# Avaya Aura® System Manager
# 6.1 Service Pack 6 Release Notes

**Release: January 2012**

**Issue: 2.0**
**January 30, 2012**

**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 Note gives you information about Avaya Aura® System Manager 6.1 SP6 application and the supported documentation. This Release Note contains information about known issues and the possible workarounds. The Appendix sections describe the procedure for changing IP address or host name, changing date and time configuration, the Cold standby procedure, how to schedule a data backup and restore a backup script for Avaya Aura ® System Manager and Avaya Aura ® System Platform HA mechanism, and how to reset a user password. For the documents on installing and upgrading to System Manager 6.1, see Installing and Upgrading Avaya Aura® System Manager Release 6.1 on the Avaya Support Web site at http://support.avaya.com.

System Manager 6.1 SP6 is delivered in the form of an installable unit that you can install on System Manager 6.1 SP1.1 and deploy as a virtual appliance on System Platform 6.0.3.0.3.with patch 6, ( 6.0.3.6.3).

# Changes delivered to System Manager 6.1 SP6

Except System Manager 6.1 SP1.1 all other Service Packs are cumulative, and changes in System Manager SP2, SP 3, SP4 and SP5 are included in System Manager 6.1 SP6. The changes delivered to System Manager 6.1 SP6 are grouped as follows:



## Product Support Notices

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

To read a PSN description online:

1. Go to the Avaya Support Web site at http://support.avaya.com.
2. In the left navigation pane, click **Products**. The system displays a search text box.
3. Enter the product name as "*System Manager*" in the search text box.
4. On the search result page, scroll down to **Product Notices** and click **Product Support Notices**.

5. On the upper-left corner of the table, filter the searched product based on the PSN release.

6. To open a specific PSN, click the PSN title link.

# Enhancements

The following changes are new to System Manager and are included in this release:

**Table 1: Enhancements delivered to System Manager 6.1 SP6**

| Enhancement | Keywords |
|---|---|
| Support aut-msg-wt feature button on SIP phones | Endpoint Management |

# Problems fixed in System Manager 6.1 SP6 and previous System Manager 6.1 SPs

System Manager 6.1 SP1.1 is a template based installation. Following are the fixes delivered in System Manager 6.1 SP1.1

# Problems fixed in System Manager in 6.1 SP1.1

**Table 2: Fixes delivered to System Manager 6.1 SP 1.1**

| Problem | Keywords |
|---|---|
| The Logging UI of System Manager 6.1 did not display the Authentication (OpenSSO) logs. | Authentication logs |
| The system did not display a warning message to the administrator that SSL is provisioned with the wrong port resulting in an unsecured connection. | External Authentication |
| The Session Timeout pop-up notification did not appear on System Manager. | Session timeout |
| When you changed the admin password through the forced change password feature or through the UPM change password link, then the bulk export utility did not accept the changed password.<br><br>**Note:**<br>You do not have to specify the user name and password while executing bulk export utilities using the CLI interface. | User Bulk Export |
| In the earlier releases, the session timeout value was specified under the Common Console settings. From Release 6.1, you can control this configuration from the **Home** > **Users** > **Administrators** > **Security** > **Policies** screen.<br>**Session Properties** > **Maximum Session Time**: The maximum session time even if the session is not idle.<br>**Session Properties** > **Maximum Idle Time**: The maximum session time when the session is idle. | Session timeout |

| | |
|---|---|
| The common console settings might still display a property for configuring the session timeout, but the property is not used and will be removed.<br><br>**Note:**<br>When you upgrade to System Manager 6.1, you must perform the modification again from **Home** > **Users** > **Administrators** > **Security** > **Policy**. | |
| If you upgraded the system from Release 6.1 Beta, the restore did not work from the UI while performing the Cold standby setup. | Restore |
| If you upgraded System Manager from an earlier release to System Manager 6.1 SP1.1, the DRS performance setting was lost. | DRS, Replication |
| If you modified the default system-provisioned and scheduled jobs, such as ClrdAlarmPurgeRule, LogPurgeRule, SoftDelRTSPurgeRule, and PurgeJobStatus to run more frequently, then the system could become unstable. | Scheduler |
| You could not set the type field of User in the Endpoint profile of **Home** > **Users** > **User Management** to support voice mail on Avaya Aura® Communication Manager. | Communication profile |
| You could not edit the endpoint with the XMOBILE set type where the port number was not required. | XMOBILE |
| If you changed the host name of System Manager from System Platform Web Console and the old short host name was a part of the new short host name, the host name change was ineffective. | Installation |
| You faced a problem with the System Manager User Interface (UI) layout when you accessed the old System Manager system (Beta or Alpha) and later upgraded to System Manager GA. | User Interface look and feel |
| If you added more than 50 signaling groups on Communication Manager, then IP telephony centralized management fetched only the first 50 signaling groups. If you added any signaling group after the first 50 of the SIP or H323 type to the trunk group of SIP, then the Communication Manager initialization synchronization failed. | IP telephony centralized management |
| A majority of the Operating system (CentOS) vulnerability issues have been addressed in System Manager 6.1 SP1.1. | Security Updates |
| Kernel security and bug fix updates. | Security Updates |
| If the Service technician logged in through etoken, the session did not end from the browser after logoff. | Service technician login |
| You were not assigned permission when authenticated by an external Active Directory server. | External Authentication |
| If a soft deleted user associated with the Communication Manager communication profile, Communication Manager synchronization failed. | User communication profile |

| | |
|---|---|
| If Communication Manager displayed an error message on the extension being used as a remote extension in UDP, the **Delete endpoint** function failed. | Communication Manager |
| Communication Manager Incremental synchronization failed if you deleted Intra Switch CDR from Communication Manager. | Communication Manager |
| If you observe a consistent backup failure, the reason might be that the backup lock was not released in one of the earlier backups. | CS1000 |
| While accessing the **Administrators** link in the dashboard, the system displayed a permission error due to the single sign-on setting after a fresh installation or an upgrade from the earlier System Manager release to System Manager 6.1 SP 1. | CS1000 |
| Synchronizing a Subscriber Manager Presence password with UPM failed if the communication profile had more than one communication address. | CS1000 |
| The system did not forward the Subscriber Manager logs to the System Manager log viewer. | Fault Management |

# Problems fixed in System Manager 6.1 SP2

System Manager 6.1 SP2 to SP6 is delivered in the form of an installable unit that you can install on System Manager 6.1 SP1.1. Following are the fixes delivered in System Manager 6.1SP2

**Table 3: Fixes delivered to System Manager 6.1 SP2**

| Problem | Keywords |
|---|---|
| The system did not handle the proper error message for UPM bulk import while performing validation. | Bulk import |
| When trying to export a trusted certificate, you could not import or open the generated trust-cert.pem file with openssl as the encrypted part of the file was one big line instead of multiple lines. | Certificate Management |
| The partial-and-replace import did not work for communication profile handles. | Bulk import |
| The system displayed the patch version when you used CLI to check with swversion. | Software Version Management |
| The system displayed the patch version when you clicked **About**. | Software Version Management |
| [RHSA-2010:0809-01] Critical: xulrunner security update. | Security update |
| [RHSA-2010:0793-01] Important: glibc security update. | Security update |
| [RHSA-2010:0811-01] Important: cups security update. | Security update |

| | |
|---|---|
| [RHSA-2010:0889-01] Important: free type security update. | Security update |
| [RHSA-2010:0893-01] Important: kernel security and bug fix update. | Security update |
| [RHSA-2010:0926-01] Moderate: krb5 security update. | Security update |
| [RHSA-2010:0966-01] Critical: firefox security update. | Security update |
| [RHSA-2010:0976-01] Important: bind security update. | Security update |
| [RHSA-2010:0970-01] Critical: exim security update. | Security update |
| [RHSA-2010:0978-01] Moderate: oer.penssl security update. | Security update |
| [RHSA-2011:0013-01] Moderate: wireshark security update. | Security update |
| [RHSA-2010:0819-01] Moderate: pam security update. | Security update |
| [RHSA-2011:0004-01] Important: kernel security, bug fix, and enhancement update. | Security update |
| Changing the endpoint set type using Global Change operation failed if the new set type had an empty list for feature buttons. | Endpoint |
| The bulk export of users failed if any user was associated with Endpoint Profile on Communication Manager Release 5.1. | Bulk export |
| You could not change COR of the station from System Manager. | Endpoint Management |
| You could not enter ring type 'i' (icon) when administering a Team button. | Endpoint Management |
| When you opened new Web pages, you had to scroll back up to the top of the New page. | User Interface |
| Scheduler jobs listing was very slow when you changed the Job List row count. | Scheduler |
| When you clicked the browser **Refresh** or **Return** button from the change password screen, all window tabs of System Manager were lost, and you were redirected to the dashboard page of System Manager. | Change Password |
| For changed password confirmation, the system displayed the navigation with a warning message. | Change Password |
| The page title did not display properly when you clicked any link from the Home page, and a new tab opened if you pressed **F5** or **Refresh** on the keyboard. | System Manager Dashboard |
| If you opened multiple tabs from the Home page and closed one of the open tabs and then clicked **F5** or **Refresh** on the keyboard, you could not view the same tab without refreshing the page. | User Interface |

| | |
|---|---|
| Voice Mail Number for SIP extension disappeared after full sync. | CM synchronization |
| Communication Manager incremental sync failed with error in database constraint violations. | CM synchronization |
| You encountered a problem with button assignments on rendering the 9650SIP template on view and edit operations. | Endpoint Management |
| Special language characters did not populate the **Name** field of an endpoint after you committed the changes. | Endpoint Management |
| The system display as RUNNING status in the scheduler for multiple jobs when the previously ran synchronization failed due to an unreliable network connection. | Scheduler |
| The Change Password pages should not display Return button. | Change Password |

# Problems fixed in System Manager 6.1 SP3

**Table 4: Fixes delivered to System Manager 6.1 SP3**

| Problem | Keywords |
|---|---|
| The Welcome matt page of the User Profile Management page displayed some typos. | Welcome matt |
| The GUI Table component did not return the selected rows in order. | User Interface |
| Unauthorized users could gain access to System Manager SNMP server if you did not change the SNMP default password during installation. | SNMP |
| If a bulk export of users job ran for more than 5 minutes, then the scheduler UI showed the incorrect job status, and the created archive name was not the same as the scheduled job name. | Bulk export |
| If you accessed System Manager through IP instead of FQDN, then the system did not display a warning message that the password had expired. | Password Expiry |
| [RHSA-2011:0153-01] Moderate: exim security update. | Security update |
| [RHSA-2011:0199-01] Important: krb5 security update. | Security update |
| [RHSA-2011:0303-01] Moderate: kernel security and bug fix update. | Security update |
| [RHSA-2011:0429-01] Important: kernel security and bug fix update. | Security update |
| [RHSA-2010:0970-01] Critical: exim security update. | Security update |
| [RHSA-2010:0839-01] Moderate: kernel security and bug fix update. | Security update |
| [RHSA-2011:0412-01] Important: glibc security update. | Security update |

| | |
|---|---|
| A restore failure occurs after performing Cold standby in the upgrade scenario. | Cold-standby |
| Backup failed during upgrade from System Manager 6.1 SP2 to System Manager 6.1 SP3 due to a CND lock. | Backup |
| After changing the session time-out configuration, if you logged in and left System Manager idle for an hour and later edited the page, the system did not redirect you to the log-in page. The system displayed an error message that the page timed out. | Session timeout |
| If an admin user tried to import the contact details of a user using the Import Users screen with Import Type set to Partial, the contact list that PPM downloaded to the endpoint was corrupted, and you could not update an existing contact. | Import User |

# Problems fixed in System Manager 6.1 SP4

**Table 5: Fixes delivered to System Manager 6.1 SP4**

| Problem | Keywords |
|---|---|
| Avaya Services CA validates the certificate present in the Avaya Technician E-token during a certificate-based authentication. The certificate will expire in December 2011 and might cause a break in the certificate-based authentication. Therefore, this CA certificate has been replaced with a new CA certificate with a longer validity period. | Certificate expiration |
| SP4 supports patching through System Platform Web Console. | Patch Installation |
| SAL Enterprise tables were corrupted while upgrading System Manager 6.0.7 to System Manager 6.2.2. | SAL Enterprise |
| [RHSA-2011:0004-01] Important: kernel security, bug fix, and enhancement update. | Security update |
| [RHSA-2011:0303-01] Moderate: kernel security and bug fix update. [CentOS] | Security update |
| [RHSA-2011:0833-01] Important: kernel security and bug fix update. | Security update |
| [RHSA-2011:0346-01] Moderate: openldap security and bug fix update. | Security update |
| [RHSA-2011:0412-01] Important: glibc security update. | Security update |
| [RHSA-2011:0429-01] Important: kernel security and bug fix update. | Security update |
| [RHSA-2011:0199-01] Important: krb5 security update [CentOS] | Security update |
| [RHSA-2011:0153-01] Moderate: exim security update. | Security update |

| | |
|---|---|
| [RHSA-2011:0025-01] Low: gcc security and bug fix update. | Security update |
| [RHSA-2011:0027-01] Low: python security, bug fix, and enhancement update. | Security update |
| [RHSA-2011:0025-01] Low: gcc security and bug fix update. | Security update |
| RHSA-2010-0442: Important: mysql security update. | Security update |
| While importing a file with two users, each with more than 200 contacts, the processes failed due to a timeout. The first user update took less than 50 seconds whereas the second user update took about 14 to 15 minutes to update the contact list. | User Bulk Import |
| The system failed to launch Element Manager due to loss of the Linux base links after UCM migration to System Manager 6.1 SP3. | CS1000 |
| Communication Manager Sync hanged in case of a break in connection between System Manager and Communication Manager. | CM synchronization |
| Communication Manager Sync failed when you used an apostrophe (‘) in node names. | CM synchronization |
| The Native Name field of Endpoint did not store correctly if the primary language of the browser was not English. | Endpoint Management |
| The system did not export all the fields for Communication Manager Messaging, Modular Messaging and Avaya Aura Messaging communication profiles. The system only exported the default fields of the Messaging communication profile. | Messaging |
| The 50-digit mailbox number for Avaya Aura Messaging did not work correctly in Manage User Messaging Communication profile and Bulk Import or Export of Users. | Messaging |
| Native Name Display did not accept Korean characters.<br><br>Some clear alarm messages which are not valid were removed from the System Manager alarm rules. | Alarm |
| The xml schema for Import User was validated and updated for *Administering Avaya Aura® System Manager Release 6.1*. | Online Help |
| Disabling a Routing Policy under **Routing** > **Routing Policies** led to database corruption that caused unexpected Session Manager SIP routing. | Routing policy |

# Problems fixed in System Manager 6.1 SP5

**Table 6: Fixes delivered to System Manager 6.1 SP5**

| Problem | Keywords |
|---|---|
| When a user admin performed account sync with the presence server, the system provided a list of anonymous accounts, that is, accounts that do not have a CS1K presence service, including the admin account. If the admin user pressed the **Delete all** button, Subscriber Manager did not send a request to User Profile Management to remove the admin account. | CS1000 |
| The system did not export presencebuddy for associated contacts if the user was exported from System Manager. | User Bulk Export |
| When an XML file was imported to System Manager, the association between the user and contacts did not happen. The system displayed the contacts in the Private Contacts list but not in the Associated Contacts list. | User Bulk Import |
| After a server replacement and a restore of data, digitmaptopolicy data were missing on System Manager. | Data Restore |
| [RHSA-2011:0927-01] Kernel security and bug fix update from CentOS. | Security Update |
| The database vacuum and reindex process running on the box took a long time to complete if the record size exceeded 4 million records. | Large record size |
| Replication status reported as Synchronized for unfinished BSM upgrade. | Data replication |
| The system did not replicate Session Managers after restoring data if you performed System Manager server replacement. | |
| The contact phone number did not support the star symbol (*) as the starting digit. | Contact phone number |
| An administrator can create users with hyphen (-) in their log-in names. | User Management |
| If you did not reach a node for a maximum period of 12 hours, Data Replication Service (DRS) invalidated the node and marked the node in the Ready For Repair state. When DRS invalidated a node, the system removed all pending events and unsent batches of the node. The node must be repaired when you reboot the nodes. | Data Replication |
| The system triggered a backup during restore and sometimes, the system overwrote the backup file. | Data Backup |
| During Security Domain registration with Avaya Aura System Manager, the system did not save the values that were too long, that is, more than 41 characters, into certain tables. | Domain Registration |
| When you log in to System Manager and click **Administrators** > **Software Deployment** on Dashboard, the page did not redirect to **UCM Deployment Manager** for CS1000. | CS1000 |
| The synchronization failed after adding endpoints as the coverage point to the coverage path. | CM synchronization |

| | |
|---|---|
| Initialization synchronization did not update the Communication Manager capacity system limit for Current System Memory Configuration. | CM synchronization |
| The server **IP address** field of IP Network Region did not synchronize with the Database. | CM synchronization |
| The system did not delete the Available Messaging mailbox range from the System Manager post a successful synchronization with Messaging if you changed any mailbox ranges in Messaging. | Messaging |
| A user with the **Communication System Viewer** role could not view Coverage Path and Service Hours Tables. | User Roles |
| Initialization synchronization failed at **list service-hours-table 100 count 50** command with the CM response: **Requires CMS R16.1 or later**. | CM synchronization |
| A user with **Communication Manager Administrator role** did not have permissions for Global Endpoint Change. | User Roles |
| The transaction remained incomplete when a station of set type 105TL was synchronized. | CM synchronization |
| Synchronization failed if remote subscribers were present on Modular Messaging. | CM synchronization |
| Synchronization hanged if Communication Manager had a large number of authorization codes, such as 40k or 50k. | CM synchronization |
| Synchronization would hang after changing group extension on hunt group in System Manager through Element Cut-through, and subsequent incremental synchronization also failed. | CM synchronization |
| User Bulk Export did not export the **voicemailnumber** field. | User Bulk Export |
| The backup announcement job created a zip file with the name, UnknownJob zip. | Announcement Management |
| After the renaming operation of an integrated announcement, the system did not display the audio file on the announcement page. | Announcement Management |
| Service-hour-table: The system did not remove the deleted entries after incremental synchronization of Communication Manager. | CM synchronization |
| IP Telephony Centralized Management does not handle station ranges properly if all leading digits (0 to 9) are present in dial plan analysis configuration. | Communication Manager |
| The filter for Class of Restriction did not work in Authorization codes. | Communication Manager |

# Problems fixed in System Manager 6.1 SP6

**Table 7: Fixes delivered to System Manager 6.1 SP6**

| Problem | Keywords |
|---|---|
| Unable to create a user from the Manage User page. | User Management |
| The bulk import with merge option fails while trying to edit an existing user with station communication profile. | User Bulk Import |
| The verisign certificates at the Avaya Data Centre upgraded from 1024 to 2048 based certificates. The same certificate needs to be inserted into the System Manager SAL enterprise trust store. | Avaya Data Center Certificate renewal |
| ecryptfs-utils security update. | Security update |
| The time zone of alarm UI changes when you clicked the Refresh button. | Alarming |
| Alarms were not generated with UID in uppercase during an LDAP authentication. | Authentication |
| Handles with the same handle ID and different domain names were not getting merged. | Bulk Import |
| During System Manager upgrade, Postgres Certificates should also be renewed along with other System Manager certificates for internal services. | Certificate Management |
| SSL Services on ports 4444, 2009, 52233 supported with Weak Encrypted Ciphers. | Security Update |
| Replication between System Manager and SM if failing due to the Unified Communication Manager signed certificate being picked when the System Manager HTTPS port is initialized. | Installation |
| After performing synch operation, only a subset of all IP interfaces are shown in System Manager when Communication Manager had 50+ IP interface objects | Communication Manager |
| Incremental/Init sync fails with constraint violation on siggrp/trunk | Communication Manager |
| System Manager does not handle station ranges for Uniform Dail Plan, if all leading digits (0-9) are present in Dialplan Analysis | Communication Manager |
| If Modular Messaging sync fails, it won't be able to add, remove or update System Manager database using Modular Messaging web management interface | Messaging |
| Incremental sync fails with  extension when referenced by port extension id in Agent Login-ID | Communication Manager |

| | |
|---|---|
| When same extension pack is assigned to a User in different Communication Manager communication profile sets for different CMs, the station get created for one Communication Manager and not for other. | User Profile Manager |
| Incremental sync fails on removing locations | Communication Manager |
| Communication Manager sync does not complete if AAR/ARS Analysis/Conversion has more than 15 entries for same dialed string | Communication Manager |
| Station delete fails if it is associated with Coverage Answer Group | Endpoint Management |
| Incremental synchronization takes a long time synchronizing the hunt group and coverage answer group if they are added as a coverage point in the coverage path and then the groups are removed from CM SAT. | Communication Manager |
| Multiple Syncs are running simultaneously | Communication Manager |
| Incremental synch fails when a user is added with set type having soft keys | Endpoint Management |
| Feature Options now working properly if changed via Global Endpoint Change | Endpoint Management |
| Group Membership not seen when endpoint editor is launched from Manage Users | User Profile Management |
| The freed extensions are not properly getting deleted in Initialization sync. So the available list of extensions not showing some extensions. | Endpoint Management |
| Cannot delete the subscriber from System Manager if it is already deleted from Messaging System | Messaging |
| User with CM Admin does not have permissions for Bulk Agent operations | Role Based Access Control |
| Button validations of ring type are missing on doing commit of template and add station. | Endpoint Management |
| Incremental Sync fails if Node Name changes | Endpoint Management |
| Using Element Cut Through to add a station and specifying "next" syncs all the extensions | Communication Manager |
| Some objects cannot be deleted if they are associated with station due to foreign key constraint violation issues | Communication Manager |
| Sync issue with username more than 27 characters | Endpoint Management |

# The System Manager software

## System Manager installation download

| # | Action | Notes |
|---|---|---|
| 1. | Download the System Platform 6.0.3.0.3 ISO image and patch 4 from the Avaya PLDS Web site. | Verify that the md5sum for the downloaded ISO image matches the number on the Avaya PLDS Web site. |
| 2. | Download the System Manager SP6 IU **System_Manager_06_01_ServicePack6_r1774.bin** file from the Avaya PLDS Web site. | PLDS download ID: **SMGR61SP601**<br>Md5Sum: **397bb9bb2e911810b068d1f8795c246e** |
| 3. | Deploy System Manager 6.1 SP6 IU. | Install System Manager 6.1 SP6 on System Manager 6.1 SP 1.1 with System Platform 6.0.3.0.3.with patch 6 that is 6.0.3.6.3.<br>**Note:**<br>See Installing the patch installer on page 20 |

Note: System Manager 6.1 SP 1.1 is a full ISO image. When you download System Manager 6.1 SP 1.1 from Product Licensing and Delivery System (PLDS), copy the software to a DVD as an ISO image. You must install System Manager 6.1 SP 1.1 on System Platform 6.0.3 with patch 6 (6.0.3.6.3) through CDOM Virtual Machine Solution Template before installing System Manager 6.1 SP6.

System Manager 6.1 SP6 is a binary file. When you download System Manager 6.1 SP6 from PLDS, copy the .bin file to a CD. Next, copy the .bin file to the System Manager 6.1 SP 1.1 Linux Shell and activate the system through the shell with a root login.

## Must Read for a fresh installation or an upgrade

**1. Installation error**

After installing or upgrading to System Manager 6.1 SP1, when you click the **Administrators** link on the dashboard, the system displays an installation error due to the single sign-on setting. To avoid the error, you must reinstall System Manager 6.1 SP1.1 and contact Avaya Support at http://support.avaya.com.

**2. Backup error**

After a fresh installation or an upgrade to System Manager 6.1 SP1, if you observe a consistent backup failure, then log in to the System Manager console through SSH and run the following command:

**$sh /home/ucmdeploy/quantum/quantumBackupRestore/backup.sh**

Contact Avaya Support at http://support.avaya.com if the command fails and the system displays the following error message:

```
INFO - Result = Quantum Backup operation failed. Error: Backup operation failed
for component:    tmp/quantumTmpBRFolder/quantum_service=securityAdmin-
CndBackupRestore.zip
```

.

**3. System Platform upgrade to be performed before System Manager upgrade**

You must deploy System Manager 6.1 SP6 on top of System Manager 6.1 SP1.1 as a virtual appliance on System Platform 6.0 3.6.3. To upgrade System Platform, you must first upgrade System Platform and install System Platform patches, if any, before upgrading System Manager.

4. **Reboot the system after upgrading to 6.1 SP6**

System Manager 6.1 SP6 includes some kernel updates. To ensure that the updated kernel runs in memory, you *must reboot the system* from System Platform or through the System Manager command line interface (CLI).

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

After successful installation of System Manager 6.1 SP6, to verify the release version of the installed System Manager, click **About** on the top-right corner of the Home page or run the **swversion** command through the CLI. The system displays the version information in the following format:

***System Manager 6.1.0 (Build No. - 6.1.0.0.7345-6.1.5.606) Software Update Revision No: 6.1.10.1.1774***

6. **Use FQDN while accessing System Manager**

Avaya recommends the use of Fully Qualified Domain Name (FQDN) instead of the IP address to gain access to System Manager 6.1 SP6.

7. **Admin user account password**

For Avaya Unified Communication Management to authenticate the administrator log-in ID admin, enter the password **admin123**. If you upgrade System Manager from 6.1 GA release to System Manager 6.1 SP6, the administrator password remains the same.

8. **Change password**

To change the **admin** password, on the dashboard, click **Users > Administrators > Avaya Unified Communication Management**. On the Avaya Unified Communication Management page, click **User Services** > **Password**.

9. **Password policy and aging for admin user account**

To verify the password policy and aging for **admin**, use the Avaya Unified Communication Management page. On the dashboard, click **Users** > **Administrators** > **Avaya Unified Communication Management**. On the Avaya Unified Communication Management page, click **Security** > **Policies**.

10. **External authentication configuration**

If you upgrade directly to System Manager 6.1 SP6 from an earlier release, and if you have configured the setup of the earlier release for an external authentication, such as LDAP and RADIUS, prior to the upgrade, you must manually reconfigure external authentication server details after the system completes the upgrade. To reconfigure System Manager, click **Users** > **Administrators** > **Avaya Unified Communication Management**. On the Avaya Unified Communication Management page, click **User Services** > **External Authentication** to modify external identity repositories.

11. **Log-in warning banner**

If you want to upgrade directly to System Manager 6.1 SP6 from an earlier release, and if you have performed any configuration for the legal notice, you must manually reconfigure the log-in warning banner content after the system completes the upgrade. To reconfigure, on the Avaya Unified Communication Management page, select **Security** > **Policies** and click **Edit** to modify the log-in warning banner in the **Security Settings** section.

12. **Authentication not needed for user bulk export**

While running the bulk export utility for bulk export of roles and users, do not specify the user name or password.

13. **Administer CS1000**

System Manager 6.1 is integrated with Unified Communications Management (UCM) 7.5. After you install the System Manager template in which the two applications reside together, you can log in to either of these applications using the Single-Sign-On page. For more information on UCM and how to administer CS1000 using System Manager, see Unified Communications Management Common Services Fundamentals and Subscriber Manager Fundamental version 7.5 at http://support.avaya.com.

14. **WebLM client certificate**

The Legacy WebLM clients communicate with the System Manager-based WebLM server over HTTPS on **Port 52233**. Until System Manager 6.1, this port was secured by self-signed certificates used by legacy or stand-alone WebLM releases. The self-signed certificates used to secure port 52233 in System Manager expired on March 1, 2011. Hence, with System Manager 6.1 SP 1.1, SIP CA-signed certificates replaced these certificates. Because System Manager 6.1 SP 1.1 uses new certificates to secure port 52233, the adopters of WebLM that fulfill the following criteria are impacted:

- Adopting products of WebLM that are integrated with legacy WebLM Java-based clients.

- Products that use port 52233 to communicate with System Manager-based WebLM.

**Impact:** For products that fulfill these criteria, the WebLM client-server communication breaks if a legacy WebLM Java-based client communicates with System Manager 6.1 SP 1.1 WebLM server over port 52233. The communication breaks because the new SIP CA-signed certificate is not added to the truststore of the Java-based WebLM clients.

**Workaround**: Delete the truststore file available with the WebLM Java client and reinitiate the connection with the WebLM server. The default name of the truststore file is **trusted_weblm_certs.jks**. When the WebLM client and the server first communicate, the system creates a new truststore file that contains the correct certificates based on the HTTPS port number for communicating with the System Manager WebLM server.

# Prerequisites

- To deploy System Manager 6.1 SP6, you must install System Manager 6.1 SP 1.1 on System Platform 6.0.3 with patch 6 (6.0.3.6.3)
- If you have deployed 6.1 SP1 and you require upgrading to System Manager 6.1 SP 1.1 you can do it by applying a .bin patch of System Manager 6.1 SP1.1, see the PCN for details of upgrading from System Manager 6.1 SP1 to System Manager 6.1 SP1.1.
- Before installing System Manager Release 6.1 SP6, you must create a backup on the system and store the backup on an external device.
- If you upgrade System Manager from an earlier release and if the System Platform upgrade is required, you must upgrade System Platform before you upgrade System Manager.

# Supported hardware

- Dell™ PowerEdge™ R610 Server
- HP ProLiant DL360 G7 Server
- Avaya S8510 server with atleast 8GB RAM
- Avaya S8800 server

# Software dependencies

| Software | Version | Note |
|---|---|---|

| | | |
|---|---|---|
| Postgres | 8.4.4 | The Postgres version 8.4.4 is used as a System Manager database.<br>For details, see: http://www.postgresql.org/docs/8.4/static/release-8-4-4.html. |
| CentOS | 5.4 64 bit | CentOS-5.4 64-bit is used as base OS for the System Manager template. |
| JDK | Version 6 Update11 32-bit | JDK6 update11 32-bit is used from R6.1 |
| JBoss | 4.2.3 | Jboss is used as application server for System Manager software. |

# Installation note

For the installation and upgrade documentation for System Manager 6.1, see Installing and Upgrading Avaya Aura® System Manager Release 6.1 on the Avaya Support Web site at http://support.avaya.com.

**Note:** For documents containing information about the earlier releases of System Manager 6.1 installation and upgrade, product support, and service packs, sees the Avaya Support Web site.

# Installing the patch installer

1. Log in to the system on which System Manager is running as a **root** user. If direct access to the system using the user **root** is disabled, then log in as a **nonroot** user using direct access to the system. Escalate access privilege restrictions by issuing the **su** command at the server command line interface.
2. Copy the patch installer file from your system to the computer on which you installed System Manager 6.1 SP 1.1.
   Verify md5sum of **System_Manager_06_01_ServicePack6_r1774.bin** with the value from PLDS.
3. Navigate to the directory where you copied the patch installer and grant execute permissions to the file using the following command:
   **chmod +x System_Manager_06_01_ServicePack6_r1774.bin**
4. Run the patch installer using the following command:
   **sh System_Manager_06_01_ServicePack6_r1774.bin**
5. Wait for the system to execute the patch installer and display the installer prompt.
6. After you upgrade the system to SP6, reboot the system from System Platform or through System Manager CLI to get the updated kernel running in memory.

7. Log on to the System Manager Console, and verify whether the System Manager UI is displayed correctly.

# Supported upgrades

**Note:**

- If a System Platform upgrade is required while upgrading System Manager, then you should first upgrade System Platform with the latest patch and then upgrade System Manager.
- A backup set obtained from performing a backup on a particular version of System Platform cannot be used to restore to an older version of System Platform

System Manager 6.1 SP6 supports the following upgrades:

**1. Upgrade from System Manager 6.1**

To upgrade from System Manager 6.1, upgrade:

1. System Manager 6.1 → System Manager 6.1 SP1.1
2. System Manager 6.1 SP1.1 → System Manager 6.1 SP6

**Note:** Before you upgrade System Platform from 6.0.2.0.5 to System Platform 6.0.3.6.3, apply the System Platform patch 6.0.2.6.5 on top of System Platform 6.0.2.0.5. If you do not apply this patch, the upgrade to later versions of System Platform fails.

**2. Upgrade from System Manager 6.0 SP1**

To upgrade from System Manager 6.0 SP1, upgrade:

1. System Manager 6.0 SP1 → System Manager 6.1 SP1.1
2. System Manager 6.1 SP1.1 → System Manager 6.1 SP6

**Note:**

Before upgrading System Platform from 6.0.2.0.5 to System Platform 6.0.3.0.3 with patch 6, apply System Platform patch 6.0.2.6.5 on top of System Platform 6.0.2.0.5. If you do not apply this patch, then the upgrade to later versions of System Platform fails.

3. **Upgrade from System Manager 5.2 SP2**

To upgrade from System Manager 5.2 SP2, upgrade:

1. System Manager 5.2 SP2 → System Manager 6.0 SP1

2. System Manager 6.0 SP1 → System Manager 6.1 SP1.1
3. System Manager 6.1 SP1.1 → System Manager 6.1 SP6.

4. **Upgrade from System Manager 1.0 SP3**

To upgrade from System Manager 1.0 SP3, upgrade:

1. Release earlier than System Manager 1.0 SP3 → System Manager 1.0 SP3
2. System Manager 1.0 SP3 → System Manager 5.2 SP2

**Note:** Upgrade from System Manager 1.0 SP3 to System Manager 5.2 SP2 involves a multistep upgrade. For details, see *Installing and Upgrading Avaya Aura® System Manager Release 6.1*

3. System Manager 5.2 SP2 → System Manager 6.0 SP1
4. System Manager 6.0 SP1 → System Manager 6.1 SP1.1
5. System Manager 6.1 SP1.1 → System Manager 6.1 SP6

# Known problems

This release includes the following known problems in System Manager:

**Table 8: Known problems in System Manager 6.1**

| Problem | Keywords | Workaround |
|---|---|---|
| After deleting and adding an entity for certain sections, the system does not allow committing of the user. You can observe this in the following sections:<br>**Communication Profile > Communication Address**<br>**Contacts > Associated contacts**<br>**Contacts > Private contacts** | | No workaround. |
| In System Manager 6.1 and earlier releases, an administrator who logged in to the System Manager console can view the time stamp of the last login on the upper-right corner of the screen. This feature is not available in System Manager 6.1. | | To check the time stamp of the last logged in information, an administrator must click **Home** > **Users** > **Administrator**. On the Avaya Unified Communication Management page, click **Tools** > **Logs**. |
| System Manager 6.1 and Service Packs do not support authentication with Security Assertion Markup Language (SAML). System Manager 6.0 and earlier releases support authentication with SAML. | | No workaround. |
| When two bulk import jobs are scheduled, that is, the bulk import with communication profile and endpoint, for the same Communication Manager, one of the jobs shows RUNNING state in the Scheduler page even though the job has actually failed. | | Schedule only one bulk job per Communication Manager at a time. |

| | |
|---|---|
| Bulk import of users adds a new user if you try to reimport an existing user through UPM bulk import after changing the log-in name. | No workaround. |
| If you upgrade System Manager from an earlier release to System Manager 6.1 SP6, the system does not retain the porting of Identity and Access Management (IAM) data related to external authentication servers, such as LDAP and Radius. | Re-enter all IAM configuration data after upgrading from any earlier release of System Manager to System Manager 6.1 SP6. |
| The original documentation does not include the additional copyright notices, author names, owner names, and terms and conditions of use as received in the code. | Preserve all additional copyright notices, author names, owner names, and terms and conditions of use, as received in the source code and binary forms. For all redistribution of the source code and the binary forms, retain this copyright notice: Copyright (c) 2000 The Apache Software Foundation. All rights reserved.<br>Also include an additional notice in the documentation and release notes: This product includes software developed by the Apache Software Foundation (http://www.apache.org/).<br>You cannot call the products derived from this software by the Apache name or use the Apache name in writing without prior written permission of the Apache Software Foundation. Include a copy of the license with the product distribution.<br>In addition, include the original and modified open source codes in a source code repository and track all modifications to the open source code in the source code repository. |

| | | |
|---|---|---|
| When you perform backup using Internet Explorer, the system displays the following message: Internet Explorer cannot display the Web page.<br><br>You can observe this issue when the time taken for the backup is more than 30 seconds. | 1. | 1. To start the Registry Editor on the computer on which Windows is running, click **Start** > **Run**.<br>Type **Regedit** and click **OK**.<br>2. Locate the following subkey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings.<br>3. Perform one of the following tasks:<br>(a) If this subkey already exists, change the decimal value to 3600000.<br>(b) If this subkey does not exist, add a Receive Timeout DWORD entry with a decimal value equal to 3600000.<br>(c) Restart the computer.<br><br>For further help, see the Microsoft support site at http://support.microsoft.com/kb/181050. |
| If you restore an older database in a system on the matching software load, the system is considered to be in the Cold standby state. If you upgrade the system to the next service pack, the database backup fails during the upgrade. | | No workaround. |
| Clearing vector steps will not remove the vector from SMGR | | Run full sync to fully remove vector from System Manager |
| After upgrading Session Manager 6.1 SP2 to Session Manager 6.1 SP3, the Replication page still shows that Session Manager 6.1 SP2 is installed. | | No workaround. |
| Alarm flooding at ADC with System Manager Heartbeat Messages. The SAL enterprise, by design, queues up all the messages which are to be sent to ADC and sends them out when the connection is up again. | | No workaround. |
| Native name field is blank even if user has given the native name for VDN | | No workaround |
| Tooltip of some objects does not give correct information for CM with medium memory configuration | | Get the correct information from CM Sat |

# Technical support

Support for System Manager 6.1 SP6 is available through Avaya Technical Support.

In case of issues with System Manager 6.1 SP6, you can:

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

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

- Log in to the Avaya Support Web site at http://support.avaya.com.
- Call or fax Avaya Support on one of the telephone numbers in the Support Directory listings on the Avaya Support Web site.

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

Before contacting Avaya Support, keep the following information handy:

- Problem description.
- Detailed steps to reproduce the problem, if any.
- The release version in which the issue occurs.

**Note:**

To know the release version and build number, log in to System Manager and click **About** on the dashboard.

- The status of the System Manager software. If the software is an upgrade, then from which release?
- The installation log files.
- System Manager JBoss server log file available at ***$JBOSS_HOME/server/avmgmt/log/server.log***.
- Additional System Manager logs at $AVAYA_LOG/mgmt.

**Contact support tasks**

Avaya Support might ask for e-mail notification files for analysis of your application and its environment.

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

# Appendix A: Changing the IP address or host name

After you deploy System Manager, you can change the IP address or the host name of the computer on which System Manager is running. Use System Platform Web Console to effect the change.

## Prerequisites

- Ensure that System Manager is installed on the system and is accessible. You can verify this by accessing the System Manager Web user interface.
- Ensure that all extension packs are successfully deployed:
    1. Log in to System Manager as an administrator using the login `admin`.
    2. On the dashboard, click **Services** > **Configurations**.
    3. In the left navigation pane, click **Extension Packs**.
    4. Verify that the status of the extension pack data is in the Confirmed state.
- After installing System Manager, if you modified any configuration settings on the Settings page, you must make these changes again after you change the IP address or the host name. Note down the changes.
- Ensure that you have performed a manual backup by using the remote backup facility of System Manager Element Manager and data is backed up successfully. For more information on backup, see "Backing up System Platform" in Administering Avaya Aura® System Manager 6.1.

  **Note**: Copy the backup to a remote computer or to an external storage device, such as a CD-ROM or a DVD.

## Changing the IP address and FQDN of System Manager

### Changing the IP address of System Manager

1. Go to the System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Log in as an administrator using the login **admin**.
3. Click **Server Management** > **Network Configuration**.
4. On the Network Configuration page, click **Template Network Configuration**.
5. Modify the following fields in the **Template Network Configuration** section:
    a. Change the IP address to **System Manager IP Address**.
    b. Change Netmask under Domain Network Interface for Bridge avpublic.
    c. Change the server to a different subnet with a new default gateway address.
    d. Change the default gateway in the General Network Settings section.

6. Click **Save**. The system displays the following confirmation message: `Changing network setting may require you to log in again into Avaya Aura System Platform webconsole. Are you sure?`
7. After you confirm the status message, the system displays: `Processing your request, please wait….` Once the system completes the processing and network change, the system displays the following status message: `Settings updated successfully`.
8. Verify that the System Manager Web Console is accessible.

If you configured the SAL Gateway to receive SNMP traps from System Manager, then perform the following tasks from the System Platform Administration user interface:

1. Go to System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Click **Server Management**.
3. Click **SAL Gateway Management**.
4. Click **Launch SAL Gateway Management Portal**.
5. On the Avaya SAL Gateway log-in page, log in as an administrator using your admin privileges.
6. Click **Managed Element**.
7. Click System Manager Hostname in the **Host Name** column displayed in the Managed Elements Found table.
   The system displays the Managed Element Configuration page.
8. Click **Edit** and modify the **Host name** field to the new host name.
9. Modify the **IP Address** to the new IP address.

**Changing the host name of System Manager**

1. Go to System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Log in as an administrator using the login **admin**.
3. Click **Server Management**.
4. Click **Network Configuration**.
5. On the Network Configuration page, click **Template Network Configuration**.
6. On the Template Network Configuration page, in the **Change the Host name marked as Hostname:** field in the **Global Template Network Configuration** section, enter the System Manager Fully Qualified Host name.
7. Click **Save**. The system displays the following confirmation message: `Changing network settings may require you to log in again into webconsole. Are you sure?`

8. After you save the changes, the system displays: `Processing your request, please wait….` Once the system completes the processing and network changes, the system displays the following status message: `Settings updated successfully.`
9. Wait for the network change to take effect and then verify that System Manager Web Console is accessible.

If the SAL Gateway is configured to receive SNMP traps from System Manager, then perform the following tasks from the System Platform Administration UI:

1. Go to System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Click **Server Management**.
3. Click **SAL Gateway Management**.
4. Click **Launch SAL Gateway Management Portal**. The system displays a new window.
5. Log in as an administrator using admin privileges.
6. Click **Managed Element**.
7. Click System Manager Hostname in the **Host Name** column displayed in the Managed Elements Found table.
   The system displays the Managed Element Configuration page.
8. Click **Edit** and modify the **Host name** field to the new host name.
9. Modify the **IP Address** to the new IP address.

## Changing the System Manager IP address and FQDN referenced in the managed elements

### Changing System Manager IP referenced in managed elements

After you change the IP address of System Manager, perform the following procedure to change the IP address of Managed Elements:

1. If the Managed Elements feature uses the JNDI lookup to communicate with System Manager, ensure that all managed elements refer to the new System Manager IP address.
2. The change in the IP address of System Manager affects License Management. Ensure that:

   - The adopting product application recreates the License Manager object with the new IP address.
   - You redo all license acquisitions after the adopting product application recreates the object.

**Changing the System Manager Hostname referenced in managed elements**

If you changed the host name of managed elements, you must also make the following change:

1. If the Managed Elements feature uses the JNDI lookup to communicate with System Manager, ensure that all managed elements refer to the new System Manager host name.

Perform the following steps to make changes in the SAL Agent from the CLI.

1. Edit the host name of the managed element to the new host name in the following files:
   - **$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_DataTransportConfig_orig.xml**
   - **$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_BaseAgentConfig_orig.xml**
   - **$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_SpiritComponentConfig_orig.xml**

   where $SPIRIT_HOME is the base location of the SAL agent deployment on the managed element.
2. Restart the SAL Agent using the following command:
   **# service spiritAgent restart**

The change in the host name impacts License Management. Ensure that:

1. The adopting product application recreates the License Manager object with the new IP address.
2. You redo all license acquisitions after the adopting product application recreates the object.

The change in the host name impacts the Data Replication Service (DRS) client application. Perform the following steps to make changes in the DRS client application:

1. Edit all occurrences of the new System Manager host name in the following files:
   - **$SYM_HOME/WEB-INF/classes/symmetric.properties**
   - **$DRS_HOME/conf/drsClientInstall.properties**
2. Restart the DRS client.

**Changing the IP address and FQDN of managed elements**

For information on changing the IP address and FQDN of the managed elements, see the product documentation of the respective managed element.

**Changing the IP address and FQDN of managed element in System Manager**

**Procedure in System Manager**

If the identity certificates of the clients contain the IP address of the client computer, ensure that the certificates are reinitialized as per the changed IP address of the client computer. This prevents host name verification failure during communication between the client and the service.

If Managed Elements is registered with System Manager using an IP address, then:

1. Log in to System Manager as an administrator using the login **admin**.
2. On the dashboard, click **Elements** > **Inventory**.
3. In the left navigation pane, click **Manage Elements**.
4. On the Manage Elements page, select the registered element and click **Edit**.
5. Update the values for **Node** in the **Application** section and **Host** in the **Access Point** section.

**Procedure in Managed Elements**

Use the following procedure to make changes in the SAL Agent from the command line interface (CLI):

1. Change all occurrences of the old IP address of Managed Elements to the new IP address in the following file:

   **$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_supportedproducts_orig.xml**

2. Restart the SAL Agent using the following command:

   **# service spiritAgent restart**

**Changing FQDN of managed element in System Manager**

**Procedure in System Manager**

If the identity certificates of the clients contain the host name of the client computer, ensure that the certificates are reinitialized as per the changed host name of the client computer.

If Managed Elements is registered with System Manager using a host name, then:

1. Log in to System Manager as an administrator using the login **admin**.
2. On the dashboard, click **Elements** > **Inventory**.
3. Click **Manage Elements**.
4. On the Manage Elements page, select the registered element and click **Edit**.
5. Update the values for **Node** in the **Application** section and **Host** in the **Access Point** section.

**Procedure in Managed Elements**

Perform these steps to make changes in the SAL Agent from the CLI:

1. Edit all occurrences of the IP address of managed elements in the following file:

   **$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_supportedproducts_orig.xml**

2. Restart the SAL Agent using the following command:

```
# service spiritAgent restart
```

This section describes the changes you must make to the DRS Client. You can opt for any of the procedures provided here.

- Re-register the node in case of Session Manager:
    1. Stop the client service that hosts the DRS client application.
    2. Remove the client node from the DRS GUI.
    3. From the CLI, run the following script:

        ```
        # sh /opt/Avaya/bin/initTM
        ```

- Reconfigure the node in case of Presence Services:
    1. Stop the client service that hosts the DRS client application.
    2. Remove the client node from the DRS GUI.
    3. From the CLI, run the following script:

        ```
        # sh $DRS_HOME/bin/start_aggregation.sh
        ```

    4. From the CLI, run the following script:

        ```
        # sh $DRS_HOME/bin/get_initial_load.sh
        ```

    5. Start the client service that hosts the DRS client application.

**Note:**
Log in to the System Manager console and verify the functionality. If the system is unstable, use the Cold standby procedure to restore the system to the state prior to the change. For Cold standby procedures, see Appendix C.

# Appendix B: Changing the date and time configuration

You can change the date, time, and time zone of System Manager from System Platform Web Console.

**Prerequisites**

- Ensure that System Manager is installed on the system and accessible.

**Changing the time zone on the computer on which System Manager is running**

1. Go to System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Log in as an administrator using the login **admin**.
3. Click **Server Management**.
4. Click **Date/Time Configuration**.
5. Select a time zone from the list in the time zones section.
6. Click **Set Time Zone** and click **OK** to confirm the change. The system displays the following status message: `Processing your request, please wait….` Once the system completes the operation, the system displays the following status message: `Time zone has been changed to` *<new time zone>*.
7. After the operation, restart the JBoss service by performing the following steps:
    a. Log in to System Manager from the CLI.
    b. Use the **`service JBoss restart`** command to restart JBoss.
    c. Wait till the system displays the System Manager log-in page again.

**Changing the date or time on the computer on which System Manager is running**

1. Go to System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Log in as an administrator using the login **admin**.
3. Click **Server Management**.
4. Click **Date/Time Configuration**.
5. Ensure that the Network Time protocol daemon (ntpd) is not running.
6. Click the text box that contains the date and time information. The system displays a pop-up calendar.
7. Enter the new time value in the **Time input** field.
8. Select a date value in the calendar.
9. Click **Apply** to proceed with the changes.
10. Click **Save Date and Time** and click **OK** to confirm the change. The system restarts.
11. Wait for System Platform to redirect you to the log-in page - `Verifying changes in the date and time configuration`
12. Log in to the system running System Manager from the CLI.
13. Type **date** and press **Enter**. You can view the updated date, time, and time zone values.
14. After verifying the updated values, type **Exit** and press **Enter**.

# Appendix C: Cold standby procedure

**Introduction**

The System Manager server in the Cold standby mode acts as a failover when the main server on which System Manager is running fails. This section covers the Cold standby failover process for the System Manager application deployed on System Platform. The process is described with the example of two nodes: an Active node and a Cold standby node. Node A is the primary machine that is active. Node B is the Cold standby server. You must implement the Cold standby procedure in a scenario where Node A fails and the application must failover to Node B.

**Prerequisites**

Ensure that:

- Node A and Node B are installed on identical servers. The system supports the following servers: S8510 with 8 GB or 12 GB of RAM, S8800, next gen S8800, and HP Proliant DL360 G7.
- Node A (Active Node) and Node B (Cold standby Server) have the same IP address and host name. Ensure that when the Active Node is running, the Cold standby server is turned off.
- The System Manager 6.1 template is deployed on Node A and Node B. For the procedure to install the template, see Installing and Upgrading Avaya Aura® System Manager Release 6.1.
- The system date is identical on both the nodes.
- Regular backups of the System Manager database of Node A are available. To create these backups, use the Remote backup facility of System Manager Element Manager or create the backups from System Platform Web Console. The backups are necessary so that the latest snapshot of the System Manager database is available in case you need to implement the Cold standby procedure. Retain the backup of the database on a remote node or an external storage device, such as a CD-ROM or DVD. Use the backup to restore the database on Node B when Node A fails. For the procedure to schedule a backup on the System Manager Node, see Appendix D.
- When you implement the Avaya Aura® System Manager Cold standby procedure on a different computer, the system does not recognize the previously installed license file as the MAC address changes for the new computer. Use the following workaround or alternative remediation:

    1. The Avaya Business Partner or services technician must generate a new license file for products that are licensed using WebLM and were installed prior to performing Cold standby. Ensure that this new license file is generated from PLDS with the same count and the new MAC address.
    2. Copy the newly generated license file where System Manager is deployed.
    3. Obtain access to the System Manager command line interface (CLI).
    4. Stop the JBoss server using the following command:

       ```
       # service jboss stop
       ```

5. Delete the unwanted license file with the file extension in xml from the following location:
   **# $JBOSS_HOME/server/avmgmt/deploy/WebLM.ear/WebLM.war/licenses**
6. To confirm which license file to delete, open the license (.xml) file in a *vi* editor and look for the <Name> tag within the <Product> element. Verify that the name of the product is similar to the newly generated product name.
7. Once confirmed, delete this xml file using the following command:
   # **rm –rf**
   **JBOSS_HOME/server/avmgmt/deploy/WebLM.ear/WebLM.war/licenses/<file_name>**
   where *file_name* is the name of the license file that you must delete.
8. Once you delete the license file, start the JBoss server using the following command:
   **# service jboss start**
   **Note**: Wait for 5 to 10 minutes for the Jboss service to start.
9. Log in to the System Manager Console with the administrative user name and password.
   a. Click **UI Licenses** > **Install license**.
   b. Click **Browse** and select the newly generated license file.
   c. Click **Install**.

   **Note**:
   - On SYSTEM MANAGER 5.2, obtain access to Licenses from the System Manager Home page and click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
   - On SYSTEM MANAGER 6.0, obtain access to Licenses from the System Manager Home page and click **Licenses**.
   - On SYSTEM MANAGER 6.1, obtain access to Licenses from the System Manager Dashboard and click **Services** > **Licenses**.
10. Confirm that the system successfully installed the new license file.
11. Perform steps 1 to 10 for each product.

**Notes:**
For the procedure to perform a backup from System Platform Web Console, see "Backing up System Platform" in Administering Avaya Aura® System Manager 6.1.

**Cold standby procedure**

1. Confirm that Node A is shut down.
2. Turn on Node B.
3. Install all the System Manager patches on Node B that were installed on Node A before you took the last backup on Node A. For example, if you installed patch 1 and patch 2 on System Manager on Node A before the backup, then install patch 1 and patch 2 on Node B before you restore the backup. In case patch 3 is available and not installed on Node A when the backup was taken, install only patch 1 and patch 2 on Node B. Do not install patch 3.

4. Restore the last database backup that was taken from Node A on Node B. For the procedure to restore the backup on the System Manager node, see Appendix E. If the backup was taken from System Platform Web Console, see "Restoring System Platform" in Administering Avaya Aura® System Manager 6.1 to restore the backup from System Platform Web Console.
5. After restoring the database on Node B, you must run the **postColdStandBy.sh** script on Node B from the location @ **$MGMT_HOME/utils/bin/coldstandby/postColdStandBy.sh**

   **Note:**

   After restoring and running the **postColdStandBy.sh** script, System Manager on Node B is available for operations.

6. After restoring the database on Node B, run the following steps to retrieve the TM truststore password:
   a. **sh /home/ucmdeploy/quantum/queryDefaultCertInfo.sh**
   b. Restart **jboss**
7. Once the System Manager comes up, run repair on all replica nodes (Session Manager and Presence nodes) to make sure replicas have data consistent with the data restore on System Manager.
   a. Log in to System Manager as an administrator.
   b. Navigate to **Services > Replications** to open the replication page.
   c. Select all replica groups and click **Repair**. The repair time of all nodes depends on the number of nodes and the size of data populated in the System Manager database.

**CLI restore for Cold standby**

You can also implement the Cold standby procedure to restore the System Manager database using the CLI utility.

**CLI utility properties**

While performing a restore from the CLI, you might need to modify some of the restore properties related to the current setup. This file contains the properties related to the CLI restore:

**$MGMT_HOME/pem/fileRestoreCLIUtility/fileRestoreCLIUtility.properties**.

The following table lists the complete set of properties related to the CLI restore:

| No. | Property name | Description |
|---|---|---|
| 1. | version | The version of the current System Manager setup where you must perform the restore. You can determine the value from both the UI and the CLI.<br>To determine the version from the UI:<br>1. Log in to System Manager.<br>2. On the dashboard, click **Services** > **Configurations** > **Settings** > **SYSTEM MANAGER**.<br>On the **System Manager Properties** page, the value in **Build Version** is the System manager version.<br>To determine the version from the CLI, use the System Manager version string: **`$MGMT_HOME/installer_relno.txt`**. |
| 2. | db_type | The database type. The default is set to **`postgres`**. Do not modify the default setting. |
| 3. | db_directory | The location of the database utility installation. The default location is set to **`/usr/bin`**. Do not modify the default setting. |
| 4. | db_host | The IP or the host name of the database computer, in this case, the computer on which System Manager is running. The default is set to **`localhost`**. Do not modify the default setting. |
| 5. | db_port | The database server port. The default is set to **`5432`**. Do not modify the default setting. |
| 6. | db_name | The database name that must be connected for a restore. The default is set to `avmgmt`. Do not modify the default setting. |
| 7. | db_scpport | The SSH port to connect the database machine. The default is set to `22`**.** Do not modify the default setting unless you modify the configuration for the SSH port. |
| 8. | backup_destination | The full path of the directory to be used as a temporary directory for extracting and processing the backup archives. The default is set to **`/var/lib/pgsql/backup`**. Do not modify the default setting. |
| 9. | backup_name | The full path to the backup archive, including the archive name. For example, if the archive name is **backup.zip** and the path where the archive is present in the directory: **`/var/lib/pgsql/backup/manual/`**<br>the value of the backup_name property must be **`/var/lib/pgsql/backup/manual/backup.zip`**. |
| 10. | scp | The location of the backup archive. Specifies whether the backup archive is stored on the local computer on which System Manager is running or a remote computer. The value `false` means the archive is on a local computer on which System Manager is running, and the value **`true`** means the archive is on a remote computer. The default is set to **`false`**. |
| 11 | scp_ip | The IP or the host name of the remote server with the backup archive. Use this property when the value of scp is set to **`true`**. |
| 12 | scp_port | The ssh port used to connect to a remote server with a backup archive. The default is set to `22`. Use this property when the value of scp is set to **`true`**. |
| 13 | user | The user performing the restore operation. You can specify any user name. |

| No. | Property name | Description |
|---|---|---|
| 14 | remote_utility_directory | The full path to the directory that has the System Manager utilities required for the restore. The default is set to **/var/lib/pgsql**. Do not modify the default setting. |

**CLI restore utility procedure**

1. Log in to the system on which System Manager is running as a **root** user. If direct access to the system using the user **root** is disabled, then log in as a **nonroot** user using direct access to the system. Then escalate access privilege restrictions by issuing the **su** command at the server command line interface.
2. Update the **$MGMT_HOME/pem/fileRestoreCLIUtility/fileRestoreCLIUtility.properties** file with the required details. If the backup archive is present on the local system on which System Manager is running and the default values related to the restore are not modified, update the following properties:
   - version
   - backup_name
   - scp (set to false)
   - user

   If the backup is on a remote system and the default values related to the restore are not modified, update the following properties:
   - version
   - backup_name
   - scp (set to true)
   - scp_ip
   - scp_port
   - user
3. Run the following command to move the CLI Restore Utility from the current directory: **$MGMT_HOME/pem/fileRestoreCLIUtility** to the directory that contains the CLI scripts:

   **cd $MGMT_HOME/pem/fileRestoreCLIUtility**
4. Run the following command from the current directory:

   **./file_restore.sh $MGMT_HOME/pem/fileRestoreCLIUtility 1**
5. At the system prompt, enter the full path of the backup archive. If the value is not specified in the **RestoreCLIUtility.properties** file, as mentioned in Step 2, then specify the full path to the backup archive. If the value is already specified in the **RestoreCLIUtility.properties** file, then do not specify any value. Press **Enter**.

6. To perform the restore with the backup archive present on a remote computer with scp set to `true`, at the system prompt, enter the scp user name. Specify the user name for performing Secure Shell (SSH) on the remote computer and obtain permission to gain access to the backup archive. Press **Enter**.
7. To perform the restore with the backup archive present on a remote computer with scp set to `true`, at the system prompt, enter the password for the scp user. Specify the password of the scp user mentioned in Step 6, and press **Enter**.
8. The system prompts you to enter the database super user name. Specify **postgres** as the value and press **Enter**.
9. At the system prompt, enter the password for the database super user. Specify the password of database super user **postgres** and press **Enter**.
10. At the system prompt, enter a choice for overwriting the current database with the one present in the backup archive. Type **y** and press **Enter**.
11. At the system prompt, enter the database application user name. Specify **postgres** as the value and press **Enter**.
12. At the system prompt, enter the password for the database application user. Specify the password of the database application user **postgres** and press **Enter**.

# Appendix D: Scheduling a data backup from System Manager Web Console

1. Log in to the System Manager Web interface as an administrator.
2. On the dashboard, click **Services** > **Backup and Restore**.
3. Click **Backup**.
4. On the **Backup** page, perform one of the following tasks:
   - To schedule a local backup:
     a. Click **Local**.
     b. In the **File Name** field, enter the name of the backup file that you want to create.
   - To schedule a remote backup:
     a. Click **Remote**.
     b. Specify the SCP Server IP, SCP Server port, user name, password, and file name in the respective fields.
5. Click **Schedule**.
6. On the **Schedule Backup** page, complete the following fields: **Job Name**, **Task Time**, **Recurrence**, and **Range**.
7. Click **Commit**.

# Appendix E: Restoring a backup from System Manager Web Console

1. Log in to the System Manager Web interface as an administrator.
2. On the dashboard, click **Services** > **Backup and Restore**.
3. Click **Restore**.
4. On the **Restore** page, perform one of the following steps:
    - To restore data from a local backup:
        a. Click **Local**.
        b. Enter the backup file name in the **File Name** field.
    - To restore data from a remote backup:
        a. Click **Remote**.
        b. Specify the SCP Server IP, SCP Server port, user name, password, and file name in the respective fields.
        c. Click **Restore**.
5. Click **Continue** on the Restore confirmation page.

**Note:**

Ensure that the backup and restore is performed on the same System Manager Patch (same Build Number and Software Update Revision Number). Click the **About** link to view information on the System Manager patch.

The system displays the patch information:

**System Manager 6.1.0 (Build No. - 6.1.0.0.7345-6.1.5.606) Software Update Revision No: 6.1.10.1.1774**

# Appendix F: System Manager HA mechanism

**Introduction**

System Manager uses the failover mechanism provided by System Platform.

System Platform High Availability (HA) implements the Active and Standby mode of failover. The resources, which are virtual machines (VMs), run only on one node. The system continuously mirrors all disk data from the active mode to the standby mode. In case of failure of the active node, the system automatically starts the resources, that is, the system boots the VMs on the standby node.

System Platform HA uses VMs running on active cluster nodes only. This configuration is also known as the Active/Standby mode. All block devices that are part of the DRBD synchronization propagate all changes from the active node to the standby node. Avaya uses a reliable protocol called C - synchronized replication to ensure that the system commits and acknowledges all block changes on the secondary node before continuing. The system immediately replicates all changes that occur on the active node to the secondary node.

The system performs the following actions in the failover scenario:

- Uses heartbeat to detect problems on the active (primary) node by missing heartbeat checks for a defined period of time.
- Assigns the secondary node as a new primary node.
- Sets the DRBD devices as a primary node on a new active node.
- Boots the VMs on the new active node.

The system performs the following actions in the manual switchover scenario:

- Shuts down the VMs on the active node.
- Sets the DRBD devices as the secondary node on the active node.
- Assigns the secondary node as a new primary node and vice versa.
- Sets the DRBD devices as the primary node on a new active node.

The system boots the VMs on a new active node.

**Prerequisites**

System Platform uses the simplest HA scenario:

- Uses two equal nodes with one public network interface card (NIC) and one HA-dedicated NIC, which is used for HA pings and DRBD propagation between the two nodes.

- Uses both NICs as ping paths between cluster nodes and uses the network switch (gateway IP address) as a public ping point. As a result, each node has three ping points. Heartbeat detects the node with more communication paths available and migrates resources into this node.
- Uses the default port for the ping (port 694).
- Uses the Active/Standby configuration, where all resources run on only one node and all resources are migrated.
- Maintains the same IP address for all VMs, for example, CDom and System Manager on the active and standby nodes.
- Uses heartbeat to start the DRBD service on both the nodes.
- For each VM on the selected cluster node, heartbeat starts the DRBD resources of all VMs and then heartbeat starts the VM itself.

The system uses a Domain 0 LVM to synchronize data by DRBD between the cluster nodes. For this resource, the system defines the mounting procedure on an active node.

**Performing System Platform-based HA**

1. Install System Platform on two computers.
2. Install the System Manager template on one of the computers. Name this computer **preferred**.
3. Connect the computers with a crossover cable on ports eth2. You must do this before you configure HA Failover.
4. Perform all the required checks on the standby node from the Web console. You must do this before you configure HA Failover. The Standby Web console is not accessible after you configure HA Failover.
5. Configure System Platform HA Failover from the preferred node Web console.
6. Ensure that you can contact the DNS servers from both the servers. You must do this before you configure HA Failover. If DNS is configured but DNS servers are not accessible, SSH communication can be delayed. The delay can cause the HA Failover configuration to fail.
7. Ensure that you can contact either NTP server from both the servers or that you can disable NTP on both the servers. You must do this before you configure HA Failover. If NTP is configured but the NTP servers are not accessible, SSH communication can be delayed. The delay can cause the HA Failover configuration to fail.
8. If the System Platform HA Failover is configured, you can start the HA Failover from the preferred node Web console Failover Web page. The system redirects the Web console to restart the Web page for about 5 minutes. Then the system redirects you to the log-in page, and you can log in again.

**Must read while performing System Platform-based HA**

- Install the template on the standby node.
- You cannot install the template on a system with a running HA Failover.
- You cannot make network configuration changes on a system with a running HA Failover.

# Appendix G: Resetting the admin user password

To reset the System Manager Web Console admin user password:

1. Log in to the System Manager command line interface (CLI) as a **root** user. If direct CLI access is not enabled for the **root** user then log in as **admin** with direct access to CLI and then escalate access privileges restrictions by issuing the **su** command at the server CLI.

2. Run the following command to create a **securityadmin** group:
   **`groupadd -g 600 securityadmin`**

   - If the system displays the error message `groupadd: GID 600 is not unique`, then use a higher value instead of 600 and run the same command.
   - If the system displays the error message `groupadd: group securityadmin exists`, then the group is already present and you do not have to create the group again.

3. Run the groups **admin** command to verify whether the user **admin** has the **securityadmin** group assigned to the user. This might happen if the group **securityadmin** was already present and assigned to user **admin**.
   The output of the command must not mention `securityadmin` in the list of groups assigned to user admin.

4. If the output of Step 3 mentions that group **securityadmin** is not assigned to user **admin**, run the following command to assign the group to the user:

   **`usermod -aG securityadmin admin`**

5. Gain access to the System Manager local log-in screen at https://<IP Address/Fully Qualified Hostname>/local-login.

6. Use the log-in credentials of the System Manager CLI user **admin** to log in. After the system displays the **Security Configuration** screen, change the URL to:

   https://< System Manager IP Address/Fully Qualified Hostname>/passwordReset

7. After the system displays the **Password Reset** screen, specify the user ID as **admin** and the new password as **admin123**.

8. After the system displays the message `Password changed successfully`, close the current browser session and gain access to the System Manager log-in screen in a new browser session at:

   https ://< System Manager IP Address/Fully Qualified Hostname>/SYSTEM MANAGER

   If you gain access to System Manager using
   - A fully qualified host name:
     a. Log in using the password specified in Step 7, **admin123**.
     b. At the system prompt, specify the new password.

   - An IP address:
     a. Click the **Change Password** link on the log-in page, and change the password.

b. Open the System Manager log-in screen again, and log in using the new password.

9. If the group `securityadmin` was assigned to user **admin** in Step 4, then perform the following steps to unassign the group **securityadmin** from user **admin**:
   a. Run the following command on System Manager CLI as a root user to list the groups assigned to user admin:
      **`groups admin`**

      Assume the output is:
      **`admin: admin xxx securityadmin xyz`**

   b. Run the following command to unassign the group **securityadmin** from user **admin**:

      **`usermod -G <list of comma separated groups except securityadmin> admin`**

      As per the example, the command should be:

      **`usermod -G admin,abc,xyz admin`**

10. If you created the group **securityadmin** in Step 2, then run the following command to delete the group:
    **`groupdel securityadmin`**