



Avaya Aura® System Manager 7.0 Release Notes

**Release 7.0
Issue: 2
October 2016**

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 AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

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

License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

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

Third-party components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

<http://www.avaya.com/support>.

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

Trademarks

Avaya, the Avaya logo, Avaya Aura® System Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading documents

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

<http://www.avaya.com/support>

Contact Avaya Support

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

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

Table of Contents

Avaya Aura® System Manager 7.0 Release Notes	1
What's new	1
Enhancements delivered to System Manager 7.0	2
Fixes for customer found defects delivered to System Manager 7.0	8
Deploying System Manager 7.0.....	9
Important.....	9
Prerequisites for a new installation of System Manager.....	15
Prerequisites for upgrade of System Manager	15
Appliance Virtualization Platform (AVP) Servers available to run System Manager 7.0	15
Software information	17
Installation and Upgrade note	17
Download System Manager 7.0.....	18
Information about SDM supported Avaya Aura® Products and their Release Notes.....	18
Information on Versions.xml	18
Known issues and workarounds.....	19
Appendix.....	20
Technical support.....	21

What's new

This Release Notes document provides information about new features, installation downloads, and the documentation of Avaya Aura® System Manager 7.0 on VMware. This document also contains information about known issues and the possible workarounds.

System Manager 7.0 deliverables include System Manager 7.0 VE OVA, 7.0 Data Migration Utility, and 7.0 Solution Deployment Manager (SDM) Client.

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 admin 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.

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

To read a PSN online:

1. Navigate to the Avaya Support website at <http://support.avaya.com>.
2. On the main menu, click **Support By Product**.
3. Click **Documents**.
4. In **Enter Your Product Here**, enter **Avaya Aura® System Manager**.
5. In **Choose Release**, click **7.0.x**.
6. In the Content Type pane, select **Product Support Notices**.
7. Click **Enter**.
8. To open a specific PSN, click the PSN title link.

Enhancements delivered to System Manager 7.0

Enhancement	Keywords
- Updated the System Manager base operating system to CentOS 6.5. - Replaced the System Manager Java SE platform from Oracle JRE to OpenJDK 1.7 Update 79. - Updated the PostgreSQL database of System Manager to 9.3.4. - Added support for Browsers - Internet Explorer versions 9.x, 10.x and 11.x and Firefox versions 36, 37, 38 - Improved System Manager Navigation and Usability UI: The System Manager User Profile Manager used for User Management has been enhanced to only display specific administration fields. For example, administration fields those are applicable to administrator activities for applications that are part of what that customer solution supports. This change removes unnecessary fields and speeds up and simplifies management tasks. - Added support for validation to prevent input greater than 50 characters for System Manager FQDN & VFQDN during deployment. - Password aging has been enabled for the OS user accounts. User passwords must be changed at least every 60 days.	Infrastructure and Serviceability Updates
Added support for installing System Manager 7.0 OVA on the Appliance Virtualization Platform (AVP) that is being introduced in Avaya Aura® 7.0 as part of the Avaya--provided appliance.	Avaya Appliance
Enhanced System Manager 7.0 to increase the scale of SIP users and devices: - Increased scale to support 250K SIP users from 125K users in 6.3.x releases. - Increased scale to support 350K SIP endpoint devices from 150K devices in 6.3.x releases. - Increased scale to support 28 Session Managers from 12 Session Managers in 6.3.x releases.	Capacity Increases
Enhanced System Manager 7.0 security as follows: - System Manager has updated its disk partitioning. - Support for processes to run as a Less Privileged User. - In System Manager 6.3.8, a CLI-based Certificate Authority (CA) Generation Utility was developed for SHA2 and RSA 2048 certificate support for customers wanting to update their CA Certificate from SHA1 and RSA 1024.	Security Improvements

Enhancement	Keywords
In System Manager fresh 7.0 deployments, the CA certificate is SHA2 and RSA 2048 by default. A customer upgrading to System Manager 7.0 can run the CA Generation Utility for updating CA certificate to SHA2 and RSA 2048. The integrated utility guides the administrator through the process of updating the certificates. If the administrator chooses to generate a new CA (SHA2), then the trust with the older Elements will be broken and must be re-established with the new CA. Refer chapter Managing Certificates from <i>Administering Avaya Aura® System Manager for Release 7.0</i> and other Element's Administrative Guides for re-establishing trust. • The System Manager Certificate Management console removes obsolete certificates that display on the Certificate Management console. • The SSH admin login password does not remain at the default value after the initial configuration.	
Solution Deployment Manager (SDM) provides a centralized software management solution in System Manager that can support deployments, migrations, upgrades, and updates to the suite of Avaya Aura® 7.0 applications. Capabilities and functional scope of SDM ▪ Physical location, virtual machine, and ESXi Host for application deployment are defined. ▪ Application configuration and IP networking parameters for application deployment are required. ▪ SDM can deploy Avaya Aura® 7.0 Application OVAs to both customer-provided VE and Avaya-provided Appliance environments: ○ Session Manager (SM) ○ Branch Session Manager (BSM) ○ System Manager ○ Application Enablement Service (AES) ○ Utility Services (US) ○ Communication Manager (CM) ○ CM Messaging (CMM) ○ Engagement Development Platform (EDP) ○ Avaya Media Server (AMS) ○ WebLM ○ ADS/SAL ○ Avaya Aura® Messaging (AAM) ▪ System Manager SDM will support Migration for the following products: ○ Communication Manager 5.2.1 to 7.0 Appliance Offer. [CM,CMM] ○ Session Manager 6.x (non-VE) to 7.0 Appliance Offer, but not previous releases of Session Manager. ○ System Platform-based Applications to a virtualized environment (VE) and on the Avaya Appliance Communication Manager (from 6.x templates): ▪ Duplex CM Main / Survivable Core [CM] ▪ Simplex CM Main / Survivable Core [CM, CMM, US] ▪ Simplex Survivable Remote [CM, BSM, US] ▪ Embedded CM Main [CM, CMM, US] ▪ Embedded Survivable Remote [CM, BSM, US]	Solution Deployment Manager (SDM) – Centralized System Manager- SDM

Enhancement	Keywords
▪ Simplex Survivable Remote [CM, BSM, US] ▪ Embedded Survivable Remote [CM, BSM, US] ▪ As part of the Apply upgrade (migration) feature, the centralized System Manager (with SDM) will also provide the following functions: ○ Support auto-selection of System platform and any associated upgradable elements after System Platform is selected for Upgrade. ○ Support On-Demand/Scheduled Pre-Upgrade check/Refresh/Analyze. Pre-Upgrade check also runs as part of the upgrade workflow. ○ Support ability to view the status of the previously run Pre-upgrade check /Refresh/Analyze and other operations. ○ Support the ability to re-run a previously run pre-upgrade check from the status page. ○ Display the EULA to the administrator as part of the Upgrade Configuration. ▪ Apply updates: 7.0 Service Packs, Feature Packs and Patches to Avaya Aura® Applications ○ Communication Manager and Adjuncts ○ Session Manager ○ Branch Session Manager ○ Utility Server ○ Appliance Virtualization Platform (AVP) – ESXi Host running on Avaya Provided Appliance ▪ As part of Apply update feature, the centralized System Manager (with SDM) will also provide the following functions: ○ Pre-update check ○ Support for On-Demand/Scheduled Refresh and Analyze. ○ Support the ability to view the status of the previously run Refresh/ Analyze/ update and other operations. ▪ Analyze customer application entitlements (analyze what releases are deployed versus what customers are entitled to; make recommendations) ▪ Define Software Library (local on System Manager or an external server) ▪ Interface with Product Licensing and Delivery System (PLDS) for OVA and Update downloads ▪ Virtual machine Lifecycle Management which includes the ability to start, stop, delete, restart and refresh all or selected VMs ▪ Flexible Footprint Definition (define virtual resources needed based on capacity). ▪ Ability change Hypervisor IP Address on the Appliance Virtualization Platform (AVP). ▪ Ability to support Hypervisor Patching on the Appliance Virtualization Platform (AVP). ▪ Re-establish key-based Trust using username and password for VMs through System Manager Web console. ▪ Deployment support for S8300D/E, ME, CSR1/CSR2 ▪ Migration support for S8300D/E, CSR1/CSR2 ▪ Support for Trust establishment between System Manager and Virtual Machines. Note: Updates of CMs, Gateways, TN Boards and Media Modules will continue to be	

Enhancement	Keywords
supported as previously provided in System Manager 6.3.8. Note: In case the CM 5.2.1 is duplex CM, it would be the administrator's responsibility to add the other server of the duplex pair in System Manager RTS web console and upgrade it as well. Note: For Upgrade (migration) using SDM : ○ The Pre-upgrade check with flexi-footprint selection helps administrator to catch any issues that might come later during migration. ○ The memory check is made mandatory. Also admin can select footprint and verify during pre-upgrade for which footprint pre-upgrade check is passing/failing. Administrator must make sure that he is selecting the footprint for which pre-upgrade has passed and which is according to prescribed guidelines. ○ The SIP entity name must not contain any special characters. However if someone proceeds with this mistake the migration will Pause, the entity name can then be rectified and migration can be resumed. For different box migration, there is no need to go to lab for switching on the already stopped server. ○ CM/US/SM/BSM data will get pre-populated. During Edit Configuration provide the administrative user and password for the element you are upgrading, click on the Pre-populate Data button, that'll pre-populate most of the fields. However make sure that if some fields are showing null and data is expected there, fill it manually. See if the time zone is proper. Note: While adding/refreshing AVP host, ensure trust is established and Refresh VM has been executed for all VMs.	
For the initial System Manager deployment or where System Manager is not accessible (such as certain remote locations), there will be a version of the Solution Deployment Manager called the SDM-Client that can reside on a technician's laptop. The SDM-Client will provide the necessary functionality to install the OVAs on either an Avaya Provided Appliance or Customer Provided VE. The SDM -Client will use the same API back-end and User Interface as the centralized System Manager-SDM providing for the same look-and-feel as the centralized System Manager-SDM version. Note that the SDM-Client is not intended to be the main solution, but rather cover special cases where a centralized SDM on System Manager is not available. Capabilities and Functional Scope of the SDM-Client • Runs on Technician PC ○ Windows 7 (Professional / Enterprise) 64bit ○ Windows 8.1 (Professional / Enterprise) 64bit • Supported Web Browsers as System Manager 7.0. • Runs on Tomcat Server • Provides Common UI Look and Feel as Central SDM in System Manager 7.0. • Supports Flexible Footprint Feature (size virtual resources based on capacity requirements for the Aura applications). • Define Physical Location, Virtual Machine and ESXi Host for application deployment.	SDM Client

Enhancement	Keywords
- Define initial application networking configuration as part of the OVA deployment process. - Ability to deploy the same Avaya Aura® applications that can be deployed from the centralized System Manager-SDM (one application at a time can be deployed). Available for Avaya Provided Appliance and Customer VE. - Support for System Manager Upgrade to 7.0 from System Platform based System Manager and update 7.0 patches. - Local computer (Technician PC) for selecting application OVA file to deploy. No PLDS interoperability that is available in the centralized System Manager-SDM. - Ability to change Hypervisor IP Address on the Appliance Virtualization Platform (AVP). - Ability to support Hypervisor Patching on the Appliance Virtualization Platform (AVP). - Lifecycle Management of the OVA Applications deployed to a VM. Includes the ability to start, stop, and reset all or selected VMs. Note: Ensure that firewall allows 443 and 1527 ports that are required for the SDM client installation and SDM functionality. Note: It is recommended that single VM deployment is done at a time using SDM client. Note: Recommendation is Utility Services (US) should be the first OVA installation during fresh installation and then other application OVA should be deployed. This is with the assumption that there is System Manager server in the network. In case, there is no System Manager installed in the network, deploy US OVA with planned System Manager IP address and Enrollment password. In case, there is no plans of installing System Manager, provide dummy values for System Manager IP address (example 194.66.82.11) and Enrollment password (example passwd) and proceed ahead with the installation. Once actual System Manager is installed, then perform trust re-establishment later for that US with System Manager so that earlier provided dummy value will get overridden. Note: While adding/refreshing AVP host, ensure trust is established and Refresh VM has been executed for all VMs.	
Support for updating the Appliance Virtualization Platform (AVP) running on an Avaya Provided Appliance from SDM. Note: This does not apply to patching Customer-provided VE, so the patching capability shall be blocked for those solutions. Note: Not applicable for Appliance Virtualization Platform (AVP) that System Manager is running on. SDM-Client is used to patch AVP when hosting System Manager.	Appliance Virtualization Platform (AVP) Patching
The swversion CLI utility will print the System Manager version in a more easy to understand format.	Software Version
System Manager 7.0 introduces the ability to synchronize Active Directory Groups as defined in a customer's LDAP Directory to System Manager Administrator roles. This new capability includes both pre-defined system roles as well as custom roles on System Manager. The User Interface for provisioning Admin Group – System Manager Role synchronization will be available as an extension to synchronization interface used to define LDAP User Syncs where you map LDAP fields to System Manager User fields.	LDAP Sync of Roles
Each release Communication Manager and Session Manager introduce new features and functionality that generate corresponding concurrency development in the management	CM Concurrency

Enhancement	Keywords
applications. The following is a list of CM enhancements that had concurrency development in System Manager 7.0: • Triple Ring Pattern for Call Pickup Button (new ring pattern option) • Support for the Avaya Media Server and associated announcements • Service Observing from SIP Phone Support (new endpoint button) • Support ability to configure the listen-only sub-field to the Service Observe (sip-sobsv) button assignment. • Support ability to add a Service Observing Coaching (so-coach) button to any non-SIP Phones through the CM Element Manager • VOA Repeat / Interrupt for SIP CC Phone Support (new endpoint button) • Add / Remove Agent Skill from SIP Phone Support (new endpoint button) • SO-Coaching (non- SIP) Support (new endpoint button) • SIP Station Reachability (field on the SIP Endpoint object) • Block 96x1SIPCC Set Type when Maximum Simultaneous Device Greater than one. • Auto Qualifier for Bulk Edit Agents • Suggest Route Pattern for SIP endpoint • System Manager to support storing the Encrypt SRTCP parameter in the database as part of the IP Codec Set tables • Support ability to automatically generate an OPS entry for an H.323 set type configured for Dual Registration • Support ability to administer the Attribute field on the Agent Login ID object. • Communication Manager Synchronization Optimization/Hardening implying implementation of a defense/hardening mechanism in the CM Sync process to prevent contention with third-party tools.	
• System Manager continues to expand support for Communication Manager (CM) centric reports through System Manager as part of the Avaya Integrated Management (AIM) transition functionality into System Manager. • System Manager 7.0 builds upon the reporting infrastructure introduced in System Manager 6.3.x, by introducing the ability to gather predefined detailed measurement, performance and status data for Communication Manager attributes. The new performance based reports help with serviceability, maintenance and troubleshooting of Communication Manager. • Approximately 140 pre-defined List and Display CM Performance Measurement and Status Reports were added to System Manager 7.0 • The addition of the List and Display Measurement and Status Reports enable customers using ASA/MSA/FPM Reporting to have the same services and capabilities available after migrating to System Manager.	Communication Manager (CM) Status and Performance Reports
System Manager 7.0 introduces the ability to separate management and non-management network traffic across two physically and/or logically separated connections which enable customers to keep non-management networking traffic off the management interface. Examples of System Manager Management Network Traffic Include: • Database Replication with Session Manager • An administrator making configurations through System Manager Webconsole. Examples of SMGR Non-Management or Public Network Traffic Include: • Support for End-user self-provisioning • Tenant Management The separation requirement is for non-routable segregation, so logical rather than physical separation options (e.g. VPN) are acceptable.	Out-of-Band Management

Enhancement	Keywords
The CM Agent communication profile association with the user can now also be imported or exported using Excel file. Note: This import and export of CM Agent communication profile association with user was already supported via. XML.	Import-Export using Excel

Fixes for customer found defects delivered to System Manager 7.0

Problem	Keywords
Blank entry in the protected column of table ipt_announcement causes Data Migration failure.	SMGR-32643
License mapping in centralized licensing deployment is retained for only a single product in license file after over-installation of the license file in case of multi-application LAR.	SMGR-32366
Mapping for one of the servers in Communication Manager duplex pair gets removed on license over-install	SMGR-32322
Issue with replacing secondary System Manager default identity certificate with a third party Certificate Authority signed certificate in a geo redundant deployment.	SMGR-32278
Self-provisioning link does not work.	SMGR-31901
User having System Admin or custom role not able remove group from existing user.	SMGR-31458
Handle Presence handle migration properly via data migration	SMGR-31243
Group of type users for Query Based causes issues with accessing the Add to Group page from User Management	SMGR-31185
LSP + ESS switch Add to Communication Manager should be unchecked while discovery	SMGR-31006
Selection of record from Manage Jobs records or loading of Manage Import Jobs screen is very slow	SMGR-30081
Unable to upgrade gateway if Communication Manager is lower version	SMGR-29517
Problem with geographic redundancy enable with huge database after enable replication fails initially	SMGR-28905
Time out required for Geographic Redundancy Enable work flow [GR-Enable:in-progress stuck more than 5 hours]	SMGR-25482

Deploying System Manager 7.0

Important

1. System Manager fresh deployment

System Manager 7.0.0 will be delivered as new OVA that can be deployed on an Avaya-provided appliance or customer-provided Virtualized Environment (VE). The SDM-Client is used to deploy System Manager to the Avaya-provided appliance. The SDM-Client or customer-provided VMware tools such as vCenter or vSphere Client can be used to deploy System Manager to the customer-provided Virtualized Environment (VE).

Utility Services 7.0 OVA must be installed on the Avaya Virtual Platform before deploying System Manager 7.0 OVA.

2. System Manager upgrades

Upgrades from 6.x versions of System Manager on an Avaya Appliance (System Platform Based)/ Virtual environment will be treated as migrations when going to the new AVP Aura 7.0 environment. You first need to must install Appliance Virtualization Platform (AVP) /VMware then the System Manager 7.0.0 OVA. Data migration will support the transferring of data from System Manager 6.x to System Manager 7.0.0.

Note: that the Utility Services 7.0 OVA must be installed on the Avaya Virtual Platform prior to the deployment of the System Manager 7.0 OVA.

Note: Always perform System Manager Backup and use it for data migration.

Upgrades from 5.x versions of System Manager on an Avaya Appliance will be supported as follows:

1. Take of backup of the existing System Manager 5.2 system (This is just for safety in the event that reverting back to the original System Manager 5.2 is needed. This back up will not be used as part of the upgrade.)
2. Export the NRP data.
3. Install AVP 7.0
4. Deploy the Utility Services 7.0 OVA (using SDM-Client)
5. Deploy the System Manager 7.0 release – with the same IP address and hostname as the original System Manager 5.2 box. SDM-Client is used to deploy System Manager.

Once System Manager 7.0 is running import the NRP data

More details for upgrading 5.x, 6.x versions of System Manager Software on Customer Provided Virtualized Environment (VE) to System Manager 7.0 please refer to [Installation and Upgrade note section](#).

3. Patch installation

System Manager on VMware

If iptables are turned off on System Manager, then patch installation does not continue.

The administrator must not override or change the existing IP table configurations.

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

4. Resource reservations for System Manager Avaya Provided Appliance or Customer Provided Virtualized Environment (VE)

For VE Footprint Flexibility, System Manager 7.0 supports the following profiles and large profile.

AVP

Footprint Profile	# vCPU Reserved	Min vCPU Speed (MHz)	vRAM	Virtual Hard Disk	CSR1 Support	CSR2 Support
Profile-1 (35K users with 35 BSM's and 12 SM's)	4	2290 MHz	9GB	105GB	Yes	Yes
Profile-2 (35K-250K users with up to 250 BSM's and 12 SM's)	6	2290 MHz	12GB	105GB	No (will not fit)	Yes
Profile-3 SMGR High Capacity (35K-250K users with up to 500 BSM's and 28 SM's)	8	2290 MHz	18GB	250GB	No (will not fit)	Yes

Customer VE

Footprint Profile	# vCPU Reserved	Min. vCPU Speed (MHz)	Virtual RAM	Virtual Hard Disk	CPU Reservation	Memory Reservation MB
Profile-1 (35K users with 35 BSMs and 12SM)	4	2290 MHz	9GB	105GB	9160	9126
Profile-2 (35K-250K users with up to 250 BSM's and 12SM's)	6	2290 MHz	12GB	105GB	13740	12288
Profile-3 SMGR High Capacity (35K-250K users with up to 500 BSM's and 28SM's)	8	2290 MHz	18GB	250GB	18320	18432

Large profile is supported as separate OVA. Details as below

5. Geographic Redundancy

For fresh deployment, reset the SSH **admin** user password for both primary and secondary System Manager before configuring geographic redundancy.

Ensure to use the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 1, the secondary System Manager must also contain Profile 1.

For more information, see Geographic Redundancy configuration in **Administrator Guide documentation**.

6. Export Users

If the admin wants to use the exported excel file for further use like importing again then, while exporting users from the Export Users webpage, clear the **Contacts** checkbox in **User Attribute Options** because Excel

export or import does not support contacts that are associated with the user to be exported or imported.

7. VE Snapshot

A snapshot preserves the state and data of a virtual machine at a specific point in time. For taking a snapshot it is mandated, uncheck the checkbox **Snapshot the virtual machine's memory** on ESXi.

Snapshots can:

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

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

8. Solution Deployment Manager

- It is required to add valid SNMP attributes while adding the Communication Manager from **Home →Inventory →Manage Elements**. This helps Refresh Element(s) to work properly for Analyze during SDM upgrade of Communication Manager.
- System Manager must gain access to **ftp.avaya.com** and **plds.avaya.com** to download firmware and for the Solution Deployment Manager Analyze functionality to work properly.
- It is required that the set of elements we want to upgrade in single go should be selected in pre-upgrade check in a single go.
For e.g. in case we have 2 different System Platforms (having CM, BSM and utility server in each). If we want to upgrade these 2 SPs, we should perform pre-upgrade check for both these SPs in a single go i.e. we should select both the SPs from landing page and do pre-upgrade check on the required target host in one batch only.
If we perform pre-upgrade check of these 2 system platforms in different batches from UI, each batch may pass but complete set (with both SPs) may fail on one target ESXi host
- VE to VE upgrade is not supported in 7.0. Patching over VE is supported once migrated to 7.0 VE.
- Scheduling of deployments is not supported in 7.0
- **vCenter add** or **host add** operations are asynchronous. If the addition fails due to wrong credentials then a row in the respective grid is show with FAILED status. Edit this row and provide proper credentials to complete the add operation.
- When user stops vm through SDM Client/System Manager, the IP and FQDN of vm will not disappear from SDM/System Manager even though vCenter will not have IP/FQDN of that vm.
- If user performs Restart operation on any vm, the current action status will be either of 'VM_START:COMPLETED' or 'VM_START:FAILED'.
- Make sure the date/time of element is in sync with date/time of System Manager before starting migration.
- If you have freshly installed AVP, make sure to accept the license by logging into AVP CLI and accepting the license before migrating/deploying VMs on it.
- On upgraded servers, if vCenter or host is already added before upgrade, then do vCenter refresh/host refresh after upgrade to get the correct information of vCenter or host.
- If user enables OOBM IP after deployment, System Manager will display the old IP. You need to refresh the host you will get the correct OOBM IP displayed in the VM IP field. After

you enable OOBM in the background, **host refresh** needs to be done before trust establishment. Then perform refresh VM.

9. CMM Migrations

Since the CMM backup size can be very large (around 250GB), here is what needs to be done to take care of CMM backup.

Manual Step:

Take CMM backup on 5.2.1 machine as well as on 6.3.x machine

If machine is on 5.2.1, Install the following RPMs:-

- Install A9021rf+i.rpm and C1317rf+i.rpm on 5.2.1 CMM enabled system. [RPMs are available on support site under CM 5.2.1 version downloads at : <https://support.avaya.com/downloads/download-details.action?contentId=C200993164541898017&productId=P0523&releaseId=5.2.x>]
- Once the above RPMs are installed, the swversion for CM Messaging would look like
Messaging: +-N5.2.1-13.0---Ci+Ak+----

Now again take CMM backup after installing the RPMs.

Note: Take the backup from CM 5.2.1 machine and keep it on a different remote server which can be used for restore post migration.

Once the user has manually taken the CMM backup, then trigger migration from System Manager webconsole. The migration will shut down CM , and deploy CMM and CM (For CM , everything thing is taken care by System Manager , including migration patch and taking backup and restoring it)

10. Same Server Migrations

- If you are Migrating same server again. Please follow below steps

For SP server Migration re-testing:

- Delete SP Backup from **System Manager Server** at location `/swlibrary/orchestrator/backup/System_Platform/<CDOM_IP>`
- Remove files `/tmp/<CDOM_IP>_spbackup.lock` and `/tmp/<CDOM_IP>_spshutdown.lock` from **System Manager Server**.
- Delete SP Backup from **CDOM BOX** at location `/vspdata/backup/archive/backup_for_migration.tgz`

11. Session Manager Migrations

For Bare Metal SM Migration re-testing:

- Delete all the files from **SM box** at location `/opt/avaya/common_services`.

12. System Platform (SP) based system Migration

- Run the command service **cdom-monitor stop** on **DOM0** before starting migration of SP based System.
- If you are migrating SP based elements, the status of backup being taken and downloaded to System Manager shows status of one of the elements of SP and rest of the elements will wait in Pre-upgrade check. Check status of all the elements under SP to know the exact steps.
- If upgrade is in process, do not restart JBOSS.

13. CM Migrations

Before Upgrade to CM6.x to CM 7.0 OVA ensure appropriate footprints. Below is the Summary of profile mapping table:

Template installed on CM6.x	Profile in CM7.0
CM_onlyEmbed * (S8300D/E)	CM Main Max users 1000

Template installed on CM6.x	Profile in CM7.0
CM_SurvRemoteEmbed (S8300 D/E)	CM Survivable Max users 1000
CM_Simplex *	CM Simplex2 Max users 36000
CM_SurvRemote	CM Simplex2 Max users 36000
CM as part of Midsize_Ent *	CM Simplex1 Max users 2400
CM_Duplex	CM Duplex Max users 30000
CM_Duplex (high capacity)	CM High Duplex Max Users 36000

14. User Management Communication Profile Page

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

If you are upgrading from System Manager 6.3.4 or earlier to System Manager 7.0, you must specify the password for the Alarm Email notification on the System Manager **Global Profile** configuration page, only if you have configured the Alarm email notification in the earlier release.

15. Verify the System Manager Release version

After installing System Manager 7.0, verify the release of the installed System Manager by clicking on **Settings** icon and then the **About** menu in the top-right corner of the Home page. You can also run the **swversion** command through the Command Line Interface (CLI).

16. 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.

17. System Manager Hostname

System Manager complies with RFC952 for hostnames.

18. Log in to System Manager

For more information, see [Log in to System Manager](#).

19. Understand the password and aging policy for the admin user account

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

20. Third- party certificate in case of upgrade

You must regenerate and reimport the third- party certificate for an upgrade from earlier releases (6.2 or earlier) of System Manager to System Manager 7.0 Release. You must follow this process if System Manager is using third- party identity certificates before the upgrade.

For System Manager-Session Manager replication, System Manager Identity certificate must have the virtual fully qualified domain name (VFQDN) of System Manager in the Subject Alternative Name. If you upgrade System Manager to 7.0, the Identity Certificate used before the upgrade is retained but this certificate does not have the VFQDN as the Subject Alternative Name. Due to this, replication to Session Managers stops when Session Managers in the environment are upgraded to 7.0 Release.

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

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

secondary System Manager Servers if the entries are missing from DNS.

22. 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.

23. External authentication configuration

If you upgrade directly to System Manager 7.0 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 7.0 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](#).

24. Login warning banner upgrade

If you want to upgrade directly to System Manager 7.0 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 7.0 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](#).

25. Browser Cache

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

26. Shell account

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

27. Remote System Manager backup

Before you select the **Use Default** checkbox, you must first set the remote parameters such as Remote Server Password, Remote Server Port, Remote Server, and Remote Server User in the *Home/Services/Configurations/Settings/SMGR/SMGR Element Manager* page.

Use absolute path while giving the remote backup name.

28. System Manager Data Backup

- System Manager supports backup and restore on Solarwinds(Windows) server.
- In **Home → Services → Configurations → Settings → SMGR → SMGR Element Manager**
 - Default value of **Backup Directory** changed to “/swlibrary/backup”
 - Range of **Maximum Backup Files** changed to 5, with 3 as default value
- It is mandatory to provide complete path while taking remote backup.

29. Out of Band Management

- Main IP and OOBM IP should not be same
- While deploying application form SDM Client/Centralizes SDM and configuring OOBM for the application, please make sure SDM Client/Centralizes SDM machine should be reachable to OOBM network.
- Management IP and Public IP should not be same

30. CS1K

CS1K 7.6 SP7 is supported with System Manager 7.0.

31. System Manager Data Migration

Recommendation is to copy System Manager Backup file to **/swlibrary** folder for data migration.

32. Logjam Error

Note: Firefox version 39 is not supported browser version.

How to make Firefox safe against logjam attack - have to install Disable DHE add-on - <http://techdows.com/2015/05/how-to-make-firefox-browser-safe-against-logjam-attack.html>.

Prerequisites for a new installation of System Manager

- a) Prerequisites for System Manager 7.0 on Avaya Provided Appliance
 - a. Appliance Virtualization Platform 7.0 (AVP) must be installed on supported hardware
 - b. SDM Client will need to be loaded on a Technicians PC to deploy the Utility Services 7.0 and System Manager 7.0 OVAs. Ensure that firewall allows 443 and 1527 ports that are required for the SDM client installation and SDM functionality.
- b) Prerequisites for System Manager 7.0 on Customer Provided VE
 - a. Install the **ESXi** 5.0/5.1/5.5 on VMware.
 - b. Install **vSphere Client** 5.0/5.1/5.5, and ensure that vSphere Client is connected to the server.
 - c. Install System Manager 7.0 VE OVA.

Refer *Deploying Avaya Aura® System Manager* for System Manager on VMware installation, configuration, and upgrade information.

Prerequisites for upgrade of System Manager

1. Create a backup of the System Manager data using System Manager backup feature.

Refer *Upgrading Avaya Aura® System Manager to Release 7.0* for System Manager Upgrade on VMware information.

Appliance Virtualization Platform (AVP) Servers available to run System Manager 7.0

For new purchases, System Manager 7.0 will be shipped with the HP ProLiant DL360 PG8 server. The server is available in three different form factors and is based on the three different Appliance Virtualization Platform (AVP) server constructs.

When new orders for System Manager 7.0 are processed, the ASD tool will use the following factors in calculating our which AVP server construct will ship to run System Manager 7.0:

1. Total number of System Manager Users.
2. Total BSMs in the enterprise.
3. Total SMs in the enterprise.
4. If System Manager will run in Standalone or in a Shared configuration (System Manager runs with other applications on the same server).

Component	DL360PG8 SRVR LARGE AVP	DL360PG8 SRVR MEDIUM AVP	DL360PG8 SRVR SMALL AVP
Form factor	1U	1U	1U
Processor family	Intel (2.9 GHz - E5-2667)	Intel (2.3 GHz - E5-2630)	Intel (2.3 GHz - E5-2630)
Number of processors	2	2	1
Memory type	4 GB RDIMM (16)	4 GB RDIMM (8)	4 GB RDIMM (4)
Total memory	64GB	32GB	16GB

Component	DL360PG8 SRVR LARGE AVP	DL360PG8 SRVR MEDIUM AVP	DL360PG8 SRVR SMALL AVP
Hard Disk Drive	300GB Drives	300GB Drives	300GB Drives
Number of Hard Disk Drive	4	3	2
RAID Level	5	3	1
Network interface	4	4	4
Optical drive	DVD+/-RW, SATA, INTERNAL	DVD+/-RW, SATA, INTERNAL	DVD+/-RW, SATA, INTERNAL
Power supply	750W AC	460W AC	460W AC
Number of power supplies	2	2	1

Table: HP DL360PG8 Specification

System Manager 7.0 and Appliance Virtualization Platform (AVP) 7.0 running on customer provided servers, including the HP ProLiant DL360PG8 and Dell PowerEdge R620 servers that are not sourced from Avaya will not be supported. System Manager 7.0 can be deployed on a customer's VMware infrastructure which includes VMware Certified Hardware.

For existing System Manager Servers in the field, the following Avaya supplied servers are certified to run System Manager 7.0. The S8800 that supported System Manager 6.x will no longer be supported for System Manager 7.0 deployments

Server	System Manager 7.0
HP ProLiant DL360 G7	√
Dell Power Edge R610	√
HP ProLiant DL360 PG8 (Common Server R2)	√
Dell Power Edge R620 (Common Server R2)	√

Table: Supported Server Platforms

Hardware Tracking Codes	Description	Usage Description
380764	DL360PG8 SRVR SMALL AVP	DL360PG8 SERVER SMALL APPLIANCE VIRTUALIZATION PLATFORM
380763	DL360PG8 SRVR MEDIUM AVP	DL360PG8 SERVER MEDIUM APPLIANCE VIRTUALIZATION PLATFORM
380762	DL360PG8 SRVR LARGE AVP	DL360PG8 SERVER LARGE APPLIANCE VIRTUALIZATION PLATFORM

System Manager Geographic Redundancy (System Manager-GR) Hardware Requirements:

- For the Avaya Provided Appliances all servers are identical (manufacturer, model, platform resources). For example Primary on Dell620 and Secondary on Dell620 would be supported; Primary on Dell620 and Secondary on HP DL360PG8 would not be supported
- For Customer Provided VE hardware environments System Manager-GR is supported on any certified VMware hardware. Note that in mixed System Manager-GR hardware environments (Primary server on Avaya Provided Appliance and the Secondary on Customer VE) System Manager-GR not supported.

Software information

Software	Version	Note
Postgres	9.3.4	Used as a System Manager database. For more information, see: http://www.postgresql.org/docs/9.3/static/index.html
CentOS	6.5 64 bit	Used as the operating system for the System Manager template
Open JDK	1.7 update 79 64 bit	For SDM Client , Open JDK 1.8.0-internal
JBoss	6.1	
Internet Explorer	9.x, 10.x and 11.x	Support for IE8 will no longer be officially supported (Microsoft announced EOS for IE8 effective as of January 2015) Use Internet Explorer 9 with following version and updated version. Version:9.0.8112.16421 Updated Versions: RTM(KB982861) Internet Explorer 10 with following version and updated version. Version 10.0.9200.16521CO Update Versions: RTM(KB2718695) Internet Explorer 11 with following version and updated version. Version : 11.0.9600.17914CO Update Versions: 11.0.21(KB3065822)
Firefox	36, 37, 38	Earlier versions of Firefox will no longer be officially supported.
Tomcat	8.0.18	
VMware vCenter Server, vSphere Client, ESXi Host	5.0, 5.1, 5.5	

Installation and Upgrade note

Download following from Avaya Support Website:

- **Administering Avaya Aura® System Manager for Release 7.0** for administering System Manager.
- **Deploying Avaya Aura® System Manager** for System Manager on VMware installation, configuration, and upgrade information.
- **Upgrading Avaya Aura® System Manager to Release 7.0** for System Manager Upgrade on VMware information.
- **Deploying Avaya Aura® applications** for deploying Aura applications using System Manager Software Deployment Manager (SDM) and Software Deployment Manager – Client (SDM-Client).
- **Upgrading Avaya Aura® applications to Release 7.0** for upgrading Aura applications using Software Deployment Manager (SDM).
- **Migrating and Installing Appliance Virtualization Platform** for installing and upgrading AVP.

Note: Deploying Avaya Aura® applications and Upgrading Avaya Aura® applications include the Installing SDM client procedure.

Download System Manager 7.0

Note: This section gives download information. For installation and upgrade procedure, see documents mentioned in Installation and Upgrade note.

#	Procedure	Notes
1.	Download System Manager 7.0 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-7.0.0.0.16266-e55-43-29-II.ova PLDS Download ID: SMGR70GA001 Size: 3,323 MB md5sum: 4cc7bb1ac1d1772d04832f0b79768323
2	Download System Manager 7.0 SDM Client from the Avaya PLDS website .	Avaya_SDMClient_win64_7.0.0.1.17824_7.zip PLDS Download ID: SMGR70GA003 Size: 212 MB MD5SUM: 68c57b545feea6e09d0ad1f853d8ba8
3	Download System Manager 7.0 VE Profile-3 OVA from the Avaya PLDS website	SMGR-PROFILE3-7.0.0.0.16266-e55-43-29-II.ova PLDS Download ID: SMGR70GA005 Size: 3,402 MB md5sum: 0a0de2f3cfaaa63489f34668e2793946

Note: To leverage deployment via Service Port using SDM client, please get the SDM client Software from Avaya support site. The SDM client version available in the media does not support Service Port deployment.

Download Data Migration Utility

Note: This section gives download information. For installation and upgrade procedure, see documents mentioned in the Installation and Upgrade note.

Note: The data migration utility is required only if you are upgrading from System Manager 6.0.x, 6.1.x, 6.2.x, and 6.3.x.

1.	Download System Manager Data Migration Utility.	Data_Migration_Utility_7.0.1.0_r94.bin PLDS Download ID: SMGR70GA002 Size: 1 MB MD5sum: 47b38d5136f8bc9c07affc6ba6ed53a8c
----	---	--

Information about SDM supported Avaya Aura® Products and their Release Notes

- Appliance Virtualization Platform : <https://downloads.avaya.com/css/P8/documents/101014487>
- Avaya Aura® Session Manager: <https://downloads.avaya.com/css/P8/documents/101013927>
- Avaya Aura® Communication Manager: <https://downloads.avaya.com/css/P8/documents/101014152>
- Avaya Aura® Presence Services: <https://downloads.avaya.com/css/P8/documents/101013731>
- Utility Services: <https://downloads.avaya.com/css/P8/documents/101014064>
- Avaya Aura® Application Enablement Services: <https://downloads.avaya.com/css/P8/documents/101014420>

Information on Versions.xml

The versions*.xml is published on <ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/SUM/>

Known issues and workarounds

All the following issues are applicable for System Manager on VMware.

Problem	Keywords	Workaround
Installed Patches page (SDM upgrade workflow) on System Manager webconsole displays the BSM OVA information which is incorrect display.	SMGR-35012	This display is incorrect and it is recommended not to perform commit, rollback and uninstall on this page for BSM 7.0 OVA.
Change IP FQDN is failing in Primary System Manager. Enable Geo Replication is failing after executing Pair IP FQDN in Primary SMGR. Change IPFQDN - Corresponding SMGR Manage Elements attributes not updated.	SMGR-33581 SMGR-33617 SMGR-33602	A hotfix is available. Contact Avaya Technical Support for information.
Unable to add vCenter	SDM-708	
Corporate Directory ,IPSec,Numbering Groups,Patches,Secure FTP Token,SNMP Profiles,Software Deployment element links from Element Manager page is not opening correct linked page.	SMGR-33187	User can access these links from HOME/Users/Administrators.
Not able to download reports from Home / Services / Reports / History page sometimes.	SMGR-32844	While downloading the generated reports, if we get following exception on page “/pages/reports/reportsHistory.xhtml @39,99 value="#{reportHistoryDataBean.percentSpaceUsed()}”: Illegal Syntax for Set Operation” , then click on left navigation and retry operation once again.
Unable to access the Home / Services / Configurations / Settings / SMGR / SMGR Element Manager page on the 6.0 SP2 to 7.0 upgrade path.	SMGR-32589	
In case of start/stop/restart VM , the VM IP/FQDN is not getting updated if browser F5 button is done while the operations are in progress and also vm state goes in inconsistent state.	SMGR-30883 SMGR-32504	Do not navigate away from the VM MGMT page or refresh the browser if start/stop/restart is triggered from that browser.
There is no option to configure the network parameters again if CMM migration is failing.	SMGR-31822	For CMM, we do not have the pre-populate script to pre fill the configuration details (i.e., the IP , subnet gateway etc.) . The reason for this is that since the CMM is residing on CM itself as a service , we would be changing the IP and other details during migration (to make it a new VM) , hence we cannot pre populates this data . Thus user is advised to fill in CMM configuration details carefully and correctly. In case CMM migration fails(due to incorrect network configurations provided) , one needs to do the following:-

Problem	Keywords	Workaround
		1) Delete VM from ESXi. 2) Deploy a new CMM OVA . 3) Restore the CMM backup (which is taken manually on CM 5.2.1 box with CMM RFUs installed , as already mentioned).
The Session Manager license becomes invalid when a new System Manager OVA is installed or when the System Manager IP address is changed.		Obtain and install a new license per normal procedures as described in the Administration guide.
While adding host via vCenter, API is throwing exception if login using sso user.	SDM-444	Recommend to use local vCenter user.
Upgrade Management web console page displays issues on IE 10 and IE11 browsers.	SMGR-31407	
Change of 'admin' password on CLI is not asked when user is logged in using console through vCenter.	SMGR-30163	
Security page: Download JKS file should display password as encrypted.	SMGR-29964	
Out-of-Band Hostname is prompting FQDN when System Manager is installed using vCenter and short name when System Manager is installed using ESXi host.	SMGR-30502	
System Manager dashboard does auto refresh after every 10 to 20 seconds on IE11.	SMGR-30272	
Issue for pre-upgrade check for first time after analyze operation on System Manager.	SMGR-31122	
Issues with Refresh plugin of CM and CMM.	CM-7723	Update the CM or CMM to Service pack 7.0.0.1
Refresh VM and Re-establish trust fails because the ID of csadmin is different on LSP and Main.	CM-11538	

Appendix

Log in to System Manager

System Manager CLI:

- You can gain access to the command line interface with admin as the user name and the password. SSH password must be changed during the first login. The default SSH user credential is admin/admin..

System Manager Web Console:

- When you log in to the System Manager Web 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 setting 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 admin users of System Manager CLI and System Manager Web console are different users and independent of each other.

External authentication configuration

To reconfigure the System Manager external authentication:

1. Click **Users > Administrators**.
2. In the left navigation pane, 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.

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 in this release:

- **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.

Technical support

Avaya Technical Support provides support for System Manager 7.0.

For any problems with System Manager 7.0, you can:

1. See the documentation that is shipped with your hardware for maintenance or hardware-related problems.
2. Retry the action. Carefully follow the instructions in the printed or online documentation.
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 problems persist, 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, if any, to reproduce the problem.
- The release version in which the issue occurs.
Note: To know the release version and build number, log in to System Manager. Click **Settings** > **About** in the top-right of the dashboard. You can also 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 the `/opt/vsp/collectLogs.sh` script for collecting logs from the system.

You might be asked to send one or more files by email 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>.