Avaya Aura® System Manager 6.3.16 Release Notes

Issue: 1.0

December 2015

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.

Contents

Introduction

This Release Notes gives you information about installation downloads and the supported documentation of Avaya Aura® System Manager Release 6.3.16. This Release Notes also contains information about features, known issues, and the possible workarounds in this Release. System Manager Release 6.3.16 is cumulative of System Manager Releases 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9, 6.3.10, 6.3.11, 6.3.12, 6.3.13, 6.3.14 and 6.3.15. System Manager 6.3.16 can be installed only on System Manager Release 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9, 6.3.10, 6.3.11, 63.12, 6.3.13, 6.314 or 6.3.15.

Note: If the deployed System Manager is 1.0.x, 5.2.x, 6.0.x, 6.1.x or 6.2.x release, you must upgrade older System Manager to System Manager Release 6.3.0, and then install System Manager 6.3.16. See "Upgrading to Avaya Aura System Manager to 6.3" to upgrade System Manager to System Manager Release 6.3.0.

If you are upgrading an older System Manager to System Manager Release 6.3.0 using the data migration utility, use the data migration utility on System Manager Release 6.3.8 and then install the System Manager 6.3.16 software. Do not run data migration utility on System Manager Release 6.3.16.

Upgrading System Manager 6.3.16 to 7.0 through Data Migration Utility Data_Migration_Utility_7.0.0.0_r81.bin is not supported so use the other Data Migration Utility available.

Product Support Notices

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

document.

To read a PSN description online:

1. Go to the Avaya Support website at http://support.avaya.com.

2. On the main menu, click Support by Product -> Documents.

3. In the **Enter Your Product Here** field, enter System Manager or select **Avaya Aura® System Manager** from the list.

4. In the **Choose Release** field, click **6.3.x**.

5. In the Content Type section, select **Product Support Notices**.

6. Click **Enter**.

7. Click the link to the specific PSN.

Problems fixed in Avaya Aura® System Manager 6.3.16

Resolved Issues	Keyword
SMGR-34575: In keeping with NIST guidelines and industry best practices, Avaya is rotating the security keys associated with remote maintenance access through the Avaya Security Gateway (ASG).	Infrastructure
SMGR-33675: Oracle Java Critical Patch Update (July 2015).	Security Updates
SMGR-32899: Oracle Java Critical Patch Update (October 2015).	Security Updates
SMGR-34410: High Vulnerabilities found with Oracle Java SE	Security Updates
SMGR-33257: [RHSA-2015:1664-01] Moderate: nss security, bug fix, and enhancement update	Security Updates
SMGR-33679: [RHSA-2015:1840-01] Important: openldap security update	Security Updates
SMGR-33598: [RHSA-2015:1706-01] Important: bind security update	Security Updates
SMGR-34366: Default passwords for users like admin/root must be forced to change after first boot.	Infrastructure
SMGR-34569-Define idle timeout explicitly in the data source to reduce the database connections.	Infrastructure
SMGR-34181: Update for Turkey DST 2015 changes	Infrastructure
SMGR-34174: System Manager (Quartz Component) sending traffic to external server (www.terracotta.org/157.189.192.67) for version update check.	Infrastructure
SMGR-33182: Disable JMS failure delivery to Dead Letter Queue to avoid unwanted memory accumulation.	Infrastructure
SMGR-34042: Remote SNMP Configuration audit logs show incorrect user details.	Alarm Management
SMGR-34153: When a large number of users greater than 100 are obtained after applying filter criteria on user management page then using the "Select All" option followed by More Action--> Export All Users does not export all the users obtained after filtering	Bulk Import Management
SMGR-34437: Unable to delete user permanently due to database constraints associated with user private contact and private contact information.	User Management
SMGR-34133: Unable to update user with Communication Profile password only if "History" is checked in Communication Profile Password Policy and also Enforce policy against previously used passwords is not getting applied to user while changing the communication profile password for a user.	User Management
SMGR-33579: Rename label "Authentication Type" to "User Type" in Identity section of User Management Page.	User Management
SMGR-33395: Password change for user from User Management removes the existing roles from User.	User Management
SMGR-33330: Updating the existing users for Avaya E164 handle with new directory synchronization mapping "Telephone Number -> Phone Number" will result in failure if the existing users are created through UPR and DSE having mapping "Telephone Number -> businessPhone"	User Management/ Directory Synchronization
SMGR-33211: Communication profile(SIP) password change done through self provisioning is not transmitted other elements like AAC so authentication is failing for member on AAC.	Self Provisioning Management

SMGR-33695: If telephone number in AD does not start with '+' prefix then the first digit of telephone number is getting replaced with prefix '+' in E164 handle.	User Provisioning Rule
SMGR-33694: Allow admin user to provide only '+' value in 'Prefix for Avaya E164 Handle' attribute in User Provisioning Rule configuration.	User Provisioning Rule
SMGR-32951: Provide correct error message if user creation is failed due to missing value for User Provisioning Rule name value in user's associated data in AD.	User Provisioning Rule
SMGR-32391: Certificates are not auto renewed on Secondary (standby) System Manager Server.	Trust Management
SMGR-32318: CND certificates are not renewed when other certificates are auto renewed.	Trust Management
SMGR-31570: Database (postgres) certificates are not renewed when other certificates are auto renewed.	Trust Management
SMGR-33725: Software Management/Software Inventory table is not showing proper data and also some time next page option is not available.	Software Upgrade Management
SMGR-33583: Analyze is not working as expected for Media Gateways and Media Modules if Hardware info is empty.	Software Upgrade Management
SMGR-32839: Scheduling more than one patch to apply on a CM is not working properly.	Software Upgrade Management
SMGR-31319: If user download file from PLDS using FTP protocol in Linux system, Download manager page show download has been completed 100 %,but actually file didn't get download the in software library.	Software Upgrade Management
SMGR-32874: Write community is not marked as mandatory while adding the SNMP detail of Communication Manager Inventory.	Software Upgrade Management
SMGR-33664: Manage/Unmanage displays in disabled mode for Messaging Element which is added after configuring Geo Redundancy.	Inventory Management
SMGR-33826: Feature buttons missing from station if station is created using custom template	Communication Manager Management
SMGR-34386: Unable to add buttons that have a second option via System Manager User Interface when the endpoint had a set type that is an alias.	Communication Manager Management
SMGR-34178: Endpoint data is getting replaced by other user's data if multiple users are accessing endpoint editor at same time.	Communication Manager Management
SMGR-33300: Init synch fails at audio groups.	Communication Manager Management
SMGR-33611: Stations available list show the station that are already in use while adding new station.	Communication Manager Management
SMGR-33844: Station profile settings revert back to default if station associated user's first name, last name, display name or extension voicemail, security code updated from User Management or Web Service or Directory Synchronization.	Communication Manager Management
SMGR-33965: Missing Label names on station form after changing the Endpoint Display Name on Identity tab of User Management.	Communication Manager Management
SMGR-33392: User associated with custom role unable to configure just buttons in spite of role having permission to edit the button.	Communication Manager Management
SMGR-32782: Adding a name with tilde characters on a CM station and running sync on SMGR deletes the feature button 9-24.	Communication Manager Management
SMGR-31806: Wrong System Manager administrator getting set on Communication Manager logs via the "change secondary-user" command before an administration task is performed.	Communication Manager Management

SMGR-32775: Global search filter does not open user details window if Localize Display name or Endpoint Display Name contains special characters like like ', :	Global Search Component

Note: System Manager 6.3.16 also contains the enhancements and fixes for System Manager Release 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9, 6.3.10, 6.3.11, 6.3.12, 6.3.13, 6.3.14 and 6.3.15.

Refer System Manager 6.3.15 release notes**:**
https://downloads.avaya.com/css/P8/documents/101015037

Refer System Manager 6.3.14 release notes**:**
https://downloads.avaya.com/css/P8/documents/101011431

Refer System Manager 6.3.13 release notes**:**
https://downloads.avaya.com/css/P8/documents/101009336

Refer System Manager 6.3.12 release notes**:**
https://downloads.avaya.com/css/P8/documents/101007304

Refer System Manager 6.3.11 release notes**:**
https://downloads.avaya.com/css/P8/documents/101004573

Refer System Manager 6.3.10 release notes**:**
https://downloads.avaya.com/css/P8/documents/100183189

Refer System Manager 6.3.9 release notes**:**
https://downloads.avaya.com/css/P8/documents/100182163

Refer System Manager 6.3.8 release notes**:**
https://downloads.avaya.com/css/P8/documents/100180576

Refer System Manager 6.3.7 release notes**:**
https://downloads.avaya.com/css/P8/documents/100179641

Refer System Manager 6.3.6 release notes**:**
https://downloads.avaya.com/css/P8/documents/100178113

Refer System Manager 6.3.5 release notes**:**
http://downloads.avaya.com/css/P8/documents/100176972

Refer System Manager 6.3.4 release notes**:**
http://downloads.avaya.com/css/P8/documents/100175426

Refer System Manager 6.3.3 release notes**:**
https://downloads.avaya.com/css/P8/documents/100173680

Refer System Manager 6.3.2 release notes**:**
https://downloads.avaya.com/css/P8/documents/100171755

Refer System Manager 6.3.1 release notes**:**
https://downloads.avaya.com/css/P8/documents/100169522

Known Issues

Table 4: Known limitations and workarounds in Avaya Aura® System Manager 6.3.16 Release

Problem	Keyword	Workaround
SMGR-28779: Exclude option is not working in Notification Filter.	Fault Management	Un-assign and assign Target Profiles.
SMGR-33437: Disable the JBoss automatic discovery happening on the default multicast address on 230.0.0.4.	Infrastructure	No workaround.
SMGR-30713: Encrypted alert packets being retransmitted even after connection reset from Session Manager.	Infrastructure	No workaround.
SMGR-28514: User having the System Admin role and authenticated using external authentication is accessing System Manager in following way with user id without full used id. • Using IP address • Using short FQDN instead of full FQDN So user will have following issues. a) User Management Create/Update/Delete/View operations. b) Access to Manage Elements, Element Type Access and Subnet Configuration pages from Inventory. c) Access to security page. d) All the buttons on Scheduler Pending/Completed page will be in disabled state. **Note:** Recommended access to System Manager is via FQDN.	Authentication	Login to System Manager using full login Id (i.e. example@domian.com) instead of just user id and schedule a job.
SMGR-29003: Signature information is missing intermittently in System Platform backup causing data restore to fail.	Backup and Restore	Perform restore using backup taken from System Manager Web console.
SMGR-27839: Data Replication between System Manager and other elements will fail if VFQDN value is greater than 50 characters.	Data Replication	Reconfigure VFQDN value with less than 50 characters using VFQDN change utility on System Manager.
SMGR-31356: GUI replication state shows "Repairing" for a node even after the Repair operation is completed.	Data Replication	Internally the initial sync completes, it only displays as "Repairing". Initiate a new repair from UI to fix the problem.
SMGR-28905: Problem with Geo enable replication operation with huge database after enable replication fails initially.	Geo Redundancy	Contact Avaya Support Team
SMGR-31346: Geo configuration fails when Primary System Manager has Sub CA configured.	Geo Redundancy	Contact Avaya Support Team
SMGR-29811: System Manager Primary server UI becomes very slow or unable to access when the secondary System Manager gets into a weird state. Whenever request is made on UI, Primary server waits till the connection times out - 5 minutes and navigates to the requested page.	Geo Redundancy	Restart JBoss service on Secondary System Manager Server.
Unable to access CS1K Elements from Secondary System Manager Web console once Secondary System Manager activated	Geo Redundancy/CS 1K	Refer PSN004598u for details.
SMGR-28978: User having custom role associated with permission on User Management unable to search users	User Management	No workaround.

from global user search filter.		
SMGR-28439: While adding new user(s), the default language preference is set to random language preference value.	User Management	No workaround.
SMGR-28840: If Tenant and sites are unchecked then all the users associated with the tenant are visible.	User Management	No workaround.
SMGR-34817: Last Name (Latin Translation) and First Name (Latin Translation) for user does not get updated if user is partial merged through Web Services or user bulk Import option.	User Management	Update the user completely through web Services or user bulk Import option.
SMGR-34422: SIP handle is not created for user through bulk edit user feature.	User Management	Create SIP handle manually for each user updated through bulk edit user feature.
SMGR-34021: Unable to delete user export job from export list if it is already deleted from scheduler.	Bulk User Export Management	No workaround.
SMGR-26743: Filter option is not available for User Provision Rules.	User Provisioning Rule	No workaround.
SMGR-34466: After upgrade to System Manager 6.3.15 or 6.3.16, view/edit/duplicate operations for existing User Provisioning rule may fail if Session Manager Profile with Secondary Session Manager is selected in existing rule.	User Provisioning Rule	Refer SOLN278139 for details.
SMGR-29039: Inventory jobs shows as Running on Web console but in database, jobs shows as completed	Discovery Management	Contact Avaya Support Team
SMGR-25823: Scheduled jobs created by a user with "administrative" privileges will start to fail once the user gets deleted from the system.	Scheduler Management	Delete the existing job and recreate with new admin user or modify the job with user existing in system.
SMGR-34782: User associated with Messaging System Admin role clicks on subscriber, response is not redirected to valid link, and it just hangs.	Role Management	Refer SOLN280163 for details.
SMGR-34780: The default 'Messaging System admin' role does not provide permission on Messaging Templates.	Role Management	Refer SOLN280163 for details.
SMGR-33013: Following Role names show an extra numeric value as ".20" instead of space. • SIP AS Auditor • SIP AS Security Administrator • SIP AS System Administrator	Role Management	No workaround.
SMGR-30008: After creating certificate signing request while creating Sub-CA of key size 4096 and SHA2, it still displays key size as 1024 and SHA1.	Trust Management	No workaround. Its display issue only but the internal values are correct.
SMGR-22580: Unable to see profile details in "Home / Services / Configurations / Settings / SMGR / Trust Management" if System Manager 6.3.x is upgraded from earlier releases.	Trust Management	Refer PSN004597u for details.
SMGR-29517: Unable to upgrade gateway if Communication Manager is lower version.	Software Upgrade Management	Contact Avaya Support Team
SMGR-32313: TN board status didn't change from "Schedule upgrade" to "Failed" if update gets failed while downloading	Software Upgrade	No workaround.

the file.	Management	
SMGR-27780: User can create two application system of type "CS 1000 Terminal Proxy server" with the same IP. This causes the CS1k and Session Manger registration to fail.	Inventory Management	Delete the application system with duplicate IP.
SMGR-30808: User cannot delete already defined report definition from Home / Services / Reports / Generation.	Communication Manager Management	No workaround.
SMGR-31678: Allow admin to decide if the end user is allowed to change the Autodial button address or not.	Communication Manager Management	No workaround
SMGR-34486: Initially CM is added in System Manager then later if a CM interchange happens due to which when admin executes the discovery in System Manager, after discovery the new active CM server as well be added so System Manager will sync with both Active and Standby CM servers.	Communication Manager Management	Contact Avaya Support Team
SMGR-34808: If an agent is updated using an agent template the skills are not updated properly.	Communication Manager Management	Update the agent again with correct skills.
SMGR-35115: Button labels/modules/profiles settings reverted back to default values in custom template if template is created from user management-> Endpoint Profile -> Endpoint Editor or Communication Manager -> Manage Endpoints section.	Communication Manager Management	Create custom template from Home / Services / Templates / CM Endpoint -> custom templates section.

System Manager Release 6.3.16 downloads

#	Action	Notes
1	Download and install the System Platform vsp-6.3.7.0.05001.iso image from the Avaya PLDS Web site. **Note**: This software is required if System Manager is System Platform based deployment.	Verify that the md5sum for the downloaded iso matches the md5sum on the Avaya PLDS Web site. File Name: vsp-6.3.7.0.05001.iso PLDS download ID: SMGR6314003 Size: 1.4 GB Md5Sum: 1f5e888f3a019dc96b459463ae8818fd
2	Download System Manager 6.3.16 bin file from the Avaya PLDS Web site.	Verify that the md5sum for the downloaded bin file matches the md5sum on the Avaya PLDS Web site. File Name: System_Manager_6.3.16_r5304210.bin PLDS download ID: SMGR6316001 Size: 1.7 GB Md5Sum: 19b46e460baa30efaf1ba8c957c67e99

Points to remember before installation

If System Manager is a System Platform-based deployment

- **Perform backup operation from System Platform Web Console.**

- **Upgrade System Platform to vsp-6.3.7.0.05001.**

- **For Service Pack installation, iptables service should be in default state (ON).**

  Note: If iptables service is turned off on the System Manager Server, then service pack installation will not proceed, also admin should not override/change existing iptables configurations (if it has been stopped, to add new configurations).

- **For Service Pack installation, geographic redundancy replication should be in disabled state.**

  Note: If geographic redundancy replication service is in enabled state, then service pack installation will not proceed.

- **Apply this service pack on both System Manager servers which are used for geographic redundancy configuration.**

- **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.

- **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.**

- **If the Patch deployment is not committed after installation and the VM is rebooted it will roll back to previous state and changes made to System Manager after patch installation will be lost.**

If System Manager is a Virtualization Enablement (VMWare) environment-based deployment

- **Perform VMWare snapshot of the System Manager VM.**

  A snapshot preserves the state and data of a virtual machine at a specific point in time. Snapshots consume large amounts of data resources, increase CPU loads on the host, and affect performance and service.

  Note: Verify that the patch installation or upgrade is successful, and ensure that the virtual application is functional. You can then delete the snapshot.

- **Perform backup operation from System Manger Web Console.**

- **For Service Pack installation, iptables service should be in default state (ON).**

  Note: If iptables service is turned off on the System Manager Server, then service pack installation will not proceed, also admin should not override/change existing iptables configurations (if it has been stopped, to add new configurations).

- **For Service Pack installation, geographic redundancy replication should be in disabled state.**

  Note: If geographic redundancy replication service is in enabled state, then service pack installation will not proceed.

- **Apply this service pack on both System Manager servers which are used for geographic redundancy configuration.**

- **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.

Points to remember:

1. Auto-activation of serviceability agents:
   - For NEWLY installed elements (with new Serviceability Agent) that are bundled with 6.3.16, you do not need to manually activation of the agents through 'Manage Serviceability Agent' page.
   - These agents will be auto-activated by the System Manager and hence these will be displayed with 'Active' status in the serviceability agent list.
   - User can therefore directly assign the target/user profiles onto such agents.
   - Please note that this functionality is only applicable to the serviceability agents with version 6.3.5 onwards.

2. Setting up the Alternate Source:
   - Keep the note while setting up the alternate source, few firmware files for System Platform based Communication Manager should be kept inside directory named by PLDSID e.g. if you want to place the 6.3.0.0.1105.iso then you need to create directory named CM000000300 and place the file inside this.
     - This should be done for following type of firmware:
       - ➢ VSP iso
       - ➢ Template iso
       - ➢ BSM iso

Installing the Service Pack

Before you begin:

System Manager 6.3.16 can be installed only on System Manager Release 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9, 6.3.10, 6.3.11, 6.3.12, 6.3.13, 6.3.14 and 6.3.15.

Note: If the deployed System Manager is Release 1.0.x, 5.2.x, 6.0.x, 6.1.x, or 6.2.x, you need to upgrade older System Manager to System Manager Release 6.3.0, prior to System Manager 6.3.16 installation. Refer "Upgrading to Avaya Aura System Manager to 6.3" to upgrade System Manager to System Manager Release 6.3.0.

If you are upgrading older System Manager to System Manager Release 6.3.0 using data migration utility, use the data migration utility on System Manager Release 6.3.8 and then install the System Manager 6.3.16 software. Do not use data migration utility on System Manager Release 6.3.16.

To determine the System Manager Release 6.3.x that is running:

 ➢ Log on to the System Manager Web console.

 ➢ On the home page, click the settings ( ) icon and then click **About**. Verify that the About page contains:

Release	About Content
6.3	System Manager 6.3.0 - GA
6.3.1	System Manager 6.3.0 - Service Pack1
6.3.2	System Manager 6.3.0 - FP2
6.3.3	System Manager 6.3.3
6.3.4	System Manager 6.3.4
6.3.5	System Manager 6.3.5
6.3.6	System Manager 6.3.6
6.3.7	System Manager 6.3.7
6.3.8	System Manager 6.3.8
6.3.9	System Manager 6.3.9
6.3.10	System Manager 6.3.10
6.3.11	System Manager 6.3.11
6.3.12	System Manager 6.3.12
6.3.13	System Manager 6.3.13
6.3.14	System Manager 6.3.14
6.3.15	System Manager 6.3.15

• Make sure that the existing System Manager is installed and is operational. To check the application state, log on to the System Manager web console with admin credentials.

Avaya Aura System Manager 6.3.16 DVD details:
• Avaya Aura® System Manager 6.3.16 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 6.3.16 -Software Update Revision No: 6.3.16.13.4210)
- If you have installed release earlier than System Manager 6.3.0, install DVD 1 of 2 first and then DVD 2 of 2.
- If you already have installed System Manager Release 6.3.0 and above, directly install DVD 2 of 2.

Installing the service pack through System Platform Web Console

1. Log on to System Platform Web Console with admin credentials.

2. Download the service pack:

    a. Click **Server Management > Patch Management**.

    b. Click **Download/Upload**.

    c. On the Search Local and Remote Patch page, select the location to search for the service pack from the following list:

    - **Avaya Downloads (PLDS)**

    - **HTTP**

    - **SP Server**

    - **SP CD/DVD**

    - **SP USB Disk**

    - **Local File System**

    d. If you select **HTTP** or **SP Server**, provide the URL to the service pack.

    e. In case of **HTTP**, click **Configure Proxy** to specify a proxy server if required.

    f. If you select **Local File System**, click **Add** to locate the service pack file on your computer and then upload.

    g. Use **Search** to search the required service pack.

    h. Choose the service pack, and click **Select**.

3. Install the service pack by performing the following:

    a. Select **Server Management > Patch Management**.

    b. Click on **Manage**.

    c. On the Patch List page, the status of the patch ID **System_Manager_R6.3.16_5304210** must be **Not Installed.**

    d. Click on a patch ID **System_Manager_R6.3.16_5304210** to see the details.

    e. On the Patch Detail page, click **Install**.

    f. Wait for the patch installation to complete.

4. Verify the service pack installation using one of the following ways:

    ➢ **From System Platform Web Console:**

    a. Log on to System Platform Web Console with admin credentials

    b. Click **Server Management > Patch Management**.

    c. Click **Manage**.

    d. On the Patch List page, verify that the status of the patch ID, **System_Manager_R6.3.16_5304210**, is **Pending.**

    If the status is:

    Pending - The service pack is applied and must be committed or rolled back.

Installed - The service pack is in the installed state.

Not Installed - The service pack is not installed. Installation has failed.

➢ **From System Manager Web Console:**

- Log on to the System Manager web console.

- On the top-right corner click the Settings ( ) icon, and click **About**. Verify that the About page displays:

    System Manager 6.3.16

    Build No. - 6.3.0.8.5682-6.3.8.5709

    Software Update Revision No: 6.3.16.13.4210

5. On the System Platform web console, perform one of the following:

    a. If the Service Pack installation is successful, commit the service pack installation using the following

    steps:

    1. Click **Server Management > Patch Management**.

    2. Click **Manage**.

    3. On the Patch List page, the status of the patch ID **System_Manager_R6.3.16_5304210** must be

       Pending.

    4. Click the patch ID **System_Manager_R6.3.16_5304210** to see the details.

    5. On the Patch Detail page, click **Commit**.

    b. If the Service Pack installation fails, click **Rollback**.

6. After you upgrade the system to 6.3.16, **reboot** the System Manager from System Platform web console or from

    System Manager CLI to get the updated kernel running in memory.

Installing the service pack through System Manager Command Line Interface (CLI) for Virtualization Enablement (VMWare) environment

1. Create a snapshot of System Manager virtual machine.

    Note: This activity might impact the services of System Manager and not of any other Avaya Aura Products like

    Session Manager/Presence Server/Communication Manager etc.

2. Copy the patch installer file to the System Manager server.

3. Log in to the System Manager virtual machine as admin.

4. Verify md5sum of the **bin** file with the value from PLDS. (**19b46e460baa30efaf1ba8c957c67e99**).

5. Run the patch installer using the following command:

    # SMGRPatchdeploy <absolute path to the System_Manager_6.3.16_r5304210.bin file>

    Note: you will be prompted to accept the EULA. You must accept the EULA inorder to install the patch.

6. Wait for the system to execute the patch installer and display the installer prompt.

7. Verify the service pack installation from below steps

    - Log on to the System Manager Web console.

- On the top-right corner click on the settings ( ) icon and then select **About**. Verify that About page contains as below:

  System Manager 6.3.16

  Build No. - 6.3.0.8.5682-6.3.8.5709

  Software Update Revision No: 6.3.16.13.4210

Note: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.

8. If the Service Pack installation fails, use the VM snapshot manager to revert to a snapshot taken prior to patch installation.

9. After you upgrade the system to service pack 6.3.16, **reboot** the System Manager from System Manager CLI to get the updated kernel running in memory.

Technical support

Avaya Technical Support provides support for System Manager 6.3

If you find any problems with System Manager 6.3.x:

- Retry the action. Carefully follow the instructions in the printed or online documentation.
- See the documentation that ships with your hardware for maintenance or hardware-related problems.
- Note the sequence of events that led to the problem and the exact messages that the system displays. For more information, see the troubleshooting section of the Avaya product documentation.

If you continue to have problems, contact Avaya Technical Support using one of the following methods:

- Log on to the Avaya Support website at **http://support.avaya.com**.
- Call or send a fax message to Avaya Support on one of the telephone numbers in the Support Directory listings on the Avaya Support website.

Using Avaya Global Services Escalation Management, you can escalate urgent service issues. For more information, see the list of Escalation Contacts on the Avaya Support website.

Before contacting Avaya 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 on to System Manager and click the settings ( ) icon and then click **About** on the dashboard.

- The status of the System Manager software. If the software is an upgrade, provide the current release number.
- The log files.
    a. Execute following command from System Manager CLI with root user credentials to collect logs

       #sh /opt/vsp/collectLogs.sh -Db -Cnd

       This will create a file (**LogsBackup_xx_xx_xx_xxxxxx.tar.gz**) @ /tmp location.

Contact support tasks

Avaya Support might request for email notification files for analysis of your application and the application environment.

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

Appendix A: Compatibility matrix for the System Manager 6.3.x and System Platform software versions

System Manager 6.3		System Platform	
Release	Build Number	Release	Required Patch
6.3	System Manager 6.3.0 - GA Build No. - 6.3.0.8.5682-6.3.8.818 Software Update Revision No: 6.3.0.8.923	6.2.1.0.9	6.2.2.06002.0
6.3.1	System Manager 6.3.0 - Service Pack1 Build No. - 6.3.0.8.5682-6.3.8.859 Software Update Revision No: 6.3.1.9.1212	6.2.1.0.9	6.2.2.08001.0
6.3.2	System Manager 6.3.0 - FP2. Build No. - 6.3.0.8.5682-6.3.8.1627 Software Update Revision No: 6.3.2.4.1399	6.3.0.0.18002	
6.3.3	System Manager 6.3.3 Build No. - 6.3.0.8.5682-6.3.8.1814 Software Update Revision No: 6.3.3.5.1719	6.3.0.0.18002	
6.3.4	System Manager 6.3.4 Build No. - 6.3.0.8.5682-6.3.8.2631 Software Update Revision No: 6.3.4.4.1830	6.3.0.0.18002	6.3.1.08002.0
6.3.5	System Manager 6.3.5 Build No. - 6.3.0.8.5682-6.3.8.2807 Software Update Revision No: 6.3.5.5.1969	6.3.0.0.18002	6.3.1.08002.0
6.3.6	System Manager 6.3.6 Build No. - 6.3.0.8.5682-6.3.8.3007 Software Update Revision No: 6.3.6.6.2103	6.3.0.0.18002	6.3.1.08002.0
6.3.7	System Manager 6.3.7 Build No. - 6.3.0.8.5682-6.3.8.3204 Software Update Revision No: 6.3.7.7.2275	6.3.0.0.18002	6.3.1.08002.0
6.3.8	System Manager 6.3.8 Build No. - 6.3.0.8.5682-6.3.8.4219 Software Update Revision No:6.3.8.5.2376	6.3.0.0.18002	6.3.4.08007.0
6.3.9	System Manager 6.3.9 Build No. - 6.3.0.8.5682-6.3.8.4414 Software Update Revision No: 6.3.9.1.2482	6.3.0.0.18002	6.3.4.08007.0
6.3.10	System Manager 6.3.10 Build No. - 6.3.0.8.5682-6.3.8.4514 Software Update Revision No: 6.3.10.7.2656	6.3.0.0.18002	6.3.5.01003.0

6.3.11	System Manager 6.3.11 Build No. - 6.3.0.8.5682-6.3.8.4711 Software Update Revision No: 6.3.11.8.2871	6.3.0.0.18002	6.3.5.01003.0
6.3.12	System Manager 6.3.12 Build No. - 6.3.0.8.5682-6.3.8.4903 Software Update Revision No: 6.3.12.9.3022	6.3.0.0.18002	6.3.5.01003.0
6.3.13	System Manager 6.3.13 Build No. - 6.3.0.8.5682-6.3.8.5108 Software Update Revision No: 6.3.13.10.3336	6.3.0.0.18002	6.3.6.01005.0
6.3.14	System Manager 6.3.14 Build No. - 6.3.0.8.5682-6.3.8.5304 Software Update Revision No: 6.3.14.11.3595	6.3.7.0.05001	
6.3.15	System Manager 6.3.15 Build No. - 6.3.0.8.5682-6.3.8.5506 Software Update Revision No: 6.3.15.12.3972	6.3.7.0.05001	
6.3.16	System Manager 6.3.16 Build No. - 6.3.0.8.5682-6.3.8.5709 Software Update Revision No: 6.3.16.13.4210	6.3.7.0.05001	