Avaya Aura® System Manager 6.3.13 Release Notes

Issue: 1.0

April 2015

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

© 2015 Avaya Inc. All Rights Reserved.

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.

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

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.

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

Contents

Introduction....6
Product Support Notices....6
New Features in Avaya Aura® System Manager 6.3.13....7
Problems fixed in Avaya Aura® System Manager 6.3.13....8
Operational Assistance....12
System Manager Release 6.3.13 downloads....15
Points to remember before installation....15
If System Manager is a System Platform-based deployment....15
If System Manager is a Virtualization Enablement (VMWare) environment-based deployment....16
Installing the Service Pack....17
Installing the service pack through System Platform Web Console....18
Installing the service pack through System Manager Command Line Interface (CLI) for Virtualization Enablement (VMWare) environment....19
Technical support....21
Appendix A: Compatibility matrix for the System Manager 6.3.x and System Platform software versions....22

Copyright 2015 Avaya Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy

Introduction

This Release Notes gives you information about installation downloads and the supported documentation of Avaya Aura® System Manager Release 6.3.13. This Release Notes also contains information about features, known issues, and the possible workarounds in this Release. System Manager Release 6.3.13 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 and 6.3.12. System Manager 6.3.13 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 or 6.3.12.

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 6.3.13. 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 6.3.13 software. Do not run data migration utility on System Manager Release 6.3.13.

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 **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.

Copyright 2015 Avaya Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy

New Features in Avaya Aura® System Manager 6.3.13

Localization: Provided support to localize the User Interface (UI) and support is only for Canadian French in several areas of the UI.
Note: The entire UI will not be available for localization in this release.
Following UI only supports the localization:

1. Authentication and landing pages
2. User Management pages.
   - In "Communication Profile", translation will be done for Session Manager, Communication Manager and Messaging Profile.

   Note: Translation will not be done for following pages.

   - Password change/management pages
   - In "Communication Profile", Profiles for Collaboration Environment, CS1000, Callpilot, IP Office, Presence, Conferencing, and Work Assignment.
   - "Membership" and "Contact" pages.

3. Communication Manager Management
   - Edit Endpoint Extension in "Manage Endpoints" page.
   - Release Endpoint, Busyout Endpoint, Test Endpoint, List Trace Station and Status Station pages In "Maintenance"
   - General Options, Group Membership, Feature Options, Site Data, Abbreviated Call Dialing, Enhanced Call Fwd, Button Assignment and Profile Settings in "Edit Endpoint" pages.

4. Messaging Management
   - Basic Information, Subscriber Directory, Subscriber Security, Mailbox Features, Secondary Extensions and Miscellaneous in "Messaging → Subscriber → Edit Subscriber"

Follow the below steps to get the support for localization for French language:

1. Login to System Manager CLI using root credentials.
2. Execute below command:
   #service jboss stop
3. Execute below command once the JBoss service is stopped.
   #sh $MGMT_HOME/CommonConsole/script/LocalizationScript.sh
   $MGMT_HOME/CommonConsole/localization/common_console/FrenchResourceBundle.zip

Note: JBoss service will be restarted during this activity so System Manager Web console will not be accessible.
If System Manager is in Geo Redundancy Mode then apply above steps on Secondary System Manager also.

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

Problems fixed in Avaya Aura® System Manager 6.3.13

Resolved Issues	Keyword
SMGR-29033: [RHSA-2014:1653-01] Moderate: openssl security update.	Security Updates
SMGR-30498: [RHSA-2015:0164-01] Moderate: kernel security and bug fix update	Security Updates
SMGR-30364: [RHSA-2015:0090-01] Critical: glibc security update.	Security Updates
SMGR-30002: [RHSA-2014:1948-01] Important: nss, nss-util, and nss-softokn security, bug fix, and enhancement update.	Security Updates
SMGR-30000: [RHSA-2014:2008-01] Important: kernel security update.	Security Updates
SMGR-29692: Fix for Security Vulnerabilities.	Security Updates
SMGR-31072: 17. Change of supported ssh ciphers causes Network Parameter Changes to fail for Midsize Enterprise solution	Infrastructure
SMGR-30607: Fix for Leap Second To Be Inserted June 30, 2015	Infrastructure
SMGR-30388 : Oracle Java Critical Patch Update (January 2015)	Infrastructure
SMGR-30870: Fix for POODLE vulnerability.	Infrastructure
SMGR-30849: Daily vacuum cron job does not work properly.	Infrastructure
SMGR-30485: IP change for System Manager does not update elements of type UCMApp.	Infrastructure
SMGR-30714: System Manager also allows client certificate logins for non-Avaya technician users.	Authentication Management
SMGR-30775: Legacy certificate expiry (alias-isable) can make Geo Redundancy Secondary UI inaccessible.	Trust Management
SMGR-30439: Large SVAR files (Snap-Ins for Engagement Development Platform) will cause backup to fail.	Backup and Restore
SMGR-30606: User Management UI and Bulk Import allow creating XMPP handle with two "@" symbols which cause issue with Presence element.	Bulk Import/ User Management
PRES-3886: Users add/edit operation will fail if user(s) is associated with Communication Manager and Presence Profile, if the operation is performed through bulk import or Directory Synchronization or Web Service.	Bulk Import Management Directory Synchronization
SMGR-29025: Import of user with complete+replace option removes presence handle from user.	Bulk Import Management
SMGR-30428: Selection of record(s) from Manage Jobs records or loading of Manage Import Jobs screen is very slow.	Bulk Import Management
SMGR-30377: Details of time stamp and received time stamp for an alarm record in mail, is appended with server time zone instead of UTC time zone	Fault Management
SMGR-30542: Pull request for a node should not be processed by DRS (Symmetric) if node is marked for Audit.	Data Replication
SMGR-28878: Unable to edit/delete an address if only one address record is associated with user.	User Management
SMGR-28907: Unable to delete user in certain scenario i.e. delete user fails while deleting contact list member reference.	User Management
SMGR-30771: Global search component is not providing proper results for users on	User Management

Copyright 2015 Avaya Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy

search after System Manager upgrade.	
SMGR-30416: For First Name and Last Name Latin translation fields, only ł and Ł polish characters are not converting properly. Note: Follow the below steps to correct existing user records associated with these ł and Ł polish characters and this should be done during maintenance window. 1. Login to System Manager CLI using root credentials. 2. Stop JBoss service using below command: #service jboss stop 3. Once the JBoss stopped, execute below command #sh /opt/Avaya/Mgmt/6.3.8/upm/sql/postgres/polish_char_update.sh 4. Restart JBoss Service using below command. #service jboss start Note: Wait for 15 minutes. 5. Log on to System Manager Web Console. 6. Perform repair for all the Session Managers.	User Management
SMGR-29526: User(s) always getting modified in data source synchronization if any attribute from data source is mapped to System Manager street address attribute	Directory Synchronization
SMGR-30414: If bi-directional mapping is done with telephone number from data source to Communication Manager Extension, data source synchronization does not update "telephone Number" in data source, if the value for attribute “telephone number” is not set in external server	Directory Synchronization
SMGR-30414:0020If bi-directional mapping is done with telephone number from data source to Phone Number (E164 handle), User(s) always getting modified in data source synchronization if the users are not configured with E164 handle value in System Manager	Directory Synchronization
SMGR-28977: Unable to delete Directory Synchronization job from Home / Users / Directory Synchronization / Sync Users-Active Synchronization Jobs section, if the job is already disabled on Scheduler.	Directory Synchronization
SMGR-30909: Unable to view Communication Manager details if Communication Manager is associated with SNMP attributes and if page is first opened in View mode and click on Edit Button.	Inventory Management
SMGR-31013: "Select Profile(s) to Create on Device(s)" shows no records after successful SNMP V3 profile add to Manage Elements	Inventory Management
SMGR-30665: When refresh button is clicked 'select All' button gets checked on the 'Select Profile(s) to Create on Device(s)' table	Inventory Management
SMGR-30666: Newly added ssh or snmp profiles are not visible in the profile list table.	Inventory Management
SMGR-28623: Advance Search is not working for System Platform device.	Inventory Management
SMGR-30483: Unable to edit IP address of element in inventory due to transaction getting timeout	Inventory Management
SMGR-30246: Enhancement done to reduce "Discovery" job execution time.	Discovery Management
SMGR-30238: Communication Manager Discovery does not happen if AES128 is selected from Privacy Type Drop down in SNMP profile.	Discovery Management
SMGR-30482: Get Inventory fails with error “EJB Transaction Rolled back Exception: deleted entity passed to persist”.	Software Upgrade Management
SMGR-30984: Upgrade of System Platform Template from 6.2.2 to 6.3.X fails if System Platform upgrade is done through Software Upgrade Management.	Software Upgrade Management
SMGR-29940: Unable to handle space provided for 'ServerPath' in Software Library UI.	Software Upgrade

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

	Management
SMGR-28430: On Subnet Configurations, Save and Cancel Buttons are getting enabled/disabled in weird manner.	Software Upgrade Management
SMGR-30500: Downloads not managed by PLDS (i.e. managed in SFAP only) are showing as entitled "NO" on Software Upgrade Management UI. The Downloads not managed by PLDS should not be visible on UI.	Software Upgrade Management
SMGR-30354: Duplicate entries of TN board(s) get created in Software Upgrade Management, if Communication Manager record is updated from Inventory management.	Software Upgrade Management
SMGR-30353: TN Board upgrade fails if Communication Manager is in Duplex mode.	Software Upgrade Management
SMGR-30626 : HTTPS option is not supported to download IPO binary still it is visible under Software Management download section	Software Upgrade Management
SMGR-28912: Help link is missing for Software Inventory	Software Upgrade Management
SMGR-29941: Upload of 2.36 GB zip file (IPO App Server and UCM) from user desktop is failing.	Software Upgrade Management
SMGR-31177: Communication Manager sync is failing during the clean-up phase associated with tenants.	Communication Manager Management
SMGR-30082: Extension available list not displaying all the extension ranges if UDP/ARP plan is superset of EXT plan	Communication Manager Management
SMGR-30996: Extension update taking 3 to 4 minutes if extension is already associated or updated with different Emergency Location Extension which is already assigned to multiple extensions.	Communication Manager Management
SMGR-30070: Value of ‘Rg’ subfield for a call-pkup button is not getting updated in template	Communication Manager Management
SMGR-30297: If user creates a template for Communication Manager endpoints and configures a pick up button with ring type single, the template saves that pick up button with ring type to "no-ring"	Communication Manager Management
SMGR-30159: Not able to see available extension, if extensions are starting from “0” like “0xxx”	Communication Manager Management
SMGR-29783: Communication Manager Sync does not collect all off-pbx station mapping entries.	Communication Manager Management
SMGR-30262: Voice mail number disappears if endpoint is updated through global search filter.	Communication Manager Management
SMGR-30359: Not able to configure Detailed (Database) Type of reports in Internet Explorer browser.	Communication Manager Management

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

Note: System Manager 6.3.13 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 and 6.3.12.

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

Copyright 2015 Avaya Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy

Operational Assistance

Table 4: Known limitations and workarounds in Avaya Aura® System Manager 6.3.13 Release

Problem	Keyword	Workaround
SMGR-26867: In rare scenario, upgrade fails.	Infrastructure	Contact Avaya Support Team
SMGR-28779 : Exclude option is not working in Notification Filter	Fault Management	Un assign and assign Target Profiles
SMGR-28812: backup logs of the previous backup are missing after restore.	Backup	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-28480: Remote backup to solar winds SFTP/SCP server is failing	Backup and Restore	Instead of providing just the filename during backup, provide the absolute path including the file name.
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-29030: Manage option for Communication Manager in Manage Elements page does not display proper error message.	Geo Redundancy	No workaround
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	Geo Redundancy	Restart JBoss service on Secondary System Manager Server.

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

minutes and navigates to the requested page.		
SMGR-31295: Scheduler pages take a very long time to load when there are over 20K jobs in the database.	Scheduler	Contact Avaya Support Team for database clean-up.
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-31252: Unable to delete user if user is associated with user preferences.	User Management	Remove the user preferences from the user and then delete user.
SMGR-31186: New User does not appear in user list after successful creation if created by user having custom role associated with Group.	User Management	Log out and log in to Web console again.
SMGR-28439: While adding new user(s), the default language preference is set to random language preference value.	User Management	No workaround.
SMGR-30785: User having custom role not able to add group to new user and unable to remove group from existing user.	User Management	Add and remove of group to user can be done using user associated with System Admin role.
SMGR-28840: If Tenant and sites are unchecked then all the users associated with the tenant are visible.	User Management	No workaround.
SMGR-31363: The links under More Actions on User Management page shows enabled even when user associated with custom role do not have enough permissions and thus when the link is clicked an error is displayed saying that user do not have enough permissions.	User Management	No workaround.
SMGR-31185: Query based Group of type "users" causes issues with accessing the “Add to Group” page from User Management	Group Management	Delete Query based Group of type "users".
SMGR-26743: Filter option is not available for User Provision Rules.	User Provisioning Rule	No workaround.
SMGR-30925: User provision rule mandatory values are reset to default value as “select” if Session Manager or Communication Manager Name is updated, which further results issue in Directory Synchronization.	User Provisioning Rule	Update the User provision rule with updated Session Manager and Communication Manager Name and execute Directory Synchronization job.
SMGR-29039: Inventory jobs shows as Running on Web console but in database, jobs shows as completed	Discovery	Contact Avaya Support Team
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-29517: Unable to upgrade gateway if Communication Manager is lower version	Software Upgrade Management	Contact Avaya Support Team
SMGR-28984: “Pre-upgrade check” button is enabled for all elements in Software Inventory Page. This button should be only enabled for supported elements (Communication Manger and System Platform) but this button is enabled for all the elements.	Software Upgrade Management	No workaround.
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.

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

SMGR-30808: User cannot delete already defined report record from web console.	Communication Manager Management	No workaround.
SMGR-31266: Connection to Communication Manager is not getting closed after generating a list report	Communication Manager Management	No workaround.
SMGR-31008: Multiple entries of Duplex Communication manager are added in Manage Element during inventory discovery.	Inventory Management	No workaround.
SMGR-31305: Help book is showing "Access to the requested resource has been denied" in French Localization OS.	Localization	Contact Avaya Support Team to get the patch.
SMGR-31304: Help Tab content showing in both French and English combination.	Localization	Contact Avaya Support Team to get the patch.
SMGR-31360: Using System Manager Web Console in French locale “Edit Endpoint Editor” from User Communication Profile (User Management) does not works.	Localization	Select Template and perform Edit Endpoint Editor” from User Communication Profile (User Management).

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

System Manager Release 6.3.13 downloads

#	Action	Notes
1.	Download and install the System Platform 6.3.0.0.18002 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 file matches the md5sum on the Avaya PLDS Web site. File Name: vsp-6.3.0.0.18002.iso PLDS download ID: SMGR6320002 Size: 1373 MB Md5Sum: e78359b9fb5f4ad3ce81b299130b69d0
2	Download and install the System Platform 6.3.6.01005.0 RPM 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 rpm matches the md5sum on the Avaya PLDS Web site. File Name: vsp-patch-6.3.6.01005.0.noarch.rpm PLDS download ID: SMGR6313003 Size: 519 MB Md5Sum: d07dfeeca8bd661ae7d07c959f12a561
2	Download System Manager 6.3.13 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_6.3.13_r5003336.bin PLDS download ID: SMGR6313001 Size: 1614 MB. Md5Sum: a8db223140b403c5d8a4e7206fd2dd39

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 6.3.6.01005.0.**
- **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.**

Copyright 2015 Avaya Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy

- **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 6.3.13, 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

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

Installing the Service Pack

Before you begin:

System Manager 6.3.13 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 and 6.3.12.

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 6.3.13 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 6.3.13 software. Do not use data migration utility on System Manager Release 6.3.13.

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

- 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 6.3.13 DVD details:
  - Avaya Aura® System Manager 6.3.13 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 6.3.13 - Software Update Revision No: 6.3.13.10.3336)

  Note –
  - 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.

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

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_R6.3.13_5003336** must be **Not Installed.**
    d. Click on a patch ID **System_Manager_R6.3.13_5003336** 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_R6.3.13_5003336**, is **Pending.**

    If the status is:

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

Copyright 2015 Avaya Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy

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 6.3.13

    Build No. - 6.3.0.8.5682-6.3.8.5108

    Software Update Revision No: 6.3.13.10.3336

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_R6.3.13_5003336** must be **Pending**.
      4. Click the patch ID **System_Manager_R6.3.13_5003336** 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 6.3.13, **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. (a8db223140b403c5d8a4e7206fd2dd39).
5. Run the patch installer using the following command:

   # SMGRPatchdeploy <absolute path to the **System_Manager_6.3.13_r5003336.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.

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

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

  System Manager 6.3.13

  Build No. - 6.3.0.8.5682-6.3.8.5108

  Software Update Revision No: 6.3.13.10.3336

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 6.3.13, **reboot** the System Manager from System Manager CLI to get the updated kernel running in memory.

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

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 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

Copyright 2015 Avaya Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy

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

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy

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

Copyright 2015 Avaya Inc. All rights reserved.

Use pursuant to the terms of your signed agreement or Avaya policy