Avaya Aura® System Manager 6.3.22 Release Notes

Issue: 1.0

August 2018

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 6.3.22. This Release Notes also contains information about features, known issues, and the possible workarounds in this Release. System Manager Release 6.3.22 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, 6.3.15, 6.3.16, 6.3.17, 6.3.18, 6.3.19, 6.3.20 and 6.3.21. System Manager 6.3.22 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, 6.3.15, 6.3.16, 6.3.17, 6.3.18, 6.3.19 or 6.3.20 or 6.3.21.

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 using the instructions in "Upgrading to Avaya Aura System Manager to 6.3" , to upgrade to System Manager 6.3.22.

To upgrade an older System Manager release to System Manager Release 6.3.0, use the data migration utility on System Manager Release 6.3.8, and then install the System Manager 6.3.22 software. Do not run data migration utility on System Manager Release 6.3.22.

IMPORTANT NOTE:

> ➢ System Manager Release 6.3.22 can not be migrated to System Manager Release 7.0.x release using the data migration utility.
> ➢ System Manager Release 6.3.22 can not be migrated to System Manager Release 7.1.0.0, 7.1.1.0, 7.1.1.1 and 7.1.2.0 releases using the data migration utility.
> ➢ System Manager Release 6.3.22 can be migrated to System Manager Release 7.1.3.0 and higher releases using the data migration utility.

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 6.3.22

Resolved Issues	Keyword
SMGR-46330: Oracle Java Critical Patch Update (July 2018).	Security Updates
SMGR-46052: On System Manager list vdn reports show skewed output.	Communication Manager Management

Note: System Manager 6.3.22 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, 6.3.15, 6.3.16, 6.3.17, 6.3.18, 6.3.19, 6.3.20 and 6.3.21.

Refer System Manager 6.3.21 release notes**:**
https://support.avaya.com/css/P8/documents/101047834

Refer System Manager 6.3.20 release notes**:**
https://support.avaya.com/css/P8/documents/101042938

Refer System Manager 6.3.19 release notes**:**
https://downloads.avaya.com/css/P8/documents/101036903

Refer System Manager 6.3.18 release notes**:**
https://downloads.avaya.com/css/P8/documents/101029130

Refer System Manager 6.3.17 release notes**:**
https://downloads.avaya.com/css/P8/documents/101020643

Refer System Manager 6.3.16 release notes**:**
https://downloads.avaya.com/css/P8/documents/101017579

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

Known limitations and workarounds in Avaya Aura® System Manager Release 6.3.22

Problem	Keyword	Workaround
SMGR-28779: Exclude option is not working in Notification Filter.	Fault Management	Un-assign and assign Target Profiles.
SMGR-30713: Encrypted alert packets being retransmitted even after connection reset from Session Manager.	Infrastructure	No workaround.
SMGR-28514: User with the System Admin role and authenticated using external authentication is accessing System Manager in following way with user ID without complete used ID. • Using IP address • Using short FQDN instead of full FQDN User will have the 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 through FQDN.	Authentication	Login to System Manager using the full login ID instead of just user ID and then schedule a job. For example@domian.com.
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-39654: Data Replication between System Manager and other elements stuck in ready for repair if element FQDN length greater than 50 characters.	Data Replication	Reconfigure element with FQDN length less than 50 characters.
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
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 from global user search filter.	User Management	No workaround.
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.

Problem	Keyword	Workaround
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-37712: Remote Backup not working if the remote system is a Communication Manager.	Backup and Restore	Use different remote server for remote backup.
SMGR-26743: Filter option is not available for User Provision Rules.	User Provisioning Rule	No workaround.
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.
SMSG-732: 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-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-35692: If you create a role which is a "copy all" from the Auditor role it enabled the "Administrators" link and when user adds the Communication Manager Auditor role to the role it still allows the creation or edit of stations and other CM objects that are managed via System Manager.	Role Management	Instead of "copy all" create new role.
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-35119: Select any "Discover Profile" field under Discover Profile table and click on delete. The Profile that you selected for delete and profile that pop on Delete page is different in some cases.	Software Upgrade Management	No Workaround
SMGR-32313: TN board status didn't change from "Schedule upgrade" to "Failed" if update gets failed while downloading the file.	Software Upgrade Management	No workaround.
Upgrade failure noticed during System Platform based Communication Manager (Survivable Remote Embed solution template) from System Manager Inventory Management (Home / Services / Software Management / Software Inventory) to latest 6.x release which consists of Branch Session Manager as one of the VM.	Inventory Management	Before initiating upgrade, BSM VM must be placed in 'Deny New Service' mode from Session Manager Dashboard. Steps to make BSM VM in 'Deny New Service' mode 1. Go to Home / Elements / Session

Problem	Keyword	Workaround
		Manager / Dashboard.
		2. Select the required BSM from Session Manager Instance's table.
		3. Click on 'Service State' button -> Select the selection as 'Deny New Service' from drop-down list.
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

System Manager Release 6.3.22 downloads

#	Action	Notes
1	Download and install the System Platform vsp-6.4.0.0.17006.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-6.4.0.0.17006.iso PLDS download ID: SMGR6318003 Size: 1,641.49 MB Md5Sum: c47457bda5fb70fb752b808ddb5fe668
2	Download System Platform vsp-patch-6.4.3.0.01002.noarch.rpm from the Avaya PLDS Web site and install on vsp-6.4.0.0.17006.iso image. **Note**: This software is required if System Manager is System Platform based deployment.	Verify that the md5sum for the downloaded rpm matches the md5sum on the Avaya PLDS Web site. File Name: vsp-patch-6.4.3.0.01002.noarch.rpm PLDS download ID: SMGR6322GA3 Size: 464 MB Md5Sum: 16cd2a2b8d78975f3fac2625eea4a63e
3	Download System Manager 6.3.22 bin file from the Avaya PLDS website.	Verify that the md5sum for the downloaded bin file matches the md5sum on the Avaya PLDS Web site. File Name: System_Manager_6.3.22_r5908226.bin PLDS download ID: SMGR6322GA1 Size: 1888 MB Md5Sum: e2c5060fc5b1f01479159d0346b3e863

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 6.4.3.0.01002.**

- **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 6.3.22, you do not need to manually activate agents from the 'Manage Serviceability Agent' page.
   - These agents will be auto-activated by 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.
   - This functionality applies only 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 6.3.22 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, 6.3.15, 6.3.16, 6.3.17, 6.3.18, 6.3.19, 6.3.20 and 6.3.21.

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 6.3.22 installation. Refer "Upgrading to Avaya Aura System Manager to 6.3" to upgrade System Manager to System Manager Release 6.3.0.

To upgrade an older System Manager release to System Manager Release 6.3.0, use the data migration utility on System Manager Release 6.3.8 and then install the System Manager 6.3.22 software. Do not use data migration utility on System Manager Release 6.3.22.

IMPORTANT NOTE:

➢ System Manager Release 6.3.22 can not be migrated to System Manager Release 7.0.x release using the data migration utility.
➢ System Manager Release 6.3.22 can not be migrated to System Manager Release 7.1.0.0, 7.1.1.0, 7.1.1.1 and 7.1.2.0 releases using the data migration utility.
➢ System Manager Release 6.3.22 can be migrated to System Manager Release 7.1.3.0 and higher releases using the data migration utility.

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
6.3.16	System Manager 6.3.16

6.3.17	System Manager 6.3.17
6.3.18	System Manager 6.3.18
6.3.19	System Manager 6.3.19
6.3.20	System Manager 6.3.20
6.3.21	System Manager 6.3.21

- Ensure 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.

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_R6.3.22_5908226** must be **Not Installed.**
   d. Click on a patch ID **System_Manager_R6.3.22_5908226** 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 by using one of the following:
   ➢ **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_R6.3.22_5908226**, 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 then click **About**. Verify that the About page displays:

    System Manager 6.3.22

    Build No. - 6.3.0.8.5682-6.3.8.6302

    Software Update Revision No: 6.3.22.19.8226

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_R6.3.22_5908226** must be **Pending**.

    4. Click the patch ID **System_Manager_R6.3.22_5908226** 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 6.3.22, **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

Note: Patch install will not work with ASG login's init/inads and craft user. You must login as admin user to perform patch installation.

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. (e2c5060fc5b1f01479159d0346b3e863).

5. Run the patch installer using the following command:

    # SMGRPatchdeploy <absolute path to the System_Manager_6.3.22_r5908226.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. To verify the service pack installation, do the following:

   a. Log on to the System Manager Web console.

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

   System Manager 6.3.22

   Build No. - 6.3.0.8.5682-6.3.8.6302

   Software Update Revision No: 6.3.22.19.8226

   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 6.3.22, **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, 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

System Manager 6.3		System Platform	
Release	Build Number	Release	Required Patch
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	
6.3.17	System Manager 6.3.17 Build No. - 6.3.0.8.5682-6.3.8.5810 Software Update Revision No: 6.3.17.14.4616	6.3.7.0.05001	6.3.8.01002.0
6.3.18	System Manager 6.3.18 Build No. - 6.3.0.8.5682-6.3.8.5906 Software Update Revision No: 6.3.18.15.5487	6.4.0.0.17006	
6.3.19	System Manager 6.3.19 Build No. - 6.3.0.8.5682-6.3.8.6008 Software Update Revision No: 6.3.19.16.6363	6.4.0.0.17006	
6.3.20	System Manager 6.3.20 Build No. - 6.3.0.8.5682-6.3.8.6107 Software Update Revision No: 6.3.20.17.6951	6.4.0.0.17006	6.4.1.0.01008
6.3.21	System Manager 6.3.21 Build No. - 6.3.0.8.5682-6.3.8.6211 Software Update Revision No: 6.3.21.18.7738	6.4.0.0.17006	6.4.2.0.01003
6.3.22	System Manager 6.3.22 Build No. - 6.3.0.8.5682-6.3.8.6302 Software Update Revision No: 6.3.22.19.8226	6.4.0.0.17006	6.4.3.0.01002