



Avaya Aura® System Manager 6.1

SP- 1.1 Release Notes

March, 2011

Version -2

Last Updated – Sept 23 rd 2011

Table of Contents

Introduction	4
Product Support Notice	4
Enhancement	4
System Manager Installation Checklist	5
Supported upgrades	5
Points to be noted during fresh installation or an upgrade	6
Issues resolved	8
Known Issues	10
Technical Support	14
Contact support tasks	14
Appendix A — Procedure to change IP address or Host name	15
Prerequisites	15
Changing IP address for System Manager	15
Changing System Manager IP reference in Managed Elements	16
Changing the host name for System Manager	17
Changing the System Manager Host name reference in Managed Elements	17
Impact of changing IP Address of Managed Elements	18
Procedure to followed on System Manager	19
Step 1	19
Step 2	19
Procedure to be followed on Managed Elements	19
Impact of changing the host name of Managed Elements	19
Procedure to be followed on System Manager	20
Step 1	20
Step 2	20
Step 1	20
Appendix B — Procedure to change the date and time configuration	21
Prerequisite	21
Changing the time zone on the computer running System Manager	21
Changing the date or time on the computer running System Manager	22
Verifying changes to the date and time configuration	22
Appendix C — Cold standby procedure	22
Introduction	22
Prerequisites	23
Cold standby procedure	23

CLI restore for Cold Standby	24
CLI Utility properties	24
CLI Restore Utility procedure	25
Appendix D — Scheduling a data backup	27
Appendix E — Restoring a backup from System Manager Web console	27
Appendix F — System Platform HA Mechanism	28
Introduction	28
Prerequisites	29
Performing System Platform-based HA	29
Don'ts	30
Appendix G — Steps for resetting Admin user Password	30

Introduction

This document provides late-breaking information to supplement Avaya Aura® System Manager 6.1 SP1.1 software and documentation. The Appendix section describes how to schedule a data backup and restore a backup script for System Manager. Documentation for installation and upgrade of System Manager 6.1 is available on the Avaya Support Center Web site <http://www.avaya.com/support>

System Manager 6.1 SP1.1 is delivered in the form of a template that gets deployed as a virtual appliance on Avaya Aura® System Platform 6.0.3.0.3

Product Support Notice

Some product changes that are implemented after the product release are documented as Product Support Notice (PSN) in the online Avaya Support Web site. The PSN number defines the relevant document and is appended to the particular document listed in the Title column.

To read the PSN description online:

1. Go to the Avaya Support Web site at <http://www.avaya.com/support>.
2. Click **Products**. A pop-up window appears. Enter the name of the product in the window, in this case **Avaya Aura® System Manager**. You can even select the product from the A-Z list in the bottom right corner of the pop-up window.
4. On the Products page, click **Product Notices > Product Support Notices**.
5. On the **Product Support Notices** page, the pdf document is listed with the PSN number in the table under Title.
6. Click on the PSN title link to open the PSN.

Enhancement

This release includes the following enhancements delivered in Avaya Aura® System Manager Release 6.1 SP-1.1

#	Enhancements
1	Support for sending INADS formatted v2c traps to SAL GW and NMS

System Manager Installation Checklist

#	Action	Notes
1	Download the System Platform 6.0.3.0.3 SP3 ISO image and applicable patch from the Avaya PLDS Web site.	Verify that the md5sum for the downloaded ISO image matches the number on the Avaya Product Licensing and Delivery System (PLDS) Web site.
2	Download the System Manager template from the System_Manager_06_01_SP1-1_b33.iso file from the Avaya PLDS Web site.	Verify that the md5sum for the downloaded template matches the number on the Avaya PLDS Web site.
3	Set up a DVD or USB flash drive to install System Platform from a DVD or USB flash drive.	For more information on installing System Platform, see Chapter 3, "Installing System Platform".
4	Deploy the System Manager template on System Platform. For more information, see <i>Chapter 5, Installing System Manager template</i> .	Refer <i>Installing and Upgrading Avaya Aura System Manager</i> document from http://support.avaya.com

Supported upgrades

System Manager 6.1 SP 1.1 supports the following upgrades

Note: *If you are upgrading from SMGR 6.0 or earlier, you MUST first upgrade to SMGR 6.0 SP1 before upgrading to SMGR 6.1 SP 1.1*

- Upgrade from SMGR 6.1 Release
 - System Manager 6.1 with SP 0 to SMGR 6.1 SP1.1
- Upgrade from SMGR 6.0 Release
 - Upgrade SMGR 6.0 to SMGR 6.0 SP 1 + integrated patches to SMGR 6.0 SP2 before upgrading to SMGR 6.1 SP1.1
- Upgrade from SMGR 5.2 Release
 - Upgrade SMGR 5.2 to SMGR 5.2 SP1 to SMGR 5.2 SP2
 - Then upgrade to SMGR 5.2 SP2 to SMGR 6.0 to SMGR 6.0 SP1 to SMGR 6.0 SP2 before upgrading to SMGR 6.1 SP1.1
- SMGR 1.0 SP3 (SP3) through SMGR 5.2 SP1 and SMGR 5.2 SP2
 - This is a multistep upgrade, first from SMGR 1.0 SP3 to SMGR 5.2 SP1 and then to SMGR 6.0 SP1

Note: Releases earlier than SMGR 1.0 SP3 must first upgrade to SMGR 1.0 SP3.

Points to be noted during fresh installation or an upgrade

- If you installed or upgraded to **SMGR 6.1 SP1** and while accessing "Administrators" link in Dashboard throws an error due to single sign-on setting after fresh installation or an upgrade, then it is a cause of Installation error. The only option is to reinstall with SMGR 6.1 SP1.1 and it is recommended to contact Avaya Support Web site at: <http://www.avaya.com/support>
- If you already installed fresh or upgraded to **SMGR 6.1 SP1** and a consistent backup failure is observed, then login to System Manager Console via SSH and run following command
\$sh /home/ucmdeploy/quantum/quantumBackupRestore/backup.sh

If it fails with following error, then it is CND lock issue

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

Then it is recommended to contact Avaya Support Web site at: <http://www.avaya.com/support>
- If you are deploying Avaya Aura® System Manager 6.1 SP -1.1 using CD then ensure following tags before proceeding the deployment
 - o Version :- **6.1.1.5.7345a**
 - o Release :- **March 2011**
- You must deploy Avaya Aura® System Manager 6.1 SP -1.1 as a virtual appliance on Avaya Aura® System Platform Release 6.0 SP3. If System Platform upgrade is required then it is recommended to first upgrade System Platform before upgrading System Manager
- While installing or upgrading System Manager 6.1 with input parameter which contains the following values as substring then the installation will not be successful.
e.g:- smgr.ip, smgr.hostname, smgr.gateway, smgr.domain, smgr.netmask, smgr.dns, smgr.searchstring, nonroot.user, loginDomain
- System Manager local-login page comes up instead of normal login page if System Manager 6.1 Service Pack 1.1 installed without Top-Level Domain in Fully Qualified Domain Name

- After successful installation of SMGR 6.1 SP1.1, you can confirm the release version of installed System Manager by clicking on “About” Link or by running “swversion” through CLI. The version should display as: **System Manager 6.1.0 (Build No. - 6.1.0.0.7345-6.1.5.9)**
- While accessing SMGR 6.1 SP1.1, Avaya recommends that you use the fully qualified domain name (FQDN) instead of the IP Address.
- For Avaya Unified Communication Management to authenticate the user *admin*, the user *admin* must enter the password *admin123*.
 - If SMGR 6.1 SP 1.1 is upgraded from SMGR 6.1 , the password of user *admin* will remain same as prior to upgrade
- To change the password for the user *admin*, you need to navigate through **Dashboard >> Administrators >> Users**. This opens the Avaya Unified Communication Management page. Click on **Password** under **User Services** to change the password for the user *admin*.
- To check the password policy and aging for the user *admin*, you need to navigate through **Dashboard >> Administrators >> Users**. This opens the Avaya Unified Communication Management page. Click on **Policies** under **Security** to check the password policy and aging.
- If you are upgrading directly to **SMGR 6.1 SP1.1** from an earlier release, and if you have configured the setup of the prior release for external authentication, such as LDAP and RADIUS, prior to the upgrade, you need to redo that configuration manually once the upgrade is complete. To reconfigure you need to go to **Dashboard >> Administrators >> Users**. This display the Avaya Unified Communication Management page. Click on **User Services >> External Authentication** to modify external identity repositories.
- If you want to upgrade directly to SMGR 6.1 SP1.1 from an earlier release, and if you have performed any configuration for the legal notice, you need to redo that configuration manually when the upgrade is complete. To reconfigure you need to navigate through **Administrators** under **Users** from the **Dashboard**. This displays the Avaya Unified Communication Management page. Navigate to **Security >> Policies** and click the Edit button to modify the login warning banner under the **Security Setting** section.
- While running of bulk export utility for bulk export of roles and users the utilities does not require specifying username/password.

- Avaya Aura® System Manager 6.1.1 has been integrated with Unified Communications Management (UCM) 7.5. After you install the System Manager template in which the two applications are co reside, you can log into 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 Fundamentals (version 7.5) at <http://www.support.avaya.com>
- In System Manager, there are two ports enabled for communication over HTTPS:
 - Port 443: Used to communicate with System Manager services over HTTPS and is secured by System Manager based certificates.
 - Port 52233: Used by legacy WebLM clients to communicate with System Manager based WebLM server over HTTPS and was (until SMGR R6.1 release) secured by self-signed certificates used by legacy/standalone WebLM releases.

The self-signed certificates used to secure port 52233 in System Manager got expired on 1st March 2011. Hence, with SMGR R6.1 SP1.1 release, these certificates have been replaced by SIP CA signed certificates. Because of new certificates being used to secure port 52233 in SMGR R6.1 SP1.1, there is an impact on the adopters of WebLM who fulfill the following criteria have been 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 the mentioned criteria, the WebLM client-server communication breaks if a legacy WebLM Java based client communicates with SMGR R6.1 SP1.1 WebLM server over port 52233. This is because the Java based WebLM clients do not have the new SIP CA signed certificate added to their truststore.

Workaround: Delete the truststore file (default name: trusted_weblm_certs.jks) available with the WebLM Java client and re-initiate the connection with the WebLM server. During the first handshake between the WebLM client and the server, a new truststore file will be created containing the correct certificates based on the HTTPS port number used to communicate with SMGR WebLM server.

Issues resolved

This SMGR 6.1 sp1.1 release includes the following resolved issues

WI Item No	Description
wi00599869	Authentication (OpenSSO) logs are not visible in the Logging UI of SMGR R6.1.

- wi00653791 There is no warning message to Admin that if SSL is provisioned with the wrong port, the result will be an unsecured connection.
- wi00599603 The Session Timeout pop-up notification does not appear on SMGR
- wi00704446 If you change the Admin password through the forced change password feature or through the UPM change password link, then Bulk export utilities does not accept the changed password.
- Note** – The issue has been fixed. Now it is not required now to specify username and password during running of user and role bulk export using CLI interface
- wi00830983 A user that has a SIP type handle configured along with Endpoint Voicemail for a default communication profile, then clicking the radio button for the non-default communication profiles doesn't load the respective communication profiles
- wi00816963 In earlier releases, the session timeout value was specified under the Common Console settings. From Release 6.1, this configuration can be controlled from the **Home > Users > Administrators > Security > Policies** screen:
Session Properties > Maximum Session Time: Maximum session time even if the session is not idle.
Properties > Maximum Idle Time: Maximum session time when the session is idle.
- Common Console settings may still display a property for configuring session timeout but the property is not used and will be removed.
- Note:** When you upgrade to SMGR 6.1, the session timeout property is not retained. In this case, the user has to perform the modification again on the suggested screen.
- wi00731363 If the system is upgraded from Release 6.1 Beta, the restore does not work from the UI while performing the Cold Standby setup.
- wi00827245 If System Manager is upgraded from a prior release for SMGR 6.1 SP1.1, DRS performance setting is lost.
- wi00829090 If the default system-provisioned and scheduled jobs, such as CldAlarmPurgeRule, LogPurgeRule, SoftDelRTSPurgeRule, and PurgeJobStatus, are modified to run more frequently, then the system may become unstable.
- wi00831644 The set type field of User under the Endpoint profile of **Home > Users > User Management** is not enabled to support voicemail on Communication Manager
- wi00832473 User cannot edit the endpoint with the XMOBILE set type where the port number is not required.
- wi00835782 If you changes the hostname of System Manager from the System Platform webconsole, with the old short hostname being a part of the new short hostname, the hostname change is not effective
- wi00554555 You face the System Manager User Interface (UI) layout issue when accessing the old System Manager system (Beta or Alpha) and later upgraded to System Manager GA

wi00832144	If there are more than 50 signaling groups added on Communication Manager, then IPTCM fetches only the first 50 signaling group. If any signaling group above the first 50 (of the type SIP or H323) is also added to trunk group of the type SIP, then the Communication Manager initialization synchronization also fails.
wi00828046	A Majority of vulnerability issues have been addressed in SMGR 6.1 Service Pack-1.1 • Kernel security and bug fix updates
wi00733654	While configuring Localized Name on Subscriber page, the page gets refreshed after clicking the Edit button, so you can not add a subscriber with Localized Name.
wi00816869	If you logged in through etoken the user session does not destroy from browser after logoff
wi00844175	User does not get assigned permission when authenticated by external Active Directory server.
wi00842991	Communication Manager synchronization fails if there was a soft deleted user with Communication Manager communication profile associated with it
wi00839692	Delete endpoint failed if the error message returned by Communication Manager was about extension is used as remote extension in UDP
wi00847445	Communication Manager Incremental synchronization fails if Intra Switch CDR is deleted from Communication Manager
wi00856368/ wi00820300	If consistent backup failure is observed then it may be due to the backup lock not released in one of earlier backup
wi00855913	While accessing the "Administrators" link in Dashboard, throws permission error due to single sign-on setting after fresh installation or an upgrade from earlier System Manager release to SMGR 6.1 SP1.
wi00848428	When Synchronizing a SubMgr Presence password with UPM, synchronization fails if there is more than one communication address in the communication profile
wi00837892/ wi00845252	Subscriber Manager logs are not getting forwarded to SMGR log viewer

Known Issues

The following known issues are in SMGR 6.1 SP-1.1

WI No.	Description	Workaround
wi00408521/ wi00653838	After deleting and adding an entity for certain sections, the system does not allow committing of the user. This is observed in the following sections: • Communication Profile > Communication Address • Contacts > Associated contacts • Contacts > Private contacts	No workaround.

wi00555545	In SMGR R6.1 and prior releases, an administrator who logged in on the System Manager console could view the time stamp of the last login in the top-right corner of the screen. This feature is not available in SMGR R 6.1	To check the time stamp of the last logged in information, you need to navigate from Home >> Users >> Administrator This opens the Avaya Unified Communication Management page. Click Logs under Tools to check the time stamp of the information that was last logged in.
wi00730231	SMGR 6.1 as well as Service Pack-1.1 does not support authentication with SAML, though it was supported in SMGR 6.0 and prior releases.	No workaround.
wi00729531	When two bulk jobs (bulk import with communication profile and endpoint bulk adds) are scheduled for the same Communication Manager, one of the jobs shows the RUNNING state in the Scheduler page even though it has actually failed.	Schedule only one bulk job per Communication Manager at a time.
wi00376209	Bulk Import of Users adds a new user if someone tries to re-import an existing user through UPM bulk import after changing the log-in name.	No workaround.
wi00844175	User does not get assigned permission when authenticated by external Active Directory server.	
wi00730565	If System Manager is upgraded from prior release to 6.1 or SP1, porting of IAM data related to external authentication servers like LDAP / Radius are not retained.	Re-enter all IAM configuration data after upgrading from any earlier release of System Manager to System Manager 6.1 or SP 1.1

Wi00822483	In Online help following attributes to be added while specifying the time zone format in the bulk User Import xml file. Daylight saving time (DST): You need to consider summer time adjustments while using the suggested possible values for the Timezone. Typically, you will need to adjust the offset — you will need add 1 hour to the offset. Using character entities: You need use the following five character entities appearing on the left side as specified on the right side in the import XML files: The less-than character (<) : &lt; The ampersand character (&) : &amp; The greater-than character (>): &gt; The double-quote character ("): &quot; The apostrophe or single-quote character (') : &apos;.	No workaround.
wi00829034	The original documentation does not include the additional <i>copyright notices, author names, owner names, and terms and conditions of use as received in the code</i>	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 redistributions of the source code and the binary forms, retain this copyright notice: Copyright (c) 2000 The Apache Software Foundation. All rights reserved. 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/). Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation. A copy of the license must be included with the product distribution. In addition, include the original and modified open source code in a source code repository; and track all modifications to the open source code in the source code repository.

wi00817241	While performing backup using IE browser, the system displays following message: Internet Explorer cannot display the webpage. This issue is observed in the following scenarios: When the time taken for the backup is more than 30 seconds	1. Start Registry Editor on the computer running Windows. To do this, click Start > Run, type Regedit, and press OK. 2. Locate the following subkey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings 3. Perform one of the following: • If this subkey already exists, change the decimal value to 3600000. • If this subkey does not exist, then add a Receive Timeout DWORD entry that has the decimal value equal to 3600000. 4. Restart the computer. Please refer Microsoft support site for further help http://support.microsoft.com/kb/181050.
wi00691693	The Status column of the landing page of users under User Management > Manage Users does not indicate whether a user is logged in.	The Active Sessions page can be viewed under the Administrators > Security > Active Sessions page.
wi00601030	When the user clicks the Log off button then sometimes, instead of redirecting to the login page, System Manager shows the following error message: viewID:/pages/Welcome.xhtml - view /pages/Welcome.xhtml could not be restored	The user can gain access to the login page by using the URL <code>https://<IP/FQDN>/SMGR</code>
wi00826443	When trying to export a trusted certificate, the generated trust-cert.pem file can not be imported or opened with openssl due to encrypted part of the file is one big line instead of multiple lines.	No workaround. This issue is addressed in 6.1 Service Pack-2
wi00674981	Proper error message is not handled for UPM bulk import while performing some validation.	No workaround. This issue is addressed in 6.1 Service Pack-2
wi00853372	Partial + replace import not working for comm profile handles	No workaround. This issue is addressed in 6.1 Service Pack-2
wi00857723	DRS invalidate a node that cannot be reached for a maximum period of 12 hours and marks it in 'Ready For Repair' state. When a node gets invalidated, any pending events and unsent batches of the node are removed and the node MUST be repaired when it comes up.	The only way to recover from this situation is by repairing the node from the DRS GUI when the node comes up.

Technical Support

Support for System Manager is available through Avaya Technical Support.

If you have trouble with System Manager, you should:

1. Retry the action. Carefully follow the instructions in the printed or online documentation.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Refer to the Avaya documentation. If the document has a troubleshooting section, refer to this section.

If you continue to have the problem, 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 at one of the telephone numbers in the Support Directory listings on the Avaya Support Web site.

If you have difficulty reaching Avaya Support using the above URL or e-mail addresses, go to <http://www.avaya.com> for further information. Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Web site.

When contacting Avaya Support, be ready to provide the following information:

- Problem description
- Detailed steps to reproduce the problem, if any
- The release version in which the issue occurs
- If System Manager is an upgrade system, then the details of prior release(s)
- Installation log files
- System Manager JBoss server log file available at
\$JBoss_HOME/server/avmgt/log/server.log
- The domain log available under \$AVAYA_LOG

Contact support tasks

You may be asked to e-mail one or more files to Avaya Support for analysis of your application and its environment.

For information about patches and product updates, see the Avaya Support Web site at:

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

Appendix A — Procedure to change IP address or Host name

After you deploy System Manager, you can change the IP address or host name of the machine running System Manager from the System Platform Web console. See below for the prerequisites and steps to change the IP address or host name of System Manager.

Prerequisites

- System Manager is installed on a system and is accessible. You can check this by accessing the System Manager Administration user interface (UI).
- Perform the following steps to verify that all extension packs are successfully deployed:
 1. Log in to System Manager as an admin user.
 2. Navigate to **Home > Services > Configurations** and click the **Extension Packs** link.
 3. Check the status of all extension pack data. The data should be in the Confirmed state.
- After installing System Manager, if you made changes to any configuration settings through the System Manager UI **Home > Services > Configurations > Settings**, make these changes again after changing the IP address or host name. Keep note of such changes.
- Run a manual backup by using remote backup facility of System Manager Element manager and ensure that data is backed up successfully. For more information, see the Online Help.

Note:

Avaya recommends that you copy the backup to a remote computer or to an external storage device, such as tape drive and DVD.

Changing IP address for System Manager

Step 1

1. Go to the System Platform Web console at <https://<C-dom IPAddress>/webconsole>.
2. Log in with admin credentials, that is, log in as the admin user.
3. Click **Server Management.> Network Configuration**.
4. In Network Configuration, go to the **Template Network Configuration** section.
5. Modify the following fields in the section with their respective new values:
 - Change IP address to “System Manager IP Address”
 - Change Netmask under Domain Network Interface for Bridge avpublic
 - Changing server to a different subnet that requires a new default gateway address, change Default Gateway under General Network Settings section

6. Click **Save**. The system displays the following confirmation message that “Changing network setting may require you to login again into webconsole. Are you sure?”
7. Once you confirm a status message: Processing your request, please wait... Once the processing and the network change are complete, the system displays the following status message: Settings updated successfully.
8. Wait for about 15 minutes for the network change to complete, and then verify that the System Manager Webconsole is accessible.

Step 2

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

1. Go to the 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**. This opens another window.
5. Log in using your **admin** privileges.
6. Click **Managed Element**.
7. Click **Host Name** on the **System Manager entry from the** list. The Managed Element Configuration page is displayed.
8. Click **Edit** and modify the **IP Address** to the new IP Address.

Changing System Manager IP reference in Managed Elements

Once the IP Address of the System Manager is changed, perform the following procedure for changing the IP Address of Managed Elements:

1. If the Managed Elements are using JNDI lookup to communicate with System Manager, there is a need to point Manage Elements to the new System Manager IP Address.
2. Due to the change in the IP Address of System Manager, License Management will be affected in the following ways:
 - The adopting product application must re-create the License Manager object with the new IP Address.

- After re-creating the object, all the license acquisitions must be done again.

Changing the host name for System Manager

Step 1

1. Go to the System Platform Web console at <https://<C-dom IPAddress>/webconsole>.
2. Log in with admin credentials, that is, log in as the admin user.
3. Click **Server Management**.
4. Click **Network Configuration**.
5. In Network Configuration, go to the **Template Network Configuration** section.
6. Modify the following field in the section with the new value:
Change the Host Name marked as “Hostname: System Manager Fully Qualified Host Name”
7. Click **Save**. The system displays the following confirmation message that “Changing network setting may require you to login again into webconsole. Are you sure?”
8. Once you confirm a status message: Processing your request, please wait... Once the processing and the network change are complete, the system displays the following status message: Settings updated successfully.
9. Wait for about 15 minutes for the network change to complete, and then verify that the System Manager Webconsole is accessible

Step 2

If the SAL Gateway has been configured to receive SNMP traps from System Manager, then from the

System Platform Administration UI, perform the following tasks:

1. Go to the System Platform Web console at <https://<C-dom IPAddress>/webconsole>.
2. Click **Server Management**.
3. Click **SAL Gateway Management**.
4. Click the **Launch SAL Gateway Management Portal** button. A new window opens.
5. Login using **admin** privileges.
6. Click **Managed Element**.
7. Click **Host Name** on the **System Manager entry** from the list. The system displays the Managed Element Configuration page.
8. Click **Edit** and modify the **Host name** field to the new host name.

Changing the System Manager Host name reference in Managed Elements

Use the procedure stated below to change the host name for the Managed Elements for System Manager Clients. This change is necessitated by the change in the host name of the Managed Elements.

Step -1

1. If the Managed Elements are using JNDI lookup to communicate with System Manager, there is a need to point Manage Elements to the new System Manager Host Name.

Step -2

Follow the below steps to make changes in SAL Agent from command-line interface

1. Edit the host name of the Managed Element to the new host name in the following file:
 - a. \$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_DataTransportConfig_orig.xml
 - b. \$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_BaseAgentConfig_orig.xml
 - c. \$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_SpiritComponentConfig_orig.xml

Note - Where **\$SPIRIT_HOME** is the base location of the SAL agent deployment on the managed element.

2. Restart SAL Agent using the following command:

service spiritAgent restart

Step - 3

There will be an impact on License Management with the change in Host Name

- a. The adopting product application must re-create the License Manager object with the new IP Address.
- b. After re-creating the object, all the license acquisitions will have to be done again.

Step – 4

There will be an impact on Data Replication Service (DRS) Client Application. Follow steps to make changes in Data Replication Service Client Application.

- a. Edit all occurrence of new System Manager host name in following files
 - \$SYM_HOME/WEB-INF/classes/symmetric.properties
 - \$DRS_HOME/conf/drsClientInstall.properties
- b. Restart Data Replication Service Client

Impact of changing IP Address of Managed Elements

This section describes the changes required on System Manager if the IP Address of the Managed Elements changes.

Note:

For the procedure to change the IP Address and host name of the Managed Elements, refer the product documentation of Managed Elements.

Procedure to followed on System Manager

Step 1

If the identity certificates of the clients contain the IP Address of the client computer, the client must ensure that those certificates are reinitialized as per the changed IP Address of the client computer. This is required to avoid any host name verification failure during communication between the client and the service.

Step 2

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

1. Log in to System Manager as an **admin** user.
2. Navigate to **Elements > Inventory**.
3. Click **Manage Elements**.
4. Select the Registered Element and click **Edit**.
5. Update the value for the **Node** in the **Application** section and **Host** value in **Access Point**.

Procedure to be followed on Managed Elements

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

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

\$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_supportedproducts_orig.xml

2. Restart SAL Agent using the following command:

service spiritAgent restart

Impact of changing the host name of Managed Elements

This section describes the changes required on System Manager if the host name of the Managed Elements changes.

Note:

For the procedure to change the IP Address and host name of the Managed Elements, refer the product documentation of Managed Elements.

Procedure to be followed on System Manager

Step 1

If the identity certificates of the clients contain the host name of the client computer, the client has to ensure that those certificates are re-initialized as per the changed host name of the client computer.

Step 2

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

1. Log in to System Manager as an **admin** user.
2. Navigate to **Elements > Inventory**.
3. Click **Manage Elements**.
4. Select the Registered Element and click **Edit**.
5. Update the value for the **Node** in the **Application** section and the **Host** value of **Access Point**.

Procedure to be followed on Managed Elements

Step 1

Perform these steps to make changes in the SAL Agent from the command-line interface (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**

- a. Restart SAL Agent using the following command:

```
# service spiritAgent restart
```

Step 2

This section describes the changes you need to make to the Data Replication Service Client. You can follow either of the two approaches, **A** or **B**.

- A. Reregister the node in the case of Session Manager:

1. Stop the client service from hosting 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
```

B. Reconfigure the node in the case of Presence:

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 does not work as expected, please use cold standby procedure to restore the system to the state prior to the change. For cold standby procedures, refer Appendix –C of Cold Standby procedure.

Appendix B — Procedure to change the date and time configuration

You can change the date, time, and time zone of System Manager from the System Platform webconsole. The prerequisite and steps to perform the changes are given below.

Prerequisite

- System Manager must be installed on a system and accessible.

Changing the time zone on the computer running System Manager

1. Go to the System Platform Web console at <https://<C-dom IPAddress>/webconsole>.
2. Log in with admin credentials, that is, log in as the admin user.
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.... Wait for the processing of the request to

complete. Once the operation completes, 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 completing the following steps:
 - a. Log in to System Manager from the command line.
 - b. Use the **service jboss restart** command to restart JBoss.
 - c. Wait for about 10 to 15 minutes, and then verify that the System Manager common console is accessible again.

Changing the date or time on the computer running System Manager

1. Go to the System Platform webconsole. The URL for the same is **https://<C-dom IPAddress>/webconsole**.
2. Log in with admin credentials, that is, log in as the admin user.
3. Click **Server Management**.
4. Click **Date/Time Configuration**.
5. Ensure that Network Time protocol daemon (ntpd) is not running.
6. Click in the text box that contains the date and time information. The system displays a pop-up calendar.
7. Click in the **time input** field and enter the new time value.
8. Select a date value in the calendar.
9. Click **Apply** to proceed with the change.
10. Click **Save Date and Time** and click **OK** to confirm the change. The system restarts.
11. Wait for 10 to 12 minutes for System Platform to redirect you to the log-in page.
12. Wait for another 5 to 7 minutes for the System Manager Webconsole to be accessible.

Verifying changes to the date and time configuration

1. Log in to the system running System Manager from the command line.
2. Type the **date** and press **Enter**. You can see the updated date, time, and time zone values.
3. After verifying the updated values, type **exit** and press **Enter**.

Appendix C — Cold standby procedure

Introduction

The System Manager server in cold standby mode acts as a failover when the main server running System Manager fails. This appendix covers the cold standby failover process for the System Manager application deployed on System Platform. The appendix explains the process with the example of two nodes, one being active and the other being the cold standby node. Node A is the primary machine that is active. Node B is the cold standby server. The cold standby procedure is to be implemented in the scenario where Node A fails and the application has to be failed over to Node B.

Prerequisites

- Node A and Node B should be on identical servers. Supported servers are 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. It is assumed that when the Active Node is running, the Cold Standby Server is powered off.
- The System Manager 6.1 template is deployed on Node A and Node B. For the procedure to install the template, see the *System Manager Installation Guide*.
- The system date is identical on both nodes.
- Regular backups of the System Manager DB of Node A are available. These backups are created either by using the Remote backup facility of System Manager Element Manager or from the System Platform webconsole. The backups are necessary so that the latest snapshot of the System Manager DB is available in case you need to implement the cold standby procedure. Retain the backup of the DB on a remote node or an external storage device, such as a tape drive or DVD. Use that backup to restore the DB on Node B when Node A fails. For the procedure to schedule a backup on the System Manager Node, see Appendix D.

Note:

The procedure to perform a backup from the System Platform webconsole, please refer section "Backing up System Platform" in the document "Administering Avaya Aura® System Platform".

Cold standby procedure

1. Confirm that Node A is shut down.
2. Power up Node B.
3. Install all System Manager patches on Node B, that were installed on Node A before the last backup was taken on Node A. (For example if patch 1 and patch 2 were installed on System Manager on Node A before the backup was taken, then install patch 1 and patch 2 on Node B before restoring the backup. Incase if patch-3 is available and not installed on Node A when backup was taken then install only patch -1 and patch-2 and not the patch-3. on Node B)
4. Restore the last DB 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 for the procedure to restore the backup on the System Manager node. If the backup was taken from the System Platform webconsole, please refer section "Restoring System Platform" in the document "Administering Avaya Aura® System Platform" to restore the backup from the System Platform webconsole.
5. After restoring the DB on Node B, you **MUST** run **postColdStandBy.sh** script on Node B from the location :- @ \$MGMT_HOME/utls/bin/coldstandby/postColdStandBy.sh

Note - After the restoration and running the postColdStandBy.sh script, System Manager on Node B is available for operations.

6. After restoring the DB on Node B, run following steps to retrieve TM trust-store password

- o `sh /home/ucmdeploy/quantum/queryDefaultCertInfo.sh`
- o `Restart jboss`

CLI restore for Cold Standby

You can also implement the cold standby procedure to restore the System Manager DB using the CLI utility.

CLI Utility properties

While performing a restore from the CLI, you may need to modify some of the restore properties related to the current setup. The file containing the properties related to CLI restore is

\$MGMT_HOME/pem/fileRestoreCLIUtility/fileRestoreCLIUtility.properties.

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

No.	Property name	Description
1	Version	The version of the current System Manager setup where you need to perform the restore. You can determine the value from both the UI and the CLI. To determine the value from the UI: 1. Log in to System Manager. 2. Go to Home > Services > Configurations> Setting > SMGR. The value in the property [System Manager Properties >> Build Version] is the System manager version. To determine the value 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 database utility installation. The default is set to /usr/bin. Do not modify the default setting.
4	db_host	The IP or host name of the DB computer, in this case, the computer running System Manager. 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.

No.	Property name	Description
6	db_name	The database name that needs to be connected for restore. The default is set to avmgt. Do not modify the default setting.
7	db_scpport	The SSH port to be used to connect the database machine. The default is set to 22. Do not modify the default setting unless you have modified 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 is directory /var/lib/pgsql/backup/manual/ , Then the value of the backup_name property should be /var/lib/pgsql/backup/manual/backup.zip .
10	Scp	Specifies if the backup archive is stored on the local computer running System Manager or a remote computer. The value false means the archive is on a local computer running System Manager and the value true means the archive is on some remote computer. The default is set to false.
11	scp_ip	The IP or 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.
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 running System Manager using the user *root*. If direct access to the system using the user *root* is disabled, then log in as *nonroot* by using direct access to the system, and then switch to the user *root*.
2. Update the **\$MGMT_HOME/pem/fileRestoreCLIUtility/fileRestoreCLIUtility.properties** file with

the required details. If the backup archive is present on the local system running System Manager and the default values related to restore are not modified, then 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 restore are not modified, then 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 **\$MGMT_HOME/pem/fileRestoreCLIUtility** to the directory that contains 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. The system prompts you to enter the full path of the backup archive. If the value is not specified in the **RestoreCLIUtility.properties** file, as mentioned in Step 2 above, 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 here. Press **Enter**.
6. If you are performing the restore with the backup archive present on a remote computer (with scp set to true), then the system prompts you to enter the scp user name. Specify the user name for performing SSH (Secure Shell) on the remote computer and obtain permission to access the backup archive. Press **Enter**.
7. If you are performing the restore with the backup archive present on a remote computer (with scp set to true), then the system prompts you to 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. The system prompts you to enter the password for database super user. Specify the password of database super user **postgres**, and press **Enter**.

10. The system prompts you to enter the choice for overwriting the current database with the one present in the backup archive. Type **y**, and press **Enter**.
11. The system prompts you to enter the database application user name. Specify **postgres** as the value, and press **Enter**.
12. The system prompts you to 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

1. Log in to the System Manager Web interface as an administrator.
2. Click **Home > 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. Click **Home > 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 patch present on the system when the backup was performed is also present when the restore is performed. System Manager patch information is available in the pop-up window when clicked **About** link.

The patch information will be displayed : System Manager 6.1.0 (Build No. - 6.1.0.5.xxxx - **6.1.5.xx**)

Appendix F — System Platform HA Mechanism

Introduction

System Manager uses the failover mechanism provided by System Platform.

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

System Platform HA uses VMs running on active cluster node only. This configuration is also known as the Active/Standby mode. All block devices that are part of DRBD synchronisation propagate all changes from the active node to the standby node. Avaya uses the most reliable protocol: C - synchronized replication. This protocol ensures that the system commits and acknowledges all block changes on the secondary node before continuing. Thus 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 the 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
- Sets the DRBD devices as primary on a new active node
- Boots the VMs on the new active node

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

- Gracefully shuts down the VMs on the active node.
- Sets the DRBD devices as secondary on the active node.
- Assigns the secondary node as a new primary node and vice versa.
- Sets the DRBD devices as primary 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 exactly 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 is able to detect which node has 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 one node only and all resources are migrated.
- Keeps the same IP addresses for all VMs, for example, CDom and System Manager, on the active and standby nodes.
- Uses Heartbeat to start the DRBD service on both nodes.
- For each VM on 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 crossover cable on ports eth2. Perform this connection before you configure HA Failover.
4. Perform all the required checks on the standby node from the Web console. Perform the checks before you configure HA Failover. The Standby Web console is not accessible after that.
5. Configure System Platform HA Failover from the preferred node Web console.
6. Ensure that you can contact the DNS servers from both servers. Perform this step before you configure HA Failover. If DNS is configured but DNS servers are not accessible, SSH communication can be delayed. This can cause the HA Failover configuration to fail.
7. Ensure that you can contact either NTP server from both servers, or that you can disable NTP on both servers. Do this before you configure HA Failover. If NTP is configured but the NTP servers are not accessible, SSH communication can be delayed. This 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. After that, it redirects to the log-in page, and you can log in again

Don'ts

- Do not install the template on 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 — Steps for resetting Admin user Password

Please follow below mentioned steps for resetting System Manager web-console admin user password:

1. Login to System Manager CLI using user root. If direct CLI access is not enable for user root then login using user admin having direct access to CLI enabled and then switch to user root.
2. Run the below mentioned command to create a group securityadmin:

```
groupadd -g 600 securityadmin
```

If it gives error “groupadd: GID 600 is not unique” then use a higher value instead of 600 and run same command.

If its give error as “groupadd: group securityadmin exists” then group is already present and does not need to be created.

3. Run the below mentioned command to verify if user admin has group securityadmin assigned to him (this may happen if the group securityadmin was already present and assigned to user admin):

```
groups admin
```

The output of command should not mention securityadmin in the list of groups assigned to user admin.

4. This step is needed only if output of step 3 mentions that group securityadmin is not assigned to user admin. Run the below mentioned command to assign group securityadmin to user admin:

```
usermod -aG securityadmin admin
```

5. Access System Manager local login screen by using below mentioned URL:

```
https://<IP Address/Fully Qualified Hostname>/local-login
```

Use the login credentials of the System Manager CLI user admin to log in.

6. Once the “Security Configuration” screen is displayed, change the URL to below mentioned URL:

```
https://<IP Address/Fully Qualified Hostname>/passwordReset
```

7. Once the “Password Reset” screen is displayed, specify the “User ID” as “admin” and new password as “admin123”.
8. Once the “Password changed successfully.” message is displayed, closed the current browser session and access System Manager login screen in new browser session using below mentioned URL:

`https://<IP Address/Fully Qualified Hostname>/SMGR`

If you are accessing using fully qualified hostname then

- a. Login using the password specified in step 7 (admin123).
- b. It will prompt for new password, specify new password.

If you are accessing using IP then

- a. Click on the “Change Password” link on the login page and change password.
- b. Re-access System Manager login screen and login using new password.

9. If group securityadmin was assigned to user admin during step 4 then follow below step to un-assign group securityadmin from user admin:
 - a. Run below mentioned command (on System Manager CLI as user root) to list the groups assigned to user admin:

`groups admin`

Consider the output is:

`admin: admin xxx securityadmin xyz`

- b. Run below mentioned command to un-assign group securityadmin from user admin:

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

e.g., as per above example the command should be:

`usermod -G admin,abc,xyz admin`

10. If group securityadmin was created during step 2 then run below mentioned command to delete group securityadmin:

`groupdel securityadmin`