Avaya Aura® 6.2 Feature Pack 2

System Manager 6.3.2 Release Notes

Release 6.3.2

Issue: 1.2
May 2013

Last Modified Date: April 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE

http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

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

Third-party components

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

http://support.avaya.com/ThirdPartyLicense/

Preventing toll fraud

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

Avaya fraud intervention

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

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Downloading documents

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

Avaya support

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

Table of Contents

Introduction

This Release Notes document provides information about new features, installation downloads, and the supported documentation of Avaya Aura® System Manager 6.3.2 on System Platform and VMware. This document also contains information about known issues and the possible workarounds.

This document provides information about System Manager 6.3.2 release deliverables,System Manager 6.3.2 GA bin file and System Manager 6.3.0 VE OVA.

Note: For information about installing and upgrading to System Manager 6.3.2 both on System Platform and VMware, contact Avaya Technical Support.

Avaya delivers System Manager 6.3.2 in the form of a bin file. You must apply the System Manager 6.3.2 bin file on the System Manager 6.3.0 release.

Product Support Notices

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

To read a PSN online:

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

Enhancements to Avaya Aura® System Manager Release 6.3.2

Table 1: Enhancements delivered to System Manager 6.3.2 GA

Enhancement	Keywords
Support for recovery when secondary System Manager server is active – This enables System Manager services to be available when recovering back to the primary System Manager server.	Geographic Redundancy
Support for displaying geographic redundancy notification failure on the Manage Element user interface and resend the failed notification while restoring data with active secondary System Manager server.	Geographic Redundancy
Enhanced granularity in role-based access control – Customer can now define specific actions /permissions over individual resource attributes. For example, for endpoints, access can be provided for a particular range of extensions along with defining the operation permissions such as Add, Edit, Test, etc.	Role
Support for generating test alarms through System Manager Web console.	Alarm
Supported browsers are Internet Explorer 8, 9, 10, and Firefox 15, 16 and 17.	Browser Support
Support for the SFTP protocol for the System Manager backup and restore.	System Manager Backup/restore
Moved Inventory menu with all sub-menus from Elements section to Services section on the System Manager dashboard.	System Manager dashboard
• Support for Communication Manager 6.3 • Support for client-side validations on THE Manage Elements page for Communication Manager for New and Edit operations • Support for encryption of security code values for Stations • Support for New Field on Off-PBX-Telephone Configuration Set Object • Support for Increased IP Network Regions, Locations, Route Patterns, ARS Analysis, AAR Analysis, ARS Digit Conversion, and AAR Digit Conversion • Support for the Location field on Endpoint, Off PBX Telephone Station Mapping, Service Hours Table, and IP Network Region forms • Support for Network Region fields on IP Network Map • Support for New Stub Network Region • Support for the Far-end Network Region field in Signaling Group • Support for the Location parameters field and the Display parameters field on the Locations page • Support for Per Location Dialplan Analysis, ARS Analysis, AAR Analysis, ARS Digit Conversion, and AAR Digit Conversion • Support for increase in Number of Coverage Answer Group Members from 8 to 100 • Support for Endpoint Options on Remove/Add of CM Endpoints/VDNs/Agent Login IDs • Support for Get Special Applications SA9120 Value • Support for Mute in Shared Control Field for 96x0 SIP and H.323 Sets and 16xx H.323 Sets • Support for Client Side RBAC Range Validation for Non-Extension Primary Key field	Communication Manager

• Support for Top level Advance Search for Communication Manager pages • Support for display of error messages when all logins are used • Support to list all the announcement files that are backed up on System Manager • Enhanced granularity in role-based access control (RBAC) support for Communication Manager objects Alias Endpoint, Intra switch CDR, Off PBX Endpoint Mapping, Off PBX Configuration Set, Site Data, Xmobile Configuration, Terminating Extension Group, Automatic Alternate Routing Analysis, Automatic Alternate Routing Digit Conversion, Automatic Route Selection Analysis, Automatic Route Selection Digit Conversion, Automatic Route Selection Toll (ARS Toll), Data Modules, IP Interfaces, IP Network Regions, Node Names, Signaling Groups, System Parameters, Abbreviated Dialing Enhanced, Abbreviated Dialing - Group or System, Authorization Code, Class of Service (COS), Class of Service Group, Dialplan Analysis, Dialplan Parameters, Feature Access Codes, Locations, Uniform Dial Plan. • Support for RBAC for UPM UI and Bulk Import for Station	
Support for updates and upgrades to Communication Manager, IP Office, Media Modules, and TN Boards using Software Management	Software Management
Support for CM Messaging 6.3. Following versions of messaging is supported for 6.3.4: Aura Messaging 6.0, 6.1, 6.2 ; MM 5.x; CMM 5.2, 6.0, 6.2, 6.3	Messaging

Table 2: Enhancements delivered to System Manager 6.3.0 VE OVA

Enhancement	Keywords
Support for the following on VMware: • Using the System Manager 6.3.0 GA release and the geographic redundancy features • Using licensing feature in the geographic redundancy setup • Configuring multiple DNSs, NTPs, and time zones for System Manager • Configuring VFQDN and the Backup definition rule for System Manager Support for customized validations of System Manager input parameters on vCenter	System Manager on VMware

System Manager software

System Manager installation downloads

Download and install System Manager on System Platform

#	Procedure	Notes
1.	Download and install the System Platform **6.3.0.0.18002** ISO image from the Avaya PLDS website.	Verify that the md5sum for the downloaded ISO image matches the number on the Avaya PLDS website. **vsp-6.3.0.0.18002.iso** **PLDS download ID**: SMGR6320002 **Size**: 1373 MB/1406684 KB **Md5Sum**: e78359b9fb5f4ad3ce81b299130b69d0
2.	Download and install System Manager 6.3.0 ISO image from the Avaya PLDS website.	You must install the System Manager 6.3.0 template on System Platform 6.3.0.0.18002. **System_Manager_06_03.iso** **PLDS download ID**: SMGR6310004 **Size**: 3315 MB **Md5Sum**: 24c5c6c1e471896931cc60c513db0e61
3..	Download and install the System Manager 6.3.2 GA bin file from the Avaya PLDS website.	**System_Manager_6.3.2_r1399.bin** **PLDS download ID**: SMGR6320001 **Size**: 732 MB / 748960 KB **Md5Sum**: bcba951a11814be68018abec2cb02815

Note: System Manager 6.3.2 is in the form of bin file.Before installing System Manager 6.3.2, download System Manager 6.3.0 from Product Licensing and Delivery System (PLDS) or purchase System Manager 6.3.0 on DVD from ASD (Order Code 700505971) and install. If the 6.3.0 image is downloaded from PLDS, copy the software to a DVD as an ISO image.You must install System Manager 6.3.0 on System Platform **6.3.0.0.18002** through CDOM Virtual Machine Solution Template before installing System Manager 6.3.2.

Download and install System Manager on VMware

#	Procedure	Notes
1.	Download and install System Manager 6.3.0 VE OVA from the Avaya PLDS website.	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. **SMGR-6.3.0.8.5682-e50-68.ova** **PLDS Download ID**: **SMGR6310008** **Md5sum**: **fcc430969434c930f284fa8e4ea5f2df**

2.	Download and install the System Manager 6.3.2 GA bin file from the Avaya PLDS website.	**System_Manager_6.3.2_r1399.bin** **PLDS download ID**: SMGR6320001 **Size**: 732 MB / 748960 KB **Md5Sum**: bcba951a11814be68018abec2cb02815

Download and execute Data Migration Utility

This is required for upgrade workflow.

1.	Download and execute System Manager Data Migration Utility.	**Data_Migration_Utility_6.3.2_r86.bin** **PLDS Download ID**: SMGR6320003 **Size**: 1 MB / 98 KB **Md5sum**: d458cf08c13d4449dff3a54d836c5cd1

Must read

1. **Upgrade sequence**

System Manager on System Platform

You must follow following sequence for upgrading System Manager Software on System Platform: (1) upgrade System Platform (2) upgrade System Manager and (3) upgrade Elements. For additional information on the installation, follow instructions from the Installation note - *Implementing Avaya Aura® System Manager 6.3.2.*

System Manager on VMware

You must follow sequence for upgrading System Manager Software on VMware from the Installation note - *Deployment Guide for Virtualized Environment.*

2. **Patch installation**

System Manager on System Platform

- Before applying the System Platform patch, ensure that the */tmp/patch* folder does not exist on CDOM.
- If IPtables are turned off on the System Manager, then patch installation does not continue.
- The administrator must not override or change the existing IPtable configurations.

System Manager on VMware

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

3. **Resource reservations for System Manager on VMware**

System Manager on VMware

VMware Resource	Value
vCPUs	4
CPU reservation	4
Memory	9 GB
Memory reservation	9 GB
Storage reservation	30GB – System Manager 30GB – Session Manager performance data 10GB – CS1000 application 2GB – AUS-collaboration framework TOTAL – 72 GB
Shared NIC(s)	1

All the below points are applicable to System Manager on System Platform and VMware

4. **Verify the System Manager Release version**

After installing System Manager 6.3.2, verify the release of the installed System Manager by clicking **About** in the top-right corner of the Home page. You can also run the **swversion** command through the CLI.

5. **Use FQDN to gain access to System Manager**

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

6. **System Manager Hostname**

System Manager complies to RFC952 for hostnames.

7. **Log in to System Manager**

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

8. **Understand the password policy and aging for admin user account**

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

9. Third party certificate in case of upgrade

Third party certificate is required to be regenerated and re-imported in case of upgrade from System Manager prior releases to System Manager 6.3.0 release. This is required only in case System Manager is using third party Identity certificates prior to upgrade.
For System Manager-Session Manager replication, it is required for System Manager Identity certificate to have the VFQDN of System Manager to be present in the Subject Alternative Name. Upgrading System Manager to 6.3.0 retains the Identity Certificate being used prior to upgrade; this certificate will not have the VFQDN present as the Subject Alternative Name. Due to this when Session Managers in the environment are upgraded to 6.3.0 release, replication to Session Managers stop.

10. Reboot System Manager for updated kernel

After you upgrade the system to 6.3.2, reboot System Manager from System Platform or from System Manager CLI to get the updated kernel running in memory.

11. IP/FQDN entry of Session Manager elements in DNS server

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

12. Schedule Jobs

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

13. External authentication configuration

If you upgrade directly to System Manager 6.3.0 GA from System Manager 6.0 or earlier release and if you configured the earlier release for an external authentication, such as LDAP and RADIUS, you must reconfigure the details of the external authentication server on System Manager 6.3.2 after the system completes the upgrade. This does not apply to upgrades from System Manager 6.1 or 6.2.
To reconfigure System Manager external authentication, see *External authentication configuration*.

14. Login warning banner upgrade

If you want to upgrade directly to System Manager 6.3.0 from System Manager 6.0 or earlier release and if you have complied with the configuration for the legal notice, you must reconfigure the login warning banner content on System Manager 6.3.2 after the system completes the upgrade.
This does not apply to upgrades from System Manager 6.1 or 6.2.

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

15. Internet Explorer compatibility

Some of the System Manager features might not work in Internet Explorer 8 and later versions if the compatibility and document mode is switched on.
To switch off the compatibility mode, see *Internet Explorer compatibility*.

16. Browser Cache

You must clear your browser cache before gaining access to the System Manager console the first time after installation or upgrade. If you do not clear the browser cache, style sheets might not load.

17. Restore data notification clearance

You must logout and re-login to clear old notifications after you have restored the data using the primary System Manager server.

18. Presence Communication Profile

The Presence services communications profile is added to accommodate new features in future releases. Do not enable this communication profile in System Manager release 6.3.2.

19. Shell account

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

20. Remote System Manager Backup

Before you select the use default checkbox, you must first set the remote parameters: Remote Server Password, Remote Server Port, Remote server, and Remote Server User in the *Home/Services/Configurations/ Settings/SMGR/SMGR Element Manager* page.

21. Software Management

System Manager should be able to access *ftp.avaya.com* and *pldsxml.avaya.com* for accessing Avaya support in order to download firmware and for analyze functionality to work properly.

22. CS1000 in System Manager geographic redundancy setup

To learn about CS1000 applications supported in System Manager geographic redundancy setup, see *CS1000 in System Manager geographic redundancy setup*.

23. CS1000 and System Manager interoperability support

CS1000-SMGR Interoperability Support is not available in System Manager 6.3.2. System Manager 6.3.0 supports CS1000 7.5.

Prerequisites for a new installation of System Manager

System Manager on System Platform

1. Create a backup of the system and store the backup on an external device.
2. Install System Platform **6.3.0.0.18002.**
3. Check the RAID Controller Battery state.
    a. Login to System Platform CDOM Web console using admin credentials
    b. Navigate to *Server Management/Log Viewer*
    c. Select System Logs, Critical/Fatal as the log level
    d. Type O_AVDM in the **Find** text box and click **Search**
    e. In the **Message Content** column of the result table, search for the **O_AVDM10101** or **O_AVDM10102** or **O_AVDM10100**.
    f. If this alarm is present, the raid battery of the system needs replacement.
4. Install System Manager Release 6.3.0.
5. Upgrade System Platform before you upgrade System Manager, in case of an upgrade.

System Manager on VMware

1. Create a backup of the system and store the backup on an external device.
2. Install the **ESXi 5.**1 server.
3. Install **vSphere Client 5.1**, and ensure that vSphere Client is connected to the server.
4. Install System Manager 6.3.0 VE OVA.

Hardware Requirements

- S8800 1U Server System Manager IBM x3550m2and material code 700478589
- R610 Server 2CPU MID2 Dell and material code 700501083
- DL360G7 Server 2CPU MID4 HP and material code 700501093

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

Software information

Software	Version	Note
Postgres	9.1.3	Used as a System Manager database. For more information, see: http://www.postgresql.org/docs/9.1/static/index.html.
CentOS	5.6 64 bit	Used as the Operating System for the System Manager template
JDK	Version 6 Update 33 64-bit	
JBoss	6.1	
Internet Explorer	8.x, 9.x, and 10.x	
Firefox	15.x, 16.x, and 17.x	

VMware vCenter Server, vSphere Client, ESXi Host	5.0, 5.1	

Installation note

Contact Avaya Support Website for the following:

- System Manager installation and configuration information for *Implementing Avaya Aura® System Manager 6.3.2*
- System Manager upgrade information for *Upgrading Avaya Aura® System Manager to 6.3.2*
- System Manager on VMware installation, configuration and upgrade information for *Deployment Guide for Virtualized Environment*
- System Manager upgrades information using Data Migration on System Platform for *Migrating System Manager Data using Data Migration utility*.
- Installation and upgrades, product support, and service pack for earlier releases of System Manager 6.3.2.

Upgrade information

System Manager on VMware
For upgrading System Manager on VMware, refer to the *Deployment Guide for Virtualized Environment*.

System Manager on System Platform
For upgrading System Manager on System Platform, refer to the *Upgrading Avaya Aura® System Manager to 6.3.2* and *Migrating System Manager Data using Data Migration utility*

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

#

Operational assistance

Table 3: Known issues and workarounds in System Manager 6.3.2

All the below issues are applicable for System Manager on System Platform and VMware

Problem	Keywords	Workaround
You may observe "Caused by: javax.jms.JMSException: Failed to create session". This is an issue with Hornet 2.2.5 final resource adaptor. And has been fixed in later versions of hornetQ.	System Manager	Step1: Stop JBoss service Step2: Execute rm –rf $JBOSS_HOME/server/avmgmt/data/hornetq Step2:Start JBoss service
CS1000-SMGR Interoperability Support is not available in System Manager 6.3.2.	CS1000	No workaround available
[wi01025130] Cannot harvest CS1K logs.	CS1000	Capture logs manually from /var/log/Nortel.
[wi01061587] Whenever any Communication Manager permission is given, the Configuration link is enabled by default.	Communication Manager	Give all operation mapping and spmoperation mapping

[wi01066033] When a System Manager 6.3.2 bin file is rolled back from the System Platform console, the data replication Nodes for 6.2 SM/BSM get synchronization failure message when System Manager is restored to the old state.	Data replication	Step1: Execute script on Primary server with the Secondary server IP Address. $MGMT_HOME/remoteSnmpConfig/utility/recoverAgent.sh
[wi01075489] Labels for the Graceful shutdown feature are not uniform across all System Manager pages.	Graceful shutdown	No workaround available
[wi01077258] Context specific help description for security assertion markup language (SAML) in Help pages.	Help	No workaround available
[wi01078301]PostgreSQL 2013-02-07 Security Update Release	Security Update	No workaround available
[wi01076536] Sorting does not work for Element type in the Administrator link.	User Interface	No workaround available
[wi01076560] The Search option does not work as expected for Release information in the Administrator link.	User Interface	No workaround available
[wi01076954] Auto refresh for Notification does not work.	User Interface	Log out System Manager and re-login
[wi01076965] In rare scenario, time-out is required for Geo Enable work flow.	Geographic Redundancy	Step1: Execute script on Primary server $MGMT_HOME/geo/bin/update_geoenabledisablestatus_table.sh disable Step2: Restart JBoss
[wi01078148] The ldap directory CND does not stop even when the system goes into the Auto disable mode.	Geographic Redundancy	No workaround available
[wi01079558] Secondary System Manager shows primary is connected, even if primary is a standalone server.	Geographic Redundancy	No workaround available
[wi01081909] If a user does not access the primary System Manager server UI when configuration was in progress, the configuration status does not refresh.	Primary Server GR user interface	Restart JBoss on Primary server
[wi01082589] A Misleading error message is displayed on trying to perform Remote restore of the secondary backup on the primary server.	Backup	No workaround available
[wi01082983] An Incorrect error message is displayed on entering the wrong filename for remote restore using the default option.	Restore	No workaround available
[wi01082994] Continue Button focus is present even if you enter the wrong filename for Remote restore.	Restore	No workaround available
[wi01083543] The File path of the restored file does not display for Remote Restore.	Restore	No workaround available
[wi01083268] The Status bar on the Inventory page gets stuck to 0 or 100% and sometimes does not appear.	Inventory	Refresh the page

[Wi01032730] Import fails when trying to change mailbox number using merge or replace import job.	Messaging	No workaround other than to make the change on the messaging system.
[Wi01082750] Bulk import fails when length of givenName and sn is greater than 27 characters.	Messaging	No workaround other than to check lengths of names or make changes on messaging system.
[Wi01083659] In User profile management page, unselecting the Use Existing Subscriber checkbox does not clear existing mailboxes.	Messaging	No workaround available
[Wi01083712] During directory synchronization, subscriber associated with user is not disassociated after the sub deleted on the messaging system.	Messaging	No workaround available
[wi01090124] Some of lower version images are getting excluded in recommendation for Media Gateway downgrade/upgrade	Software Management	No workaround available
[wi01091307] After applying filter once in Software Management page, if filter criteria is changed and again applied then filter criteria automatically get cleared. Get Inventory and Analyze operation cannot be scheduled after this.	Software Management	Close Software Management tab and open a new tab OR log off and login again.
[wi01091642] Gateway upgrade using LSP as file server through FTP protocol does not work	Software Management	Download a file to LSP server using SCP protocol and then upgrade gateway using FTP protocol.
[wi01091690] While performing SAMP firmware update by default first option is selected i.e. Install and Activate. But performing Install and Activate operation for SAMP firmware fails.	Software Management	Select option Install (Copy and Unpack) / Update SAMP, MPC
[wi01092753] If only one gateway firmware file is present in software library then gateway upgrade job does not get scheduled.	Software Management	Download two or more gateway firmware files into software library
[wi01095473] When Software Library is clicked, an error stating Some internal error has occurred is shown on the page. This is seen in the System Manager upgrade path from 6.1 SP4 -> 6.2 FP1 -> 6.2 FP2	Software Management	No workaround available
[wi01093373] After applying some filter **Select All** selects rows outside the filter criteria.	User Interface	No workaround available
[wi01087595] 1.While duplicating 'agent default template' if we change value of COR (Valid values are 0-995) then template is not created successfully. 2.Password and Confirm Password is not validated while duplicating default template.	Template	No workaround available
[wi01091498] Agent cannot be assigned to User if skill number is changed from its default value	User Management	After error shown on UI, click on "Agent Editor" button. Now click "Done" and then click "Commit" button.
[wi01092084] User created on the **Administrators** page does not have	Alarm	Create user from System Manager User Management screen and assign proper

permissions on alarming user interface so for this user alarms will not be visible on Alarms page. e-Token user is not able to view the alarms on **Events/Alarms** page.		permissions required for accessing Alarming UI.

Appendix

Log in to System Manager

System Manager CLI:

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

System Manager Web console:

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

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

External authentication configuration

To reconfigure System Manager external authentication:

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

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

Login warning banner upgrade

To reconfigure the login warning banner:

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

Internet Explorer compatibility

To switch off the compatibility mode:

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

To switch off the document mode:

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

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

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

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

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

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

Shell account

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

Instead two aliases are introduced:

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

These restrictions apply for the admin user only.

CS1000 in System Manager geographic redundancy setup

Primary state	Secondary state	CS1000 applications available from primary server	CS1000 applications available from secondary server

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

Technical support

Avaya Technical Support provides support for System Manager 6.3.2.

For any problems with System Manager 6.3.2, you can:

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

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

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

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

You might be asked to send by email one or more files to Avaya Technical Support Team for analysis of your application and the environment.
For information about patches and product updates, see the Avaya Support website at http://support.avaya.com.