *Implementing Avaya Aura® System Manager 6.3.8.*

   System Manager on VMware

   You must follow the procedure for upgrading System Manager Software on VMware provided in *Upgrading Avaya Aura® System Manager on VMware in Virtualized Environment*.

3. Upgrade Session Manager and Communication Manager after the System Manager upgrade.
   Upgrade or install System Manager before you upgrade or install any of the elements like Session Manager and Communication Manager. The version of the elements at any point in time must always be compatible with the version of System Manager

4. **Patch installation**

   System Manager on System Platform

   - Before applying the System Platform patch, ensure that the */tmp/patch* folder does not exist on CDOM.
   - Cleanup any uninstalled patches. Follow below for the procedure:
     - Navigate to **Server Management →Patch Management →Manage** on System Platform Web Console. The Patch List web page is displayed.
     - Identify any patches that are in the state **Not Installed** and that are no longer needed. For each patch identified to be removed, perform the following steps:
       a. Click on the Patch **ID** link. This action displays the Patch **Detail** web page.
       b. Click on the **Remove Patch File** button. This action results in a popup dialog box
       c. Click on the **OK** button.
       d. Click on the **Patch List** button. This action displays the **Patch List** page.

       These actions, if performed, will prevent excess buildup of files in the */vspdata/patch/cache* directory
   - If IP tables are turned off on System Manager, then the system does not install the patch.
   - The administrator must not override or change the existing IP table configurations.

   System Manager on VMware

   - If iptables are turned off on System Manager, then patch installation does not continue.
   - The administrator must not override or change the existing IP table configurations.

   Common Guideline: In a Geographic redundancy setup, the patch installation should be done on Primary first. Once the installation is completed on Primary, only then install the patch on the Secondary Server.

   Common Guideline: This is applicable for both System Manager on System Platform and VMware. After you upgrade the system to 6.3.8, reboot System Manager using System Platform or System Manager command line interface (CLI) or vSphere client to get the updated kernel running in memory. The bin file should be in committed on System Platform before you reboot System Manager.

Due to kernel changes made by the System Manager patch, a reboot is required after the System Manager patch installation is complete. For VE systems, you will be prompted to reboot after logging into the Command line interface. For System Platform systems, follow these steps:

1. Install the System Manager patch via the System Platform web console
2. Verify you can login to the System Manager Web console.
3. Commit the patch from the System Platform web console (Important: Rebooting the System Manager before committing the patch will cause the patch to rollback
and changes made to System Manager after patch installation will be lost.)
4. Reboot the SYSTEM MANAGER (this can be done from the System Platform web console – Virtual Machine Management > Manage > SMGR > Reboot)
5. In System Platform HA environment, stop the HA configuration and then apply the Service Pack on System Manager. Once the service pack installation is successful, start the HA on System Platform.

5. Resource reservations for System Manager on VMware

For VE Footprint Flexibility, System Manager 6.3.8 supports the following profiles.
Multi-tenancy is not supported for Profile-2.

VMware resource	**Profile-1Values**	**Profile-2Values**
vCPUs	4	3
CPU reservation	4(9600MHz)	3(7200 MHz)
Memory	9 GB	7 GB
Memory reservation	9 GB / 9216 MB	7 GB / 7168 MB
Storage reservation	30GB – System Manager 30GB – Session Manager performance data 10GB – CS1000 application 2GB – AUS-collaboration framework TOTAL – 72 GB	30GB – System Manager 30GB – Session Manager performance data 10GB – CS1000 application 2GB – AUS-collaboration framework TOTAL – 72 GB
Shared NICs	1	1
Number of users	>35K to 250K	Up to 35k

6. VE Snapshot

A snapshot preserves the state and data of a virtual machine at a specific point in time. The snapshot is a copy of the running system that is created before a major upgrade or a patch installation. Snapshots can:

- Consume large amounts of data resources
- Increase CPU load on the host
- Affect performance
- Affect service

Snapshots are not backups. Do not use a single snapshot for more than 24-72 hours. Do not maintain snapshots over long periods of time for application or Virtual Machine version control purposes.

Note: All the following points are applicable to System Manager on System Platform and VMware

7. User Management Communication Profile Page

While adding communication profiles to a user, prior to selecting a survivability server / application sequence from the dropdown in the Session Manager communication profile section, ensure that you first select the **Communication Manager communication profile** checkbox so that list of Communication Manager(s) is populated in the dropdown. If you do not select the **Communication Manager communication profile** section checkbox prior to selecting a survivability server / application sequence you will get a pop-up telling you that the Communication Manager system is not selected and that it should be corrected before continuing.

8. If you are upgrading from earlier release to System Manager 6.3.8, you must specify the password for the Alarm Email notification on the System Manager **Global Profile** configuration page, only if you have configured the Alarm email notification in the earlier release.

9. Session Manager and Collaboration Environment re-install will cause a duplicate entry of the element's

serviceability agent in the database records. This situation is likely to come in case of hardware replacement. For more information on element re-install, see *Procedure to recover from an element re-installs*.

10. **Verify the System Manager Release version**
    After installing System Manager 6.3.8, verify the release of the installed System Manager by clicking **About** in the top-right corner of the Home page. You can also run the **swversion** command through the Command Line Interface (CLI).

11. **Use FQDN to gain access to System Manager**
    Use Fully Qualified Domain Name (FQDN) instead of the IP address to gain access to System Manager.

12. **System Manager Hostname**
    System Manager complies with RFC952 for hostnames.

13. **Log in to System Manager**
    For more information, see *Log in to System Manager*.

14. **Understand the password and aging policy for the admin user account**
    To verify the password policy and aging for **admin**, on the dashboard, click **Users** > **Administrators**. In the left navigation pane, click **Security** > **Policies**.

15. **Third- party certificate in case of upgrade**
    You must regenerate and reimport the third- party certificate for an upgrade from earlier releases of System Manager to System Manager 6.3.0 Release. You must follow this process if System Manager is using third-party identity certificates before the upgrade.
    For System Manager-Session Manager replication, System Manager Identity certificate must have the virtual fully qualified domain name (VFQDN) of System Manager in the Subject Alternative Name. If you upgrade System Manager to 6.3.0, the Identity Certificate used before the upgrade is retained but this certificate does not have the VFQDN as the Subject Alternative Name. Due to this, replication to Session Managers stops when Session Managers in the environment are upgraded to 6.3.0 Release.

16. **Reboot System Manager for updated kernel**
    This is applicable for both System Manager on System Platform and VMware. After you upgrade the system to 6.3.8, reboot System Manager using System Platform or System Manager CLI or vSphere client to get the updated kernel running in memory. The bin file should be in committed on System Platform before you reboot System Manager.

17. **IP/FQDN entry of Session Manager elements in DNS server**
    The DNS server must contain the IP/FQDN entry of all the Session Manager elements configured with System Manager to ensure that forward and reverse lookups of Session Manager work from primary and secondary System Manager Servers. Alternatively, the entries must be in */etc/hosts* of both primary and secondary System Manager Servers if the entries are missing from DNS.

18. **Schedule Jobs**
    If a scheduled job has completed all occurrences, do not edit the job and enable the job again. Instead, create a new scheduler job for performing the same task. If you enable a job which has completed all occurrences, then after an upgrade, the job is in the disabled state and you must manually enable the job again.

19. **External authentication configuration**
    If you upgrade directly to System Manager 6.3.0 GA from System Manager 6.0 or earlier release and if you configured the earlier release for an external authentication, such as LDAP and RADIUS, you must reconfigure the details of the external authentication server on System Manager 6.3.8 after the system completes the upgrade. This does not apply to upgrades from System Manager 6.1 or 6.2.
    To reconfigure System Manager external authentication, see *External authentication configuration*.

20. **Login warning banner upgrade**
    If you want to upgrade directly to System Manager 6.3.0 from System Manager 6.0 or earlier release and if you have complied with the configuration for the legal notice, you must reconfigure the login warning banner content on System Manager 6.3.8 after the system completes the upgrade.
    This does not apply to upgrades from System Manager 6.1 or 6.2.

    To reconfigure the login warning banner, see *Login warning banner upgrade*.

21. **Internet Explorer compatibility**
    Some of the System Manager features might not work in Internet Explorer 8 and later versions if the

compatibility and document mode is switched on.
To switch off the compatibility mode, see *Internet Explorer compatibility*.

22. **Browser Cache**
    You must clear the browser cache before gaining access to the System Manager Web Console the first time after the installation or upgrade. If you do not clear the browser cache, style sheets might not load.
23. **Language characters**
    The Internet Explorer 8 browser does not display Chinese and Korean language characters.
    You must Go to */tools/internet options/fonts/.* Set the *Language Script* to Chinese Simplified.
    Select the only option - *Arial Unicode MS*. Accept the changes.

24. **Presence communication profile**
    The Presence services communications profile is added to accommodate new features in future releases. Do not enable this communication profile in System Manager Release 6.3.8.

25. **Shell account**
    An admin user cannot use standard JBoss and Postgres service commands. For more information, see *Shell account*.

26. **Remote System Manager backup**
    Before you select the **Use Default** checkbox, you must first set the remote parameters such as Remote Server Password, Remote Server Port, Remote Server, and Remote Server User in the *Home/Services/Configurations/Settings/SMGR/SMGR Element Manager* page.
27. **Software management**
    System Manager must gain access to *ftp.avaya.com* and *pldsxml.avaya.com* to download firmware and for the Software Manager Analyze functionality to work properly.

28. **CS1000 in the System Manager geographic redundancy setup**
    For information about CS1000 applications supported in System Manager geographic redundancy setup, see *CS1000 in System Manager geographic redundancy setup*.

29. **CS1000 and System Manager interoperability support**
    System Manager 6.3.8 supports CS1000 7.6.

30. **WebLM (**License Management**) Licensing – WebLM CPP client**
    For WebLM CPP client adopters, they must be integrated with WebLM CPP client R6.3.2 or later in order to point to System Manager WebLM 6.3.8.

31. **Avaya SIP communication address**
    System Manager supports characters in communication address as per the SIP RFC.
    For WebLM CPP client adopters, they must be integrated with WebLM CPP client R6.3.2 or later in order to point to System Manager WebLM 6.3.8.

32. **Network Administrator** Role has been removed.
    System Manager does not support the Network Administrator role. System Manager maps the Network Administrator role to the System Administrator role.

    During upgrades, the system assigns all users of the Network Administrator role to System Administrator role and all child roles of the Network Administrator role to the System Administrator role.

33. For System Manager 6.3.8, the bulk import/export template should be used which is released along with 6.3.8. Ensure you are not using earlier release excel template. The Excel files exported in earlier release will not be supported in 6.3.8 release for user import.

34. **Repair Serviceability Agent:**

- On the Services >> Inventory >> Manage Serviceability Agent >> Serviceability Agent page, click **Repair Serviceability agent** to repair the alarming functionality for an element
- **Repair Serviceability agent** is enabled when you select the “Activated” agents.
- When you click **Repair Serviceability agent,** at the SA side the re-initialization of snmp configuration will be triggered.

- This snmp configuration initialization change will be conveyed to the System Manager with the agent's next HeartBeat (HB interval is 15 minutes So once repair button is clicked, wait time for the user is 15 minutes before user tries to test alarms from that element.
- On receiving the HB at System Manager, auto-reactivation of the selected agent will be performed. And already pushed target and user profiles will be automatically pushed again to the selected agents.

35. Some Do's & Don'ts

Do's

- Disable Scheduled jobs before running an **upgrade**.
- Create a backup before performing an **upgrade**.

Don'ts

Do not change / modify permissions of files on the System Manager / System Platform (c-dom, dom-0) unless explicitly stated.

Prerequisites for a new installation of System Manager

System Manager on System Platform

1. Create a backup of the system and store the backup on an external device.
2. Install System Platform **SP_6.3.4.08007.0**
3. Check the RAID Controller Battery state.
   a. Login to System Platform CDOM Web console using admin credentials
   b. Navigate to *Server Management/Log Viewer*
   c. Select System Logs, Critical/Fatal as the log level
   d. Type O_AVDM in the **Find** text box and click **Search**
   e. In the **Message Content** column of the result table, search for the **O_AVDM10101** or **O_AVDM10102** or **O_AVDM10100.**
   f. If this alarm is present, the raid battery of the system needs replacement.
4. Install System Manager Release 6.3.0. The System Manager 6.3.8 bin file can be installed on the System Manager 6.3.x release.
5. Upgrade System Platform before you upgrade System Manager, in case of an upgrade.

System Manager on VMware

1. Create a backup of the system and store the backup on an external device.
2. Install the **ESXi** 5.5 server.
3. Install **vSphere Client 5.5**, and ensure that vSphere Client is connected to the server.
4. Install System Manager 6.3.0 VE OVA. The System Manager 6.3.8 bin file can be installed on the System Manager 6.3.x release.

Hardware Requirements

- S8800 1U Server System Manager IBM x3550m2and material code 700478589
- R610 Server 2CPU MID2 Dell and material code 700501083
- DL360G7 Server 2CPU MID4 HP and material code 700501093
- In addition, System Manager 6.3.8 shall support the next generation common servers
  HP DL360p G8 SRVR Communication Manager S/D/MBT/SBC (HP; material code 654081-B21)
  Dell R620 SRVR 1CPU MID3 (Dell; material code 632298870)

Note: The RAM requirement on the System Manager 6.3.x VM is 9 GB.

Software information

Software	Version	Note
Postgres	9.2.4	Used as a System Manager database. For more information, see: http://www.postgresql.org/docs/9.2/static/
CentOS	5.6 64 bit	Used as the Operating System for the System Manager template
JDK	1.7 update 17 64 bit	
JBoss	6.1.0	
Internet Explorer	8.x, 9.x, and 10.x	
Firefox	26.x, 27.x, and 28.x	
VMware vCenter Server, vSphere Client, ESXi Host	5.0, 5.1,5.5	

Installation note

Contact Avaya Support Website for the following:

- System Manager installation and configuration information for *Implementing Avaya Aura® System Manager 6.3.8*
- System Manager upgrade information on System Platform *Upgrading Avaya Aura® System Manager on System Platform*
- System Manager on VMware installation, configuration and upgrade information for *Deploying Avaya Aura® System Manager on VMware in Virtualized Environment*
- System Manager upgrades information using Data Migration on System Platform for *Upgrading Avaya Aura® System Manager on VMware in Virtualized Environment*
- Installation and upgrades, product support, and service pack for earlier releases of System Manager 6.3.8.

Upgrade information

System Manager on VMware

- For upgrading System Manager on VMware, refer to the *Upgrading Avaya Aura® System Manager on VMware in Virtualized Environment.*

System Manager on System Platform

For upgrading System Manager on System Platform, refer to the Upgrading Avaya Aura® System Manager to 6.3.8 and Migrating System Manager Data using Data Migration utility

If you must upgrade System Platform while upgrading System Manager, first upgrade System Platform with the latest patch and then upgrade System Manager.

Download and install System Manager 6.3.8

Download and install System Manager on System Platform:

#	Procedure	Notes
1.	Download and install the "**System Platform SP_6.3.4.08007.0 rpm for System Manager 6.3.8**" from the Avaya PLDS website.	Verify that the md5sum for the downloaded file matches the number on the Avaya PLDS website. **File Name :** vsp-patch-6.3.4.08007.0.noarch.rpm **PLDS download ID**: SMGR6380005 **Size:** 420 MB / 430186 KB **Md5Sum:** 6852f47b7b45c6f69b1f3c314295e14c

2.	Download and install “System Manager 6.3.0 ISO image” from the Avaya PLDS website.	You must install the System Manager 6.3.0 template on System Platform 6.3.4.08007.0 **File Name :** System_Manager_06_03.iso **PLDS download ID**: SMGR6310004 **Size**: 3315 MB **Md5Sum**: 24c5c6c1e471896931cc60c513db0e61
3..	Download and install the **“System Manager 6.3.8 Software ”** from the Avaya PLDS website.	**File Name :** System_Manager_6.3.8_r4502376.bin **PLDS download ID**: SMGR638001 **Size**: 1567 MB/ 1604087 KB **Md5Sum**: 8fb88372b51e4f7311c4f44e1e7055c6

Note: System Manager 6.3.8 is in the form of bin file. Before installing System Manager 6.3.8, download System Manager 6.3.0 from Product Licensing and Delivery System (PLDS) or purchase System Manager 6.3.0 on DVD from ASD (Order Code 700505971) and install. If the 6.3.0 image is downloaded from PLDS, copy the software to a DVD as an ISO image. You must install System Manager 6.3.0 on System Platform **SP_6.3.4.08007.0** through CDOM Virtual Machine Solution Template before installing System Manager 6.3.8.

Download and install System Manager on VMware

#	Procedure	Notes
1.	Download and install “System Manager 6.3.0 VE OVA” from the Avaya PLDS website.	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. **File Name :** SMGR-6.3.0.8.5682-e50-64.ova **PLDS Download ID**: SMGR6310005 **Size**: 2929 MB / 2998350 KB **Md5sum**: 582af87e5f96acfcafe393968b3578c1
2.	Download and install the “System Manager 6.3.8 Software ” from the Avaya PLDS website.	**File Name :** System_Manager_6.3.8_r4502376.bin **PLDS download ID**: SMGR638001 **Size**: 1567 MB/ 1604087 KB **Md5Sum**: 8fb88372b51e4f7311c4f44e1e7055c6

Download and execute Data Migration Utility

This is required for upgrade workflow.

1.	Download and execute “**Data Migration Utility for System Manager 6.3.8 Software**”.	**File Name :** DMUtility_6.3.8_r4.bin **PLDS Download ID**: SMGR6380003 **Size**: 1 MB/ 392 KB **Md5sum**: d1860e77d7e70178cdb1ca836b6b1338

Known issues and workarounds

All the following issues are applicable to System Manager on System Platform and VMware

Problem	Keywords	Workaround
[wi01168920] False GR replication status on Primary System Manager	Geo-R	Restart system monitor service on System Manager
[wi01168927] Geo-R Health Status is not available primary System Manager	Geo-R	Restart system monitor service on System Manager
If Avaya Aura® System Manager Release 6.3.8 (SP8) or higher Releases are synchronizing with Avaya Aura® Communication Manager Release 6.2 ,and “CM Notify Sync” is being used, over-writable Communication Manager patch 21578 (02.0.823.0-21578.tar) must be activated on Communication Manager to allow “CM Notify Sync” to complete successfully. If Avaya Aura® System Manager Release 6.3.8 (SP8) or higher Releases are synchronizing with Avaya Aura® Communication Manager Release 6.3 ,and “CM Notify Sync” is being used, Security Service Pack (SSP) 3 (PLAT-rhel5.3-3014.tar.gz) must be activated on Communication Manager to allow “CM Notify Sync” to complete successfully.	Notify Sync	This patch is available on support.avaya.com under Avaya Aura® Communication Manager 6.2.x Downloads. This SSP is available on support.avaya.com under Avaya Aura® Communication Manager 6.3.x Downloads.
[wi01170452] User must change voice messaging password at next login" in Avaya Aura Messaging Release 6.3 template is not being set by default using System Manager web services with 3rd party provisioning tool.	Messaging	Directly login to the Avaya Aura Messaging system via SMI and set the ‘User must change voice messaging password at next login’ checkbox for just created via SMGR subscriber.
[wi01169724] – Branch Session Manager upgrade from 6.x to Branch Session Manager 6.3.8 (6.3.8.0.103011) and higher release using Software Management feature in System Manager get stuck due to EULA prompt.	BSM Upgrade	Contact Avaya Technical Support.
[wi01168540] Bulk Import fails using Complete XML with **Merge** or **Replace** option.	User Bulk Import	Exported XML needs to be converted to Partial / Delta XML and provide the updated XML for User Bulk Import using Merge / Replace option.
Domain synchronization does not work on AAC web console	Conferencing	>Domain is added automatically from System Manager to AAC when user with conferencing profile and appropriate domain is added. >Admin can login to Conferencing server (AAC Provisioning Client) and enter domains manually.
User with Conferencing Profile created in System Manager 6.2 GA (or SP4) cannot be exported in System Manager 6.3.8.	Conferencing	Login to System Manager 6.3.8 GUI, go to User Management page, find the

		user and click Edit button. Then on the Edit User page click Commit button. After this action the user can be exported successfully.
[wi01117419] Cleanup is not happening properly for un-installed license file.	License Management(WebLM)	After uninstalling a license file, click on “**WebLM Home**” or “**Server properties**” page to refresh the left navigation pane.
[wi01019992] No help link for CS 1000 and Call Pilot Synchronization on the Inventory landing page.	CS1000	None
[wi01140534] In VMware environment, the usage by WebLM page is not showing any data after deleting one of the local WebLM.	WebLM	Logout and login and then access the WebLM page to run usage query.
[wi01138339] Tenant Admin User page should not show the Public Contact and Shared Address links	Multi Tenancy	None
[wi01147606] Backup dates changes on different browsers.	Backup	None
[wi01147558] Multiple communication profile set creation is not showing Communication Managers in the drop down	Manage User	None
[wi01144975] Issues in Avaya AutoComplete component	Common Console	None
[wi01142601] Tenant Users can be created with elements which are not added in site details.	User Multi-Tenancy	None
[wi01141349] On System Manager SNMP Access web console there is no provision to handle IP **Addresses for SNMP Access**.	Upgrade	None
[wi01149062] Bulk import of users fails to valid the basic fields of User Provisioning rule.	User Bulk Import	None
[wi01166155] Cannot STOP "**Get Inventory**" / "**Analyze**" jobs from scheduler.	Inventory, Analyze	None
[wi01167015]Advance Search is not working for System Platform in Software Inventory.		None
[wi01166854] "**System Platform**" name is not displayed in Software inventory page; where as it displays names for other elements.	Software Inventory, Virtual Applications	None
[wi01166157] "**Get Inventory**" / "**Analyze**" job hangs on System Manager if both are started simultaneously.	Inventory, Analyze	Don’t perform/schedule both of them for same execution time
[wi01166362] Select some elements on Software Inventory for analyze, scheduler name is incorrect	Analyze	None
[wi01167116] Tree View in Software Inventory page in getting refreshed randomly.	Software Inventory	None
[wi01166850] The Analyze drop down menu overlaps with Show selection on Software Inventory page.	Software Inventory	None
[wi01167947]-PPR error on Software inventory page is coming	Pre-upgrade check	None

if we are trying to navigate to Software inventory page after starting Pre-upgrade check.		
[wi01166745] Cannot perform upgrade of Communication Manager 5.0 to 5.2.1 from Software inventory tree view.	Upgrade 5.0 Communication Manager	Use legacy page on System Manager i.e. Home / Services / Software Management / Manage Software / Communication Manager
[wi01169238] Communication Manager 5.2.1 upgrade fails due to validation of EPW file.	Upgrade 5.2.1 Communication Manager	Provide Gateway IP in the same subnet
[wi01160756] Implementing the integration comments for 6.X page and Branch Session Manager Patching	Upgrade 6.x, BSM	Provide password length less than 9 character
[wi01142376] xml file shows passwords in clear text for exported Elements	Element Bulk Export	None
[wi00875141] Complete replace of xml is not happening if we do changes in Communication profile set with same handle.	User Bulk Import	Use Merge option while importing xml.
[wi01138084] – Bulk Export from Command Line Interface does not work.	Bulk Export	None
[wi01155146] - Reverse proxy unconfigure fails to remove the Element Manager proxy link created	Reverse proxy	None
[wi01151350] Additional Role assigned to the tenant Administrator does not take effect and the authorized link is not listed in the Navigation Pane of the Tenant Admin Dashboard	Multi-Tenancy	None
[wi01111346] User can enable tenant management on VE Profile 2.	VMware	None
[wi01162468] “**Merge**" and "**Delete** "option for import of elements not working.	Element Bulk import	None
[wi01081272] – If we try to access the Reverse_proxy-> Launching ”Phone” link on Element Manager of CS1K then throws “**HTTP Status 404**”.	Reverse proxy	None
[wi01150504] - Quick Navigator doesn’t show the CS1K details as well as some details on Administrators page.	Common Console	None

Appendix

Log in to System Manager

System Manager CLI:

- You can gain access to the CLI with *admin* as the user name and *admin* as the password.

System Manager Web console:

- When you log in the System Manager console for the first time after a new installation, you **must** change the password. The procedure to change the password depends on whether you used an IP address or a domain name in the URL to open the Web console. To upgrade from 6.0, you **must** change the password**.** The admin password for the user interface is reset to the default when you upgrade from 6.0 to 6.1. For upgrades from 6.1 and later, you need not change the password.
- If you use a domain name to gain access to the Web console using the default **admin** password of **admin123**, the system prompts you to change the password after you log in.
- If you use an IP address in the URL to gain access to the Web console, press the change password link in the bottom-right corner of the login page and change the **admin** password. Use **admin123** as the current password.
- Use the FQDN, either by adding FQDN to DNS or by updating your computer host file, and add a line similar to: *135.9.1.2 smgr.dr.avaya.com.*
- Web login now enforces strict password rules. The rules for the password are on the Change Password page.

Note: The System Manager CLI admin user and System Manager Web console admin user are different users and independent of each other.

External authentication configuration

To reconfigure System Manager external authentication:

1. Click **Users** > **Administrators**.
2. In the navigation pane to the left**,** click **User Services** > **External Authentication** to modify external identity repositories.

To perform external authentication, enable the authentication when the primary System Manager server is installed and configured and before you install and configure the secondary System Manager server.

Login warning banner upgrade

To reconfigure the login warning banner:

1. Click **Users** > **Administrators.**
2. In the left navigation pane**,** select **Security** > **Policies**.
3. Click **Edit** and modify the login warning banner in the **Security Settings** section.

Internet Explorer compatibility

To switch off the compatibility mode:

1. On the browser menu, click **Tools** and select **Compatibility view setting**.
2. Clear the selected checkboxes.
   Ensure that the System Manager domain is not in the websites you added to the **Compatibility View** list.

To switch off the document mode:

1. On the browser menu, click **Tools** and select **Developer Tools**.
2. In the menu bar of the Developer Tools page, click **Document Mode to IE8 Standards**.

If you are using Internet Explorer 9, ensure that the System Manager URL is added in the trusted sites in the browser.

1. Click **Tools** and select **Internet Option**.
2. Click the **Security** tab and select **go to Trusted Sites**.
   If you add the URL in the browser, the system does not display a blank page when you open the System Manager URL.

If you cannot see the activation success or the failure status on GR console pages of the System Manager Web console using Internet Explorer browser, install a patch from Microsoft for IE to rectify this issue. For more information, see,

http://support.microsoft.com/kb/181050

The error occurs as Internet Explorer imposes a time-out limit for the server to return data.

Shell account

As the privileges for admin user are reduced, the admin user cannot run the standard service commands for JBoss *#service jboss start* and Postgres *#service postgresql start*

Instead two aliases are introduced:

- **smgr**: For System Manager JBoss **Usage : smgr {start|stop|restart|status}**

- **smgr-db**: For System Manager Postgres **Usage: smgr-db {start|stop|status|restart|condrestart|try-restart|reload|force-reload|initdb}**

These restrictions apply for the admin user only.

<u>CS1000 in System Manager geographic redundancy setup</u>

Primary state	Secondary state	CS1000 applications available from primary server	CS1000 applications available from secondary server
Active	Standby	- User Authentication and Authorization - Trust Management - Alarm Management (Display CS1000 Alarms) - Audit Log Collection - User Management of CS1000 & Call Pilot Endpoints - Deployment Manager - Patching Manager - SNMP Manager - IPSec Manager - Numbering Groups - Corporate Directory - Registration of new CS1000 member elements - Launching of Remote Element Managers	- User Authentication and Authorization. - Launching of Remote Element Managers
Down	Standby	None	- User Authentication and Authorization - Launching of Remote Element Managers
Down	Active	None	- User Authentication and Authorization - Launching of Remote Element Managers - Alarm Management (Display CS1000 Alarms) - Audit Log Collection

Technical support

Avaya Technical Support provides support for System Manager 6.3.8.

For any problems with System Manager 6.3.8, you can:

1. Retry the action. Carefully follow the instructions in the printed or online documentation.
2. See the documentation that is shipped with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the messages that the system displays. See the troubleshooting section of the Avaya product documentation.

If you continue to have problems, contact Avaya Technical Support by logging in to the Avaya Support website at http://support.avaya.com.

Before contacting Avaya Technical Support, keep the following information handy:

- Problem description.
- Detailed steps to reproduce the problem, if any.
- The release version in which the issue occurs.
  Note: To know the release version and build number, Log in to System Manager Web console. Click on the Settings icon (🔧) and navigate to About link. If System Manager Console is inaccessible, you can log in to System Manager SSH interface and run the **swversion command** to get the System Manager version.
- The status of the System Manager software. If the software is an upgrade, then the release from which the software is upgraded.
- All required log files. Run */opt/vsp/collectLogs.sh* script for collecting logs from the system.

You might be asked to send by email one or more files to Avaya Technical Support Team for analysis of your application and the environment.

For information about patches and product updates, see the Avaya Support website at http://support.avaya.com.