Deploying Avaya Aura® System Manager in Software-Only Environment
© 2018-2020, Avaya Inc.  
All Rights Reserved.

Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in the Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service
THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE. HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACQUIRES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types
Designated System(s) License (DS), End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order, or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software
“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.
Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization
The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two instances of the same type of products, then two products of that type must be ordered.

Third Party Components
“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, solely with respect to the applicable Third Party Components. The Third Party Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws
You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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

Avaya Toll Fraud intervention
If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities
Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation
For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support
See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks
The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.
Chapter 1: Introduction

Purpose

This document describes how to deploy the Avaya Aura® System Manager Software-Only ISO image on a customer-provided hardware.

This document is intended for people who install and configure System Manager ISO image at a customer site.

The software-only offer is for customers who want to deploy the Avaya Aura® applications on their own standard Linux operating system. Avaya Aura® applications support third party applications only on the software-only deployments.

⚠️ Note:

A virtualized environment is required for the software-only deployment.

Prerequisites

Before deploying the System Manager ISO image, ensure that you have the following knowledge, skills and tools.

Knowledge

• Linux® Operating System
• Avaya Aura® System Manager
• Virtualized environment

Skills

To administer the Linux server and Avaya Aura® applications.

Tools

For information about tools and utilities, see Configuration tools and utilities on page 16.
## Change history

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>May 2020</td>
<td>For Release 8.1.2, updated the section: <a href="#">Software-only environment overview</a> on page 9</td>
</tr>
<tr>
<td>4</td>
<td>October 2019</td>
<td>For Release 8.1.1, updated the section: <a href="#">Software details of System Manager</a> on page 13</td>
</tr>
<tr>
<td>3</td>
<td>August 2019</td>
<td>Added the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">System Manager disk partitioning</a> on page 20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">System Manager RPMs</a> on page 74</td>
</tr>
<tr>
<td>2</td>
<td>July 2019</td>
<td>Added the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Supported Red Hat Enterprise Linux operating system versions for Software-only Environment</a> on page 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura application OVAs</a> on page 11</td>
</tr>
<tr>
<td>1</td>
<td>June 2019</td>
<td>Release 8.1 document.</td>
</tr>
</tbody>
</table>
Chapter 2: Software-only environment overview

Avaya Aura® Release 8.0 and later supports software-only installation. In a software-only installation, the customer owns the operating system and must provide and configure the operating system for use with Avaya Aura® application. With the software-only offer, the customer can install and customize the operating system to meet the requirements to install the Avaya Aura® application.

You must run the software-only offer on the supported environments to enable the use of Avaya approved third-party applications for anti-virus, backup, and monitoring.

Customers must procure a server that meets the recommended hardware requirements and the appropriate version of Linux® Operating System.

Software security updates

Avaya Security Service Packs (SSP) and Kernel Service Packs (KSP) are built for customers who do not use the software-only distribution. Software-only installation is in the control of the operating system and is responsible for applying the relevant security patches from Red Hat.

Supported third-party applications

With the software-only (ISO) offer, you can install third-party applications on the system and get more control on the system. For the list of supported third-party software applications in Release 8.0 and later, see Avaya Product Support Notice at PSN020360u.

Avaya Aura® Software-Only environment RPMs

In a software-only installation, the customer will also install the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, it is recommended to check the list of tested RPMs and follow the instructions in the PSN periodically published by Avaya. PSN is available at PSN020361u.

Note:

For information about RPM updates for the Red Hat Linux Enterprise operating system and required changes to operating system files on Software only installation, see Avaya Aura® Software Only White paper on the Avaya Support website.

Supported platforms

You can deploy the Avaya Aura® application software-only ISO image on the following platforms:

- VMware
- Kernel-based Virtual Machine (KVM)
- Hyper-V
**Note:**
Starting with the Release 8.0.1, Avaya Aura® applications support Hyper-V.

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

## Supported applications in Software-only Environment

- Avaya Aura® System Manager
- Avaya WebLM
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Application Enablement Services
- Avaya Aura® Media Server

## Supported Red Hat Enterprise Linux operating system versions for Software-only Environment

The following table lists the supported Red Hat Enterprise Linux operating system versions for deploying or upgrading Avaya Aura® applications in Software-only Environment.

<table>
<thead>
<tr>
<th>Red Hat Enterprise Linux operating system</th>
<th>Avaya Aura® Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux operating system Release 7.4 with 64-bit</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>System Manager Release 8.0.x only supports the Red Hat Enterprise Linux operating system Release 7.5 with 64-bit.</td>
</tr>
<tr>
<td>Linux operating system Release 7.6 with 64-bit</td>
<td></td>
</tr>
</tbody>
</table>
## Supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura® application OVAs

The following table lists the supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura® application OVAs.

<table>
<thead>
<tr>
<th>Red Hat Enterprise Linux operating system</th>
<th>Avaya Aura® Release</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.0.x</td>
</tr>
<tr>
<td>Linux operating system Release 6.5 with 64-bit</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: System Manager Release 7.0.x only supports the CentOS Operating System Release 6.5 with 64-bit.</td>
<td></td>
</tr>
</tbody>
</table>

| Linux operating system Release 7.2 with 64-bit | Y |
|                                               |   |
| Note: Utility Services Release 7.1 uses the Red Hat Enterprise Linux operating system Release 7.3 with 64-bit. |

*Table continues*...
<table>
<thead>
<tr>
<th>Red Hat Enterprise Linux operating system</th>
<th>Avaya Aura® Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux operating system Release 7.4 with 64-bit</td>
<td>7.0.x</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
</tr>
<tr>
<td>System Manager Release 8.0.x only supports the Red Hat Enterprise Linux operating system Release 7.5 with 64-bit.</td>
<td></td>
</tr>
<tr>
<td>Linux operating system Release 7.6 with 64-bit</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 3: Planning and preconfiguration

Planning checklist

Before creating a virtual machine and installing the operating system, you must perform the following:

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Description/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download and install the virtualization software and the operating system. Note: The operating system needs to be configured to meet the application's requirement.</td>
<td>Ensure that the virtual environment with required operating system is installed and is available for software-only deployment.</td>
</tr>
<tr>
<td>2</td>
<td>Download the ISO.</td>
<td>See “Software details”</td>
</tr>
<tr>
<td>3</td>
<td>Install the required third-party software.</td>
<td>For the list of supported third-party software applications in Release 8.0 and later, see the Avaya Product Support Notice at PSN020360u.</td>
</tr>
<tr>
<td>4</td>
<td>Purchase and obtain the required licenses.</td>
<td>Downloading software from PLDS on page 15</td>
</tr>
<tr>
<td>5</td>
<td>Register for PLDS and activate license entitlements.</td>
<td>Downloading software from PLDS on page 15</td>
</tr>
<tr>
<td>6</td>
<td>Prepare the site.</td>
<td>Site preparation checklist on page 14</td>
</tr>
</tbody>
</table>

Software details of System Manager

For Avaya Aura® application software build details of OVA, ISO, service patch, Data migration Utility, or Solution Deployment Manager Client, see Avaya Aura® Release Notes on the Avaya Support website at http://support.avaya.com/.
**Latest software updates and patch information**

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSN), and Product Correction Notices (PCN) for the product or solution on the Avaya Support Web site at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.

⚠️ **Important:**

The customer is responsible for updates to the virtual environment and the operating system. Avaya is only responsible for Avaya Aura® application updates in the software-only deployment. You must refer to the appropriate PSN for Avaya approved software-only updates.

---

**Verifying if TMOUT variable is not set to read-only**

**About this task**

Ensure that the **TMOUT** variable permission is not set to read-only. Use the following procedure to check if TMOUT is set as read-only.

**Procedure**

1. Using the SSH client, type `export TMOUT=0` command.
   - If the system does not return an error then no further action is required.
2. If the system returns an error, do the following:
   a. Comment out line `readonly TMOUT` (from the profile which sets TMOUT as read-only).
   b. Close the existing session and open a new SSH session.

---

**Site preparation checklist**

Use the following checklist to know the set up required to deploy the application ISO file in the software-only environment:
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a virtual machine on the supported virtualized environment.</td>
<td>See the corresponding virtualized environment documentation.</td>
</tr>
<tr>
<td>2</td>
<td>Subscribe to Red Hat network.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Install the Red Hat Enterprise Linux (RHEL) 7.6 with minimal configuration for the Software-Only deployment.</td>
<td>See Red Hat documentation.</td>
</tr>
</tbody>
</table>

---

**Downloading software from PLDS**

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from [http://support.avaya.com](http://support.avaya.com) using the Downloads and Documents tab at the top of the page.

⚠️ **Note:**

Only the latest service pack for each release is posted on the support site. Previous service packs are available only through PLDS.

**Procedure**

1. Enter [http://plds.avaya.com](http://plds.avaya.com) in your Web browser to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Click **View Downloads**.
5. Click on the search icon (magnifying glass) for **Company Name**.
6. In the %Name field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. In the **Download Manager** box, click the appropriate download link.
Note:

The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.

13. If you use Internet Explorer and get an error message, click the **install ActiveX** message at the top of the page and continue with the download.

14. Select a location where you want to save the file and click **Save**.

15. If you used the Download Manager, click **Details** to view the download progress.

---

**Supported browsers**

- Internet Explorer 11
- Mozilla Firefox 65, 66, and 67

---

**Configuration tools and utilities**

To deploy Avaya Aura® ISO for the software-only environment and to configure the application, you need the following tools and utilities:

- PuTTY and WinSCP
- SDM Client (Optional)

---

**Supported footprints of System Manager Software-Only ISO image**

<table>
<thead>
<tr>
<th>Footprint</th>
<th>CPUs (GHz)</th>
<th>Number of vCPUs</th>
<th>CPU reservation</th>
<th>RAM (GB)</th>
<th>Memory reservation</th>
<th>HDD (GB)</th>
<th>NICs</th>
<th>Number of users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile 2</td>
<td>2.29</td>
<td>6</td>
<td>13740</td>
<td>12</td>
<td>12288</td>
<td>105</td>
<td>1</td>
<td>250000</td>
</tr>
<tr>
<td>Profile 3</td>
<td>2.29</td>
<td>8</td>
<td>18320</td>
<td>18</td>
<td>18432</td>
<td>250</td>
<td>1</td>
<td>250000</td>
</tr>
<tr>
<td>Profile 4</td>
<td>2.2</td>
<td>18</td>
<td>39600</td>
<td>36</td>
<td>39600</td>
<td>850</td>
<td>1</td>
<td>300000</td>
</tr>
</tbody>
</table>

*Table continues…*
For deploying System Manager *Software-Only ISO image* on VMware, AWS, GCN, and Azure, you must configure the system with the following hard disk (GB) and in the same order:

- **Profile 2**: HDD1: 44, HDD 2: 25, HDD3: 15, HDD4: 21
- **Profile 3**: HDD1: 150, HDD 2: 30, HDD 3: 20, HDD4: 50
- **Profile 4**: HDD1: 650, HDD 2: 30, HDD 3: 20, HDD4: 150

For deploying System Manager *Software-Only ISO image* on KVM, you must configure the system with the following hard disk (GB):

- **Profile 2**: HDD: 105
- **Profile 3**: HDD: 250
- **Profile 4**: HDD: 850

### Users and groups

The following tables list all the users and groups added by the installer.

#### Users

<table>
<thead>
<tr>
<th>Username</th>
<th>Login account</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Yes</td>
<td>Admin user</td>
</tr>
<tr>
<td>csadmin</td>
<td>Yes</td>
<td>User needed for SDM access</td>
</tr>
<tr>
<td>smgr</td>
<td>Yes</td>
<td>System Manager user</td>
</tr>
<tr>
<td>nortel</td>
<td>Yes</td>
<td>Nortel user</td>
</tr>
<tr>
<td>init</td>
<td>Yes</td>
<td>Service account (EASG)</td>
</tr>
<tr>
<td>inads</td>
<td></td>
<td></td>
</tr>
<tr>
<td>craft</td>
<td>Yes</td>
<td>Service account (EASG)</td>
</tr>
<tr>
<td>sroot</td>
<td>Yes</td>
<td>Service account (EASG)</td>
</tr>
<tr>
<td>rasaccess</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Groups

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>susers</td>
<td>Members of this group have the necessary privileges needed to operate and maintain the application.</td>
</tr>
<tr>
<td>admin</td>
<td>Members of this group have the administrator privileges.</td>
</tr>
<tr>
<td>securityadmin</td>
<td></td>
</tr>
<tr>
<td>smgr</td>
<td></td>
</tr>
</tbody>
</table>

*Table continues…*
### Group & Description

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nortel</td>
<td></td>
</tr>
<tr>
<td>csadmin</td>
<td></td>
</tr>
<tr>
<td>logadmin</td>
<td></td>
</tr>
<tr>
<td>cust</td>
<td></td>
</tr>
<tr>
<td>groot</td>
<td></td>
</tr>
<tr>
<td>gadmin</td>
<td></td>
</tr>
<tr>
<td>gsmgr</td>
<td></td>
</tr>
<tr>
<td>gcliuser</td>
<td></td>
</tr>
<tr>
<td>gasguser</td>
<td></td>
</tr>
<tr>
<td>gcacadmin</td>
<td></td>
</tr>
<tr>
<td>gcacnonadmin</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4: Deploying the System Manager
Software-Only ISO image using operating system console

Preparing for software-only deployments

About this task
Use this procedure to prepare the setup for software-only deployments.

Procedure

1. Create an RHEL instance with required resources. For more information on creating RHEL instance, see Red Hat documentation.
   For more information about the required resources, see Supported footprints information for respective environments.

2. Register the RHEL instance to the Red Hat subscription or create local repository for RPM installation or updates.
   For example,
   ```bash
   subscription-manager repos --enable rhel-7-server-rpms
   ```

3. To create a directory, run the following command:
   ```bash
   mkdir /var/installer
   ```

4. Download the Avaya Aura® application ISO to the RHEL instance.

5. Run the following command to mount the ISO:
   ```bash
   mount -o loop AvayaAuraSystemManager-8.1.x.0.xxxxxx_v47.iso /mnt
   ```

6. Run the following command to copy the ISO to the directory:
   ```bash
   cp -rvf /mnt/* /var/installer
   ```

7. Run the following command to install dependencies:
   ```bash
   yum install SMGR-Dependencies-0.1-1.noarch.rpm -y
   ```

8. Run the following command to unmount the /mnt directory:
   ```bash
   umount /mnt
   ```
9. Run the following commands to install required RPMs:
   
   ```bash
   cd pre-install_rpms
   rpm -Uivh *.rpm --nodeps
   ```

   For the list of tested Avaya Aura® Software-Only RPMs, see Avaya PSN020361u at PSN020361u.

   **Important:**
   The PSN PSN020361u provides details of the latest RPMs tested with Avaya applications. These RPM versions should be used when installing and updating the operating system. Using the RPM versions that are not tested might result in an operational impact to the Avaya application.

10. Disable SELinux if already enabled.

    For disabling SELinux, see Red Hat documentation.

11. For AWS, run the following commands to remove cloud-init package:

    ```bash
    systemctl stop cloud-init
    systemctl disable cloud-init
    yum remove cloud-init -y
    ```

12. Reboot the system.

---

**System Manager disk partitioning**

Use the following table to refer to the recommended values for disk size and partition.

The disk partitioning is recommended. Alternatively, a single root partition can be used as long as it meets the minimum total disk size for the profile.

<table>
<thead>
<tr>
<th>Partition</th>
<th>Profile 2</th>
<th>Profile 3</th>
<th>Profile 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>4.2 GB</td>
<td>16 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>/tmp</td>
<td>1.5 GB</td>
<td>5.9 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>/var</td>
<td>5.5 GB</td>
<td>18 GB</td>
<td>40 GB</td>
</tr>
<tr>
<td>/opt</td>
<td>9.7 GB</td>
<td>34 GB</td>
<td>45 GB</td>
</tr>
<tr>
<td>/var/log</td>
<td>1.9 GB</td>
<td>7.3 GB</td>
<td>36 GB</td>
</tr>
<tr>
<td>/var/lib/pgsql/data</td>
<td>14 GB</td>
<td>51 GB</td>
<td>450 GB</td>
</tr>
<tr>
<td>/home</td>
<td>1.9 GB</td>
<td>7.3 GB</td>
<td>10 GB</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>1.9 GB</td>
<td>7.3 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td>/boot</td>
<td>509 MB</td>
<td>509 MB</td>
<td>509 MB</td>
</tr>
<tr>
<td>/perfdata</td>
<td>25 GB</td>
<td>30 GB</td>
<td>30 GB</td>
</tr>
<tr>
<td>/emdata</td>
<td>15 GB</td>
<td>20 GB</td>
<td>20 GB</td>
</tr>
</tbody>
</table>

Table continues…
### Checking the environment

**Before you begin**
- Create an RHEL instance.
- Create a user before running the installer.
- Install required RPMs.

**Procedure**

1. Log in to the RHEL instance as a default user and switch to the root account.
   You must run the installer as a root user.
2. Go to, `#cd /var/installer`.
3. To check for installer environment check, do one of the following:
   - For profile 2, type the following command:
     ```bash
     ./Install_System_Manager_8.1.0.0.xxxxxx -c -p 250Kuser
     ```
   - For profile 3, type the following command:
     ```bash
     ./Install_System_Manager_8.1.0.0.xxxxxx -c -p 250Kuser-prof3
     ```
   - For profile 4, type the following command:
     ```bash
     ./Install_System_Manager_8.1.0.0.xxxxxx -c -p 300Kuser-prof4
     ```

The system checks for the environment against the installer. During this time, you cannot perform any other action.

If the check fails, take necessary steps to fix errors and perform the installer check again.

---

### Note:

If you are planning to use an antivirus or another approved third party application, you must add the disk space required by the third party application to the values in the above table.

---

<table>
<thead>
<tr>
<th>Partition</th>
<th>Profile 2</th>
<th>Profile 3</th>
<th>Profile 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>/swlibrary</td>
<td>21 GB</td>
<td>50 GB</td>
<td>150 GB</td>
</tr>
<tr>
<td>swap</td>
<td>4 GB</td>
<td>4 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Minimal disk size</td>
<td>105 GB</td>
<td>250 GB</td>
<td>850 GB</td>
</tr>
</tbody>
</table>
Deploying System Manager **Software-Only ISO image** using the OS console

**About this task**
Use this procedure to deploy the System Manager ISO image in a Software-Only environment.

**Before you begin**
- Create an operating system instance.
- Copy the installer and check the environment.

**Procedure**
1. Log on to the RHEL instance.
2. Go to the `/var/install` directory.
3. Run the following installation script as a root user:
   ```
   ./Install_System_Manager_8.1.0.0.xxxxxx
   ```
   The system runs the command and displays the installation status of the required RPMs.
4. Read the prompt messages.
5. Press **Enter** to continue.
6. The installer checks the package and environment settings.
   The system displays the following message:
   ```
   A reboot will be required in order to complete this. Please exit any other sessions before continuing.
   ```
7. Press **Enter** to continue.
8. If the installer does not find old network interfaces naming scheme (eth0 and eth1), when prompted, type **yes** to convert network interfaces to old scheme.
   The system displays the message: Rebooting the system and please re-run the SMGR install after reboot.
9. After reboot of the system, go to `/var/installer`, and re-run the following installation script as a root user:
   ```
   ./Install_System_Manager_8.1.0.0.xxxxxx
   ```
10. On the End User License Agreement page, press **Y** to start the installation process.
11. The system starts the installation and prompts you to configure the System Manager configuration and network parameters such as IPv4 address, IPv4 netmask, IPv4 gateway, short hostname, domain name, DNS server IP, IPv6 address, IPv6 network prefix, IPv6 gateway address, default search list, NTP IP, virtual hostname, virtual domain name, SNMP V3 parameters, SMGR CLI username and Password before proceeding to the next
step. For more information on configuration and network parameters, see Network and configuration field descriptions on page 33

11. In the Enter profile page, select the required System Manager profile from the following:
   • Press 1 for profile 2
   • Press 2 for profile 3
   • Press 3 for profile 4

12. On the Enhanced Access Security Gateway (EASG) page, read the EASG information, and click OK.

13. Select one of the following options to enable or disable EASG and click OK:
   • Enable EASG (Recommended)
   • Disable EASG

14. Verify the configuration details and press Enter to continue.

15. Select the required Backup definition parameter for System Manager schedule backup.

16. Click Yes to install Avaya’s version of bash RPM.

   Installing Avaya’s customized bash is optional, but Avaya recommends to install Avaya’s customized bash to help Avaya support.

   This step is applicable only if the installed version of the bash RPM is older than the Avaya provided bash RPM.

17. Click Continue to reboot the system for post installation configuration.

18. To verify post installation status, run the following command:

   ```
   cd/var/log/Avaya/PostDeployLogs/
   tail -f post_install_sp.log
   ```

   **Note:**
   On successful post installation, exit status of eject command is 0 is displayed.

19. Access System Manager web interface using IP address or FQDN. If installation is successful, Installation of latest System manager patch is mandatory is displayed.

   **Note:**
   For more information on mandatory patch installation, see “Installing mandatory patch” in Upgrading Avaya Aura® System Manager
Chapter 5: Deploying System Manager ISO image using Solution Deployment Manager

Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® applications. Solution Deployment Manager supports the operations on customer Virtualized Environment and Avaya Aura® Virtualized Appliance model.

Solution Deployment Manager provides the combined capabilities that Software Management, Avaya Virtual Application Manager, and System Platform provided in earlier releases.

From Release 7.1 and later, Solution Deployment Manager supports migration of Virtualized Environment-based 6.x, 7.0.x, and 7.1.x applications to Release 8.0 and later in customer Virtualized Environment. For migrating to Release 8.0, you must use Solution Deployment Manager Release 8.0.

Release 7.0 and later supports a standalone version of Solution Deployment Manager, the Solution Deployment Manager client. For more information, see Using the Solution Deployment Manager client.

System Manager with Solution Deployment Manager runs on:

- **Avaya Aura® Virtualized Appliance**: Contains a server, Appliance Virtualization Platform, and Avaya Aura® application OVA. Appliance Virtualization Platform includes a VMware ESXi 6.0 hypervisor.
  
  From Release 7.0 and later, Appliance Virtualization Platform replaces System Platform.

- **Customer-provided Virtualized Environment solution**: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.

- **Software-Only environment**: Avaya Aura® applications are deployed on the customer-owned hardware and the operating system.

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Refresh applications and associated devices, and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
• Upgrade Avaya Aura® applications.
• Install software patch, service pack, or feature pack on Avaya Aura® applications.

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 8.0, see Avaya Aura® System Manager Solution Deployment Manager Job-Aid.

Installing the Solution Deployment Manager client

Prerequisites

1. If an earlier version of the Solution Deployment Manager client is running on the computer, remove the older version from Control Panel > Programs > Programs and Features.

   For information about uninstalling the Solution Deployment Manager client, see “Uninstalling the Solution Deployment Manager client”.

2. Ensure that Windows 7, Windows 8.1 64-bit, Windows 10 64-bit, or Windows 16 64-bit, operating system is installed on the computer.

   Tip:
   On Computer, right-click properties, and ensure that Windows edition section displays the version of Windows operating system.

3. Ensure that at least 5 GB of disk space is available at the location where you want to install the client. To deploy applications, you must have additional 15 GB of disk space on your system.

   Tip:
   Using the Windows file explorer, click Computer, and verify that the Hard Disk Drives section displays the available disk space.

4. To avoid port conflict, stop any application server that is running on your computer.

   Tip:
   From the system tray, open the application service monitor, select the application server that you want to stop, and click Stop.

5. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client installation and use the Solution Deployment Manager functionality.

   Note:
   Ensure that port 8005 or 8009 is available for installing and running Solution Deployment Manager Client. If port 8005 or 8009 is assigned to any other application, you must free up the ports for starting the Avaya SDM service.
Installing the Solution Deployment Manager client on your computer

About this task
In Avaya Aura® Virtualized Appliance offer, when the centralized Solution Deployment Manager on System Manager is unavailable, use the Solution Deployment Manager client to deploy the Avaya Aura® applications.

You can use the Solution Deployment Manager client to install software patches of only System Manager and hypervisor patches of Appliance Virtualization Platform.

Use the Solution Deployment Manager client to deploy, upgrade, and update System Manager.

From Avaya Aura® Appliance Virtualization Platform Release 7.0, Solution Deployment Manager is mandatory to upgrade or deploy the Avaya Aura® applications.

Procedure
2. On the Avaya Support website, click Support by Products > Downloads, and type the product name as System Manager, and Release as 8.1.x.
3. Click the **Avaya Aura® System Manager Release 8.1.x SDM Client Downloads, 8.1.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

You can also copy the zip file to your software library directory, for example, *c:/tmp/Aura*.

4. Right click on the executable, and select **Run as administrator** to run the *Avaya_SDMClient_win64_8.1.x.0.xxxxxx_xx.exe* file.

The system displays the Avaya Solution Deployment Manager screen.

5. On the Welcome page, click **Next**.

6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.

7. On the Install Location page, perform one of the following:

   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.

     If the *C:\Program Files\Avaya\AvayaSDMClient* directory is not empty, the installer displays the following message: To install the SDM client, select an empty directory or manually delete the files from the installation directory.

     If the file is locked and you are unable to delete it, reboot the machine, and then delete the file.

   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

     To restore the path of the default directory, click **Restore Default Folder**.

     The default installation directory of the Solution Deployment Manager client is *C:\Program Files\Avaya\AvayaSDMClient*.

8. On the Pre-Installation Summary page, review the information, and click **Next**.

9. On the User Input page, perform the following:

   a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.

   b. To change the default software library directory on windows, in Select Location of Software Library Directory, click **Choose** and select a directory.

      The default software library of the Solution Deployment Manager client is *C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts*.

      You can save the artifacts in the specified directory.

   c. In **Data Port No**, select the appropriate data port.

      The default data port is 1527. The data port range is from 1527 through 1627.
d. In **Application Port No**, select the appropriate application port.
   
The default application port is 443. If this port is already in use by any of your application on your system, then the system does not allow you to continue the installation. You must assign a different port number from the defined range. The application port range is from 443 through 543.

   **Note:**
   
   After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.

e. (Optional) Click **Reset All to Default** to reset all values to default.

10. Click **Next**.

11. On the Summary and Validation page, verify the product information and the system requirements.
   
The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the user must make the required disk space, memory, and the ports available to start the installation process again.

12. Click **Install**.

13. On the Install Complete page, click **Done** to complete the installation of Solution Deployment Manager Client.
   
   Once the installation is complete, the installer automatically opens the Solution Deployment Manager client in the default web browser and creates a shortcut on the desktop.

14. To start the client, click the Solution Deployment Manager client icon.

**Next steps**

- Configure the laptop to get connected to the services port if you are using the services port to install.

- Connect the Solution Deployment Manager client to Appliance Virtualization Platform through the customer network or services port.

   For information about “Methods to connect the Solution Deployment Manager client to Appliance Virtualization Platform”, see *Using the Solution Deployment Manager client*.

---

**Adding a location**

**About this task**

You can define the physical location of the host and configure the location specific information. You can update the information later.
**Procedure**

1. On the desktop, click the SDM icon (SDM), and then click **Application Management**.
2. On the **Locations** tab, in the Locations section, click **New**.
3. In the New Location section, perform the following:
   a. In the Required Location Information section, type the location information.
   b. In the Optional Location Information section, type the network parameters for the virtual machine.
4. Click **Save**.

   The system displays the new location in the **Application Management Tree** section.

---

**Adding a software-only platform**

**About this task**

Use this procedure to add an operating system on Solution Deployment Manager. In Release 8.1.2, the system supports the Red Hat Enterprise Linux Release 7.6 64-bit operating system.

**Before you begin**

Add a location.

**Procedure**

1. On the desktop, click the SDM icon (SDM), and then click **Application Management**.
2. On the **Platforms** tab, click **Add**.
3. In **Platform Name**, type the name of the platform.
4. In **Platform FQDN or IP**, type the FQDN or IP address of the base operating system.
5. In **User Name**, type the user name of the base operating system.

   For a software-only deployment, the user name must be a direct access admin user. If the software-only application is already deployed, provide the application cli user credentials.

6. In **Password**, type the password of the base operating system.
7. In **Platform Type**, select **OS**.
8. Click **Save**.

   If the platform has some applications running, the system automatically discovers those applications and displays the applications in the **Applications** tab.

   - If Solution Deployment Manager is unable to establish trust, the system displays the application as Unknown.
Deploying System Manager ISO image using Solution Deployment Manager

• If you are adding OS, only **Add** and **Remove** operations are available on the **Platforms** tab. You cannot perform any other operations. On the **Applications** tab, the system enables the **New** option. If the application is System Manager, the system enables **Update App** on Solution Deployment Manager Client.

The system displays the added base operating system on the **Platforms** tab.

---

**Deploying the System Manager **Software-Only ISO image** by using Solution Deployment Manager Client**

### About this task

Use this procedure to deploy the System Manager ISO image in a Software-Only environment.

### Before you begin

- Add a location.
  
  See **Adding a location** on page 28

- Add a platform
  
  See **Adding a software-only platform** on page 29

- Add an Operating System user on RHEL instance.
  
  For example, you can add a user using the following commands: `adduser <username>`, `passwd <username>`

- Set the password for the root user.
  
  For example, you can set the password using the following command: `passwd <root>`

- Install System Manager dependencies on RHEL instance.

- Delete the `/var/installer` folder from RHEL machine, after installing the dependencies.

### Procedure

1. To start the Solution Deployment Manager client, click **Start > All Programs > Avaya > Avaya SDM Client** or click the SDM icon on the desktop.

2. Click **Application Management**.

3. In **Application Management Tree**, select a location.

4. On the **Applications** tab, click **New**.

   The system displays the Application Deployment dialog box.

5. In the Select Location and Platform section, do the following:
   
   a. In **Select Location**, select a location if not already selected.

   b. In **Select Platform**, select a platform to deploy the **Software-Only ISO image**.
The system displays the IP Address and FQDN of the platform in the **Platform IP** and **Platform FQDN** fields.

6. In the Provide admin and root Credentials section, do the following:
   a. In **Admin User of OS**, type the admin user name.
   b. In **Admin Password of OS**, type the admin user password.
   c. In **Root User of OS**, type the root user name.
   d. In **Root Password of OS**, type the root user password.
   e. **(Optional)** Click **Test Connection**.
      The system logs into the platform by using the credentials to test the platform connectivity. If connectivity is established, the system displays the message: **Test Connection Successful**.
   f. Click **OK**.

7. Click **Next**.

8. To select the required application, on the **ISO** tab, click one of the following:
   - **SW Library / Select from software library**: Select the local library where the **ISO image** is available.
     If you are deploying the **ISO image** from the Solution Deployment Manager client, you can use the default software library that is set during the Solution Deployment Manager Client installation.
   - **Browse**: Select the **ISO image** from your local computer, and click **Submit File**.
   - **URL**: Click **URL** and provide the path to the **ISO image**.

Select the required application, click **Submit**.

If the application **ISO image** supports the patch deployment, the system enables the **Service or Feature Pack** tab.

9. **(Optional)** To install the patch file for the application, click **Service or Feature Pack**, and enter the appropriate parameters.
   a. Click **URL**, and provide the absolute path to the latest service or feature pack.
   b. Click **SW Library / Select from software library**, and select the latest service or feature pack.
   c. Click **Browse**, and select the latest service or feature pack.

You can install the System Manager Release 8.1.2 bin file now or after completing the System Manager deployment.

If you do not provide the System Manager Release 8.1.2 bin file at the time of deploying the System Manager, the system displays the following message:

```
Installation of the latest System Manager patch is mandatory. Are you sure you want to skip the patch installation? If Yes, ensure to manually install the System Manager patch later.
```
10. In **Flexi Footprint**, select the footprint size for the application.

11. In Test Your Operating System Compatibility Against Element Software Package, click **Test Environment Compatibility**.

   The installer checks if the platform has all the dependent rpms, network, cpu, memory, and hard disk configuration as specified for the element. This process takes about 4-5 minutes. After the process starts, you cannot proceed further until the process is complete. If you get any error or warning, make the necessary changes before the next steps. After the check is completed successfully, the system displays a message “Environment check is successful”.

   ✪ **Note:**

   If the browser hangs, the system provides the option to end the script or wait. Always click **Wait**.

12. (Optional) To view the installer compatibility results in a separate window, click **View Output**.

   The system displays the Environment Check Output window.

13. Click **Next**.

14. On the Configuration Parameters page, provide all the information required.

   For more information, see [Network and configuration field descriptions](#) on page 33

15. Click **Deploy**.

16. On the EULA Acceptance window, click **Accept**.

   After accepting EULA, the system displays Software only Installation Warning for software-only application deployment.

17. To continue with the deployment, click **Accept**.

   The system displays the deployment status in the **Current Action Status** column and the deployed application on the **Applications** tab.

18. To view details, click **Status Details**.
# Chapter 6: Configuration

## Network and configuration field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IPv4 Address</td>
<td>The IPv4 address of the System Manager application for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.</td>
</tr>
<tr>
<td>Management Netmask</td>
<td>The Out of Band Management subnetwork mask to assign to the System Manager application.</td>
</tr>
<tr>
<td>Management Gateway</td>
<td>The gateway IPv4 address to assign to the System Manager application.</td>
</tr>
<tr>
<td>IP Address of DNS Server</td>
<td>The DNS IP addresses to assign to the primary, secondary, and other System Manager applications. Separate the IP addresses with commas (,).</td>
</tr>
<tr>
<td>Management FQDN</td>
<td>The FQDN to assign to the System Manager application.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address of the System Manager application for out of band management. The field is optional.</td>
</tr>
<tr>
<td>IPv6 Network prefix</td>
<td>The IPv6 subnetwork mask to assign to the System Manager application. The field is optional.</td>
</tr>
<tr>
<td>IPv6 Gateway</td>
<td>The gateway IPv6 address to assign to the System Manager application. The field is optional.</td>
</tr>
<tr>
<td>Default Search List</td>
<td>The search list of domain names. The field is optional.</td>
</tr>
<tr>
<td>NTP Server IP/FQDN</td>
<td>The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The timezone where the System Manager application is located. A list is available where you select the name of the continent and the name of the country.</td>
</tr>
</tbody>
</table>

**Note:**

You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public IP Address</td>
<td>The IPv4 address to enable public access to different interfaces. The field is optional.</td>
</tr>
<tr>
<td>Public Netmask</td>
<td>The IPv4 subnetwork mask to assign to System Manager application. The field is optional.</td>
</tr>
<tr>
<td>Public Gateway</td>
<td>The gateway IPv4 address to assign to the System Manager application. The field is optional.</td>
</tr>
<tr>
<td>Public FQDN</td>
<td>The FQDN to assign to the System Manager application. The field is optional.</td>
</tr>
<tr>
<td>Public IPv6 Address</td>
<td>The IPv6 address to enable public access to different interfaces. The field is optional.</td>
</tr>
<tr>
<td>Public IPv6 Network Prefix</td>
<td>The IPv6 subnetwork mask to assign to System Manager application. The field is optional.</td>
</tr>
<tr>
<td>Public IPv6 Gateway</td>
<td>The gateway IPv6 address to assign to the System Manager application. The field is optional.</td>
</tr>
</tbody>
</table>
### Virtual Hostname

The virtual hostname of the System Manager application.

**Note:**

- The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.
- VFQDN is a mandatory field.
- By default, VFQDN entry gets added in the `/etc/hosts` file during installation. Do not remove VFQDN entry from the `/etc/hosts` file.
- VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value.
- You must keep VFQDN domain value same as of FQDN domain value.
- If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved.
- Secondary Server (Standby mode) IP address value is mapped with VFQDN value in hosts file of Primary server IP address. After Secondary Server is activated, then the IP address gets updated with Secondary Server IP address.
- In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.
- After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:
  1. Log in to System Manager with administrator privilege credentials.
  2. Run the `changeVFQDN` command.

**Important:**

When you run the `changeVFQDN` command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails. To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.

### Virtual Domain

The virtual domain name of the System Manager application.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv3 User Name Prefix</td>
<td>The prefix for SNMPv3 user.</td>
</tr>
<tr>
<td>SNMPv3 User Authentication Protocol</td>
<td>The password for SNMPv3 user authentication.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Password</td>
<td>The password that you retype to confirm the SNMPv3 user authentication protocol.</td>
</tr>
<tr>
<td>SNMPv3 User Privacy Protocol Password</td>
<td>The password for SNMPv3 user privacy.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password that you must provide to confirm the SNMPv3 user privacy protocol.</td>
</tr>
<tr>
<td>SMGR command line user name</td>
<td>The user name of the System Manager CLI user.</td>
</tr>
<tr>
<td>Note:</td>
<td>Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.</td>
</tr>
<tr>
<td>SMGR command line user password</td>
<td>The password for the System Manager CLI user.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password that you retype to confirm the System Manager CLI user authentication.</td>
</tr>
<tr>
<td>Schedule Backup?</td>
<td>• <strong>Yes</strong>: To schedule the backup jobs during the System Manager installation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No</strong>: To schedule the backup jobs later.</td>
</tr>
<tr>
<td>Note:</td>
<td>If you select <strong>No</strong>, the system does not display the remaining fields.</td>
</tr>
<tr>
<td>Backup Server IP</td>
<td>The IP address of the remote backup server.</td>
</tr>
<tr>
<td>Note:</td>
<td>The IP address of the backup server must be different from the System Manager IP address.</td>
</tr>
<tr>
<td>Backup Server Login Id</td>
<td>The login ID of the backup server to log in through the command line interface.</td>
</tr>
<tr>
<td>Backup Server Login Password</td>
<td>The SSH login password to log in to the backup server from System Manager through the command line interface.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password that you reenter to log in to the backup server through the command line interface.</td>
</tr>
<tr>
<td>Backup Directory Location</td>
<td>The location on the remote backup server.</td>
</tr>
<tr>
<td>File Transfer Protocol</td>
<td>The protocol that you can use to create the backup. The values are SCP and SFTP.</td>
</tr>
</tbody>
</table>
### Network and configuration field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Repeat Type</strong></td>
<td>The type of the backup. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>- Hourly</td>
</tr>
<tr>
<td></td>
<td>- Daily</td>
</tr>
<tr>
<td></td>
<td>- Weekly</td>
</tr>
<tr>
<td></td>
<td>- Monthly</td>
</tr>
<tr>
<td><strong>Backup Frequency</strong></td>
<td>The frequency of the backup taken for the selected backup type.</td>
</tr>
<tr>
<td></td>
<td>The system generates an alarm if you do not schedule a System Manager backup every seven days.</td>
</tr>
<tr>
<td><strong>Backup Start Year</strong></td>
<td>The year in which the backup must start. The value must be greater than or equal to the current year.</td>
</tr>
<tr>
<td><strong>Backup Start Month</strong></td>
<td>The month in which the backup must start. The value must be greater than or equal to the current month.</td>
</tr>
<tr>
<td><strong>Backup Start Day</strong></td>
<td>The day on which the backup must start. The value must be greater than or equal to the current day.</td>
</tr>
<tr>
<td><strong>Backup Start Hour</strong></td>
<td>The hour in which the backup must start. The value must be six hours later than the current hour.</td>
</tr>
<tr>
<td><strong>Backup Start Minutes</strong></td>
<td>The minute when the backup must start. The value must be a valid minute.</td>
</tr>
<tr>
<td><strong>Backup Start Seconds</strong></td>
<td>The second when the backup must start. The value must be a valid second.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public</strong></td>
<td>The port number that is mapped to public port group.</td>
</tr>
<tr>
<td></td>
<td>You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.</td>
</tr>
<tr>
<td><strong>Out of Band Management</strong></td>
<td>The port number that you must assign to the Out of Band Management port group. The field is mandatory.</td>
</tr>
</tbody>
</table>

### Enhanced Access Security Gateway (EASG) - EASG User Access

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG</strong></td>
<td>Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks.</td>
</tr>
<tr>
<td></td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>- 1: To enable EASG.</td>
</tr>
<tr>
<td></td>
<td>- 2: To disable EASG.</td>
</tr>
<tr>
<td></td>
<td>Avaya recommends to enable EASG.</td>
</tr>
<tr>
<td></td>
<td>You can also enable EASG after deploying or upgrading the application by using the command: <code>EASGManage --enableEASG</code>.</td>
</tr>
</tbody>
</table>
Customer Root Account

Note:

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using VMware vSphere Web Client.
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Customer Root Account for this Application</td>
<td>Enables or disables the customer root account for the application.</td>
</tr>
<tr>
<td></td>
<td>Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click <strong>Accept</strong>.</td>
</tr>
<tr>
<td></td>
<td>When you accept the root access statement, the system displays the <strong>Customer Root Password</strong> and <strong>Re-enter Customer Root Password</strong> fields.</td>
</tr>
<tr>
<td>Customer Root Password</td>
<td>The root password for the application</td>
</tr>
<tr>
<td>Re-enter Customer Root Password</td>
<td>The root password for the application</td>
</tr>
</tbody>
</table>

Data Encryption

Note:

- From Release 8.1.2, Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized Environment.
- For data encryption, you must use a new encryption capable variant of Release 8.1E OVA.

For more information, see the application-specific Data Privacy Guidelines on the Avaya Support website.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Data Encryption          | Enables or disables the data encryption.  
The options are:  
• 1: To enable the data encryption.  
• 2: To disable the data encryption.  

**Important:**  
• An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa.  
• While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled.  
• **On Solution Deployment Manager:** When the Data Encryption field is set to 1, the system enables the **Encryption Pass-Phrase** and **Re-enter Encryption Pass-Phrase** fields to enter the encryption passphrase.  
• **On vCenter or ESXi:** When the Data Encryption field is set to 1, enter the encryption passphrase in the **Password** and **Confirm Password** fields.                                                                                                                                                                                                                   |
| Encryption Pass-Phrase   | This field is applicable when data encryption is enabled.  
The passphrase for data encryption.  
When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules.  
When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.                                                                                                                                                                                                                              |
<p>| Re-enter Encryption Pass-Phrase | The passphrase for data encryption.                                                                                                                                                                                                                                                                                                                                                                                                                                               |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Encryption Pass-Phrase at Boot-Time</td>
<td>If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default the <strong>Require Encryption Pass-Phrase at Boot-Time</strong> check box is selected.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application.</td>
</tr>
<tr>
<td></td>
<td>If you lose the data encryption passphrase, the only option is to reinstall the OVA.</td>
</tr>
<tr>
<td></td>
<td>If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure.</td>
</tr>
<tr>
<td></td>
<td>You can also set up the remote key server by using the <code>encryptionRemoteKey</code> command after the deployment of the application.</td>
</tr>
</tbody>
</table>
Chapter 7: Post-installation verification

Post-installation steps

Procedure

Recreate all licenses with the new host ID format, and install the new license files.

System Manager on VMware uses a new host ID format for Avaya WebLM server. Therefore, all licenses previously installed becomes invalid. For instructions to install the license file, see Managing licenses in *Administering Avaya Aura® System Manager*.

Verifying the installation of System Manager

About this task

Perform the following verification procedure after you install System Manager Release 8.1.2 and configure System Manager.

Procedure

1. On the web browser, type `https://<fully qualified domain name of System Manager>`, and ensure that the system displays the System Manager web console.

2. On the upper-right corner, click and click About.

   The system displays the About SMGR window with the build details.

3. Verify the System Manager version number.

Installing language pack on System Manager

About this task

After you install, upgrade, or apply a service or a feature pack, run the language pack to get the localization support for the French language.

Note:

After installing the language pack, you cannot uninstall the language pack.
**Procedure**

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.

2. Type `locate LocalizationScript.sh`, and press Enter.

   System Manager displays the path of the localization script.

   **For example:** `/opt/Avaya/Mgmt/8.1.x/CommonConsole/script/LocalizationScript.sh`

3. Type `locate FrenchResourceBundle.zip`, and press Enter.

   The System Manager displays the path of the `FrenchResourceBundle.zip` script.

   **For example:** `/opt/Avaya/Mgmt/8.1.x/CommonConsole/localization/common_console/FrenchResourceBundle.zip`

   This is just an example of the path, the path might vary based on actual path that you get.

4. Type `cd $MGMT_HOME/CommonConsole/script/` to go to the localization script folder.

5. To run the localization script, type `sudo ./LocalizationScript.sh $MGMT_HOME/CommonConsole/localization/common_console/FrenchResourceBundle.zip`.

6. If you are running the data migration through SSH connection, then do not close the SSH session or terminate the connection.

   If you close the SSH session or terminate the connection, System Manager kills the process and the installation fails.

   **Note:**

   During this activity, System Manager restarts the JBoss service. Therefore, the System Manager web console will not be accessible. If System Manager is in the Geographic Redundancy mode then apply these steps on the secondary System Manager server also after secondary server is active.

7. Change the browser language setting to French.

---

**Enhanced Access Security Gateway (EASG) overview**

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.
Managing EASG from CLI

About this task
After deploying or upgrading an Avaya Aura® application, you can enable, disable, or view the status of EASG.

Before you begin
Log in to the application CLI interface.

Procedure
1. To view the status of EASG, run the command: `EASGStatus`.
   The system displays the status of EASG.
2. To enable EASG, do the following:
   a. Run the command: `EASGManage --enableEASG`.
      The system displays the following message.
      By enabling Avaya Services Logins you are granting Avaya access to your system. This is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.
      The product must be registered using the Avaya Global Registration Tool (GRT, see https://grt.avaya.com) to be eligible for Avaya remote connectivity. Please see the Avaya support site (https://support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.
   b. When the system prompts, type `yes`.
      The system displays the message: EASG Access is enabled.
3. To disable EASG, do the following:
   a. Run the command: `EASGManage --disableEASG`.
      The system displays the following message.
      By disabling Avaya Services Logins you are denying Avaya access to your system. This is not recommended, as it can impact Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Services Logins should not be disabled.
   b. When the system prompts, type `yes`.
      The system displays the message: EASG Access is disabled.
Viewing the EASG certificate information

Procedure

1. Log in to the application CLI interface.
2. Run the command: `EASGProductCert --certInfo`.
   
The system displays the EASG certificate details, such as, product name, serial number, and certificate expiration date.

EASG product certificate expiration

The Avaya Aura® application raises an alarm if the EASG product certificate has expired or is about to expire in 365 days, 180 days, or 30 days. To resolve this alarm, the customer must apply the patch for a new certificate or upgrade to the latest release. Else, the customer loses the ability for Avaya to provide remote access support.

If the EASG product certificate expires, EASG access is still possible through the installation of EASG site certificate.

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge/response.

Managing site certificates

Before you begin

1. Obtain the site certificate from the Avaya support technician.
2. You must load this site certificate on each server that the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to `/home/cust` directory, where `cust` is the login ID. The directory might vary depending on the file transfer tool used.
3. Note the location of this certificate and use in place of `installed_pkcs7_name` in the commands.
4. You must have the following before loading the site certificate:
   • Login ID and password
   • Secure file transfer tool, such as WinSCP
   • Site Authentication Factor

Procedure

1. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>.
   b. Save the Site Authentication Factor to share with the technician once on site.

2. To view information about a particular certificate: run the following command:
   • `sudo EASGSiteCertManage --list`: To list all the site certificates that are currently installed on the system.
   • `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.

3. To delete the site certificate, run the following command:
   • `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   • `sudo EASGSiteCertManage --delete all`: To delete all the site certificates that are currently installed on the system.
Chapter 8: Maintenance

Backup and restore

Creating a data backup on a remote server

Before you begin
Ensure that the backup server supports the required algorithms for the System Manager remote backup.

System Manager requires password authentication to enable the remote backup servers for successful backup.

⚠️ Note:
System Manager does not support authentication mechanisms, such as Keyboard-Interactive and public key-based support.

Procedure
1. On the System Manager Web console, click Services > Backup and Restore.
2. On the Backup and Restore page, click Backup.
4. Perform one of the following:
   • Perform the following:
     a. In the File transfer protocol field, click SCP or SFTP.
     b. Enter the remote server IP, remote server port, user name, password, and name and the path of the backup file that you create.
   • Select the Use Default check box.

⚠️ Important:
To use the Use Default option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For Use Default, on the SMGR Element Manager page, you can click Services > Configurations and navigate to Settings > SMGR > SMGR Element Manager.
5. (Optional) To create encrypted backup using encryption password, do the following:
   a. Deselect the **Use Global Backup Encryption Password** check box.
      System Manager displays the following fields:
      - **Backup Encryption Password**
      - **Confirm Backup Encryption Password**
   b. In **Backup Encryption Password**, type the encryption password.
   c. In **Confirm Backup Encryption Password**, retype the encryption password.
      You must remember the password to restore the backup.

6. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: **Backup job submitted successfully. Please check the status detail below!!**

---

### Creating a data backup on a local server

**About this task**

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption on the Services > Configurations > Settings > SMGR > SMGR Element Manager page.

**Procedure**

1. On the System Manager web console, click **Services > Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In **File name**, type the backup file that you want to create.
5. (Optional) To create encrypted backup using encryption password, do the following:
   a. Deselect the **Use Global Backup Encryption Password** check box.
      System Manager displays the following fields:
      - **Backup Encryption Password**
      - **Confirm Backup Encryption Password**
   b. In **Backup Encryption Password**, type the encryption password.
   c. In **Confirm Backup Encryption Password**, retype the encryption password.
      You must remember the password to restore the backup.
6. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: **Backup job submitted successfully. Please check the status detail below!!**
Restoring a backup from a remote server

About this task

Note:

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

To restore the original system at any point of time, you must restore the backup on the same release and the same software patch of that of the original System Manager. For example, if you have created a backup of System Manager xyz with 1234 software patch installed, System Manager on which you restore the backup must run xyz that has 1234 software patch installed.

If the System Manager release on which you restore the backup does not match, the restore operation fails.

Procedure

1. On the System Manager web console, click Services > Backup and Restore.
2. On the Backup and Restore page, click Restore.
4. (Optional) To restore encrypted backup using encryption password, do the following:
   a. Deselect the Use Global Backup Encryption Password check box.
      System Manager displays the Backup Encryption Password field.
   b. In Backup Encryption Password, type the encryption password.
5. To specify the file name for the restore operation, perform one of the following:
   • Click the Backup List tab, and select a file name.
      Use this method if the path of the backup file on the remote server is valid, and the credentials used while creating the backup file is unaltered.
   • Click the Parameterized Restore tab, enter a valid file name, the file transfer protocol, the remote server IP address, remote server port, user name, and the password to access the remote computer in the respective fields.

   Note:

   System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

   • Click the Parameterized Restore tab, select the Use Default check box.

   Important:

   To use the Use Default option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For Use Default, on the SMGR Element Manager page,
you can click Services > Configurations and navigate to Settings > SMGR > SMGR Element Manager.

6. Click Restore.

On the Restore Confirmation page, the system displays the following message:

The Restore operation will terminate all sessions and no services will be available until the operation completes. So, the System Manager console will not be available for approximately 45 minutes but this time may vary based on Database size. Click on Continue to go ahead with the Restore operation or click on Cancel to abort the operation.

7. Click Continue.

The system logs you out of the System Manager web console and then shuts down.

**Result**

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

---

**Restoring data backup from a local server**

**About this task**

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption on the Services > Configurations > Settings > SMGR > SMGR Element Manager page.

⚠️ **Note:**

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

**Procedure**

1. On the System Manager web console, click Services > Backup and Restore.
2. On the Backup and Restore page, click Restore.
3. On the Restore page, click Local.
4. In the **File name** field, type the file name that you must restore.
   
   If the file name does not appear in the list, specify the absolute path to the backup file and the file name that you must restore.

   ⚠️ **Note:**

   System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.
5. **(Optional)** To restore encrypted backup using encryption password, do the following:
   a. Deselect the **Use Global Backup Encryption Password** check box.
      
      System Manager displays the **Backup Encryption Password** field.
   b. In **Backup Encryption Password**, type the encryption password.

6. Click **Restore**.

   On the Restore Confirmation page, the system displays the following message:
   
   The Restore operation will terminate all sessions and no services will be available until the operation completes. So, the System Manager console will not be available for approximately 45 minutes but this time may vary based on Database size. Click on Continue to go ahead with the Restore operation or click on Cancel to abort the operation.

7. Click **Continue**.

   The system logs you out of the System Manager web console and then shuts down.

**Result**

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

---

**Backup and Restore field descriptions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td>The type of operation. The values are:</td>
</tr>
<tr>
<td></td>
<td>• Backup</td>
</tr>
<tr>
<td></td>
<td>• Restore</td>
</tr>
<tr>
<td><strong>File Name</strong></td>
<td>• For the backup operation, the name of the backup file.</td>
</tr>
<tr>
<td></td>
<td>• For the restore operation, the name of the backup file that was used for</td>
</tr>
<tr>
<td></td>
<td>the restore.</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>• For the backup operation, the path of the backup file.</td>
</tr>
<tr>
<td></td>
<td>• For the restore operation, the path of the backup file that was used for</td>
</tr>
<tr>
<td></td>
<td>the restore.</td>
</tr>
</tbody>
</table>

*Table continues…*
### Table: Status Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Description</td>
<td>The error details of the backup or restore operation that has failed.</td>
</tr>
<tr>
<td>Operation Time</td>
<td>The time of the backup or restore operation.</td>
</tr>
<tr>
<td>Operation Type</td>
<td>Defines whether the backup or restore operation is local or remote.</td>
</tr>
<tr>
<td>User</td>
<td>The user who performed the operation.</td>
</tr>
</tbody>
</table>

### Table: Button Description

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>Opens the Backup page from where you can back up the System Manager data.</td>
</tr>
<tr>
<td>Restore</td>
<td>Opens the Restore page from where you can restore the data to System Manager.</td>
</tr>
</tbody>
</table>

---

## Installing the System Manager service pack or patch from CLI

### Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the 📘 icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- Take a snapshot of the System Manager virtual machine.

### Procedure

Type `SMGRPatchdeploy <absolute path to the service pack or patch for System Manager>`. 

If you do not provide the name of the patch or service pack, the console displays menu items. Provide the absolute path to the patch or service pack that you want to install for System Manager.
Next steps
Delete the snapshot after you verify the System Manager functionality.

Viewing the job history of virtual machine operations

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. On the desktop, click the SDM icon (SDM icon), and then click Application Management.
3. In the lower pane, click Job History.
4. On the Job History page, in Operation, select one or more operations.
5. Click Submit.
   The page displays the details of jobs that you selected.

Related links
Job History field descriptions on page 52

Job History field descriptions

<table>
<thead>
<tr>
<th>Name/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>The operation that is performed on a virtual machine. You can select one or more operations that are performed on a virtual machine, such as host restart, virtual machine deployment, and patch installation.</td>
</tr>
<tr>
<td>Submit</td>
<td>Provides details of jobs that you selected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>The unique name of the virtual machine management job.</td>
</tr>
<tr>
<td>IP/FQDN</td>
<td>The IP address or host name of the virtual machine or the host where the operation is performed.</td>
</tr>
<tr>
<td>Operation</td>
<td>The operation performed on the virtual machine or host. For example, host refresh, virtual machine deployment, and patch installation.</td>
</tr>
</tbody>
</table>

Table continues…
### Changing the IP address, FQDN, DNS, Gateway, or Netmask address of System Manager from CLI

#### About this task
Use this procedure to change the network configuration parameters for Public interface and Management interface when OOBM is enabled.

**Important:**
- Do not change the network settings from vSphere Web Client when the virtual machine is in the power off state.
- FQDN value must be unique and different from the virtual FQDN value of System Manager.

#### Before you begin
- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the `Console` icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- Create the System Manager virtual machine snapshot.

**Note:**
Delete the snapshot after the System Manager operation is complete.

#### Procedure
1. To configure Management network parameters, type `changeIPFQDN -IP <IPv4 address> -FQDN <FQDN> -GATEWAY <Gateway IPv4 address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH <search list of domain names> -IPV6 <IPv6 address> -IPV6GW <IPv6 Gateway address> -IPV6PREFIX <IPv6 prefix>.

For information, see `changeIPFQDN`. 

---

**Related links**
- [Viewing the job history of virtual machine operations](#) on page 52

---

**Table: Status, Start Time, End Time**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the job.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The start time of the job.</td>
</tr>
<tr>
<td>End Time</td>
<td>The end time of the job.</td>
</tr>
</tbody>
</table>
2. To configure Public network parameters, type `changePublicIPFQDN -IP <IP address> -PublicFQDN <FQDN> -PublicGATEWAY <Gateway IP address> -PublicNETMASK <Netmask address>.

   For information, see `changePublicIPFQDN`.

Next steps

Get new licenses from PLDS containing the new host ID and install the new licenses.

After you change the IP address of System Manager, the system generates a new host ID for WebLM server that System Manager hosts. Therefore, all previously installed licenses become invalid.

For instructions to install a license file, see Managing Licenses in *Administering Avaya Aura® System Manager*.

Related links

- [changeIPFQDN command](#) on page 54
- [changePublicIPFQDN command](#) on page 55

### changeIPFQDN command

Use the `changeIPFQDN` command to change the Management IP address when Out of Band Management is enabled. With this command you can change the IP address, FQDN, DNS address, Gateway, Netmask address for Management network configuration of System Manager, and the search list for the DNS address.

**Note:**

On the System Manager Release 7.1 and later system, if you change the IP Address of System Manager by using the `changeIPFQDN` command, the system changes the host ID of System Manager and invalidate the existing installed license file. Therefore, you must reinstall the license file on System Manager after changing the IP Address of System Manager.

To change the Public IP address when Out of Band Management is enabled, use the `changePublicIPFQDN` command

#### Syntax

```
changeIPFQDN -IP < > -FQDN < > -GATEWAY < > -NETMASK < > -DNS < > -SEARCH < > -IPv6 < > -IPv6GW < > -IPv6PREFIX < >
```

<table>
<thead>
<tr>
<th>#</th>
<th>Option</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP</td>
<td>The new Management IPv4 address of System Manager.</td>
<td><code>changeIPFQDN -IP 10.11.12.13</code></td>
</tr>
<tr>
<td>2</td>
<td>FQDN</td>
<td>The new Management FQDN of System Manager.</td>
<td><code>changeIPFQDN -FQDN a.mydomain.smgr.com</code></td>
</tr>
<tr>
<td>3</td>
<td>GATEWAY</td>
<td>The new Management Gateway IPv4 address of System Manager.</td>
<td><code>changeIPFQDN -GATEWAY 10.11.1.1</code></td>
</tr>
</tbody>
</table>

*Table continues...*
### Option Description

<table>
<thead>
<tr>
<th>#</th>
<th>Option</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>NETMASK</td>
<td>The new Management netmask address of System Manager.</td>
<td>changeIPFQDN -NETMASK 255.255.203.0</td>
</tr>
<tr>
<td>5</td>
<td>DNS</td>
<td>The new Management DNS address of System Manager.</td>
<td>changeIPFQDN -DNS 10.11.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can provide multiple DNS addresses. Separate each address by a comma.</td>
<td>changeIPFQDN -DNS 10.11.12.5,10.11.12.3</td>
</tr>
<tr>
<td>6</td>
<td>SEARCH</td>
<td>The new search list of domain names.</td>
<td>changeIPFQDN -SEARCH smgr.com</td>
</tr>
<tr>
<td></td>
<td>IPV6GW</td>
<td>The new Management Gateway IPv6 address of System Manager.</td>
<td>changeIPFQDN -IPV6GW 2001:b00d::1</td>
</tr>
<tr>
<td>8</td>
<td>IPV6PREFIX</td>
<td>The new Management netmask prefix of System Manager. The default value is 64.</td>
<td>changeIPFQDN -IPV6PREFIX 64</td>
</tr>
</tbody>
</table>

### Example

You can provide options in any combination that the system supports:

```
changeIPFQDN -IP 10.11.y.z -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1 -NETMASK 255.255.255.0 -DNS 10.11.1.2 -SEARCH platform.avaya.com
```

```
changeIPFQDN -IP 10.11.y.z
```

```
```

### Related links

- Changing the IP address, FQDN, DNS, Gateway, or Netmask address of System Manager from CLI on page 53

---

### changePublicIPFQDN command

Use the `changePublicIPFQDN` command to change the Public IP address when Out of Band Management is enabled. With this command, you can change the IP address, FQDN, Gateway, and Netmask address for Public network configuration of System Manager.

To change the Management IP address when Out of Band Management is enabled, use the `changeIPFQDN` command.

### Syntax

```
changePublicIPFQDN -publicIP < > -publicFQDN < > -publicGATEWAY < > -publicNETMASK < >
```
<table>
<thead>
<tr>
<th>#</th>
<th>Option</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>publicIP</td>
<td>The new Public IPv4 address of System Manager.</td>
<td>changePublicIPFQDN -IP 10.11.12.13</td>
</tr>
<tr>
<td>3</td>
<td>IPV6GW</td>
<td>The new public IPv6 Gateway address of System Manager.</td>
<td>changePublicIPFQDN -IPV6GW 2001:b00d::1</td>
</tr>
<tr>
<td>4</td>
<td>IPV6PREFIX</td>
<td>The new public IPv6 Prefix address of System Manager.</td>
<td>changePublicIPFQDN -IPV6PREFIX 64</td>
</tr>
<tr>
<td>5</td>
<td>publicFQDN</td>
<td>The new Public FQDN of System Manager.</td>
<td>changePublicIPFQDN -FQDN a.mydomain.smgr.com</td>
</tr>
<tr>
<td>6</td>
<td>publicGATEWAY</td>
<td>The new Public Gateway IPv4 address of System Manager.</td>
<td>changePublicIPFQDN -GATEWAY 10.11.1.1</td>
</tr>
<tr>
<td>7</td>
<td>publicNETMASK</td>
<td>The new Public netmask address of System Manager.</td>
<td>changePublicIPFQDN -NETMASK 255.255.203.0</td>
</tr>
</tbody>
</table>

**Example**

You can provide options in any combination that the system supports:

```shell
changePublicIPFQDN -publicIP 10.11.y.z -publicFQDN a.domain.weblm.com -publicGATEWAY 10.11.1.1 -publicNETMASK 255.255.255.0
```

**Related links**

[Changing the IP address, FQDN, DNS, Gateway, or Netmask address of System Manager from CLI](#) on page 53
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>changeIPFQDN</td>
<td>• -IP &lt;new Management interface or Out of Band Management IP address for System Manager&gt;</td>
<td>Updates the existing Management interface or Out of Band Management IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value.</td>
<td>• changeIPFQDN - IP &lt;new IP address&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• -FQDN &lt;new Management or Out of Band Management fully qualified domain name for System Manager&gt;</td>
<td>Note: On the System Manager Release 7.1 and later system, if you change the IP Address of System Manager by using the changeIPFQDN command, the system changes the host ID of System Manager and invalidate the existing installed license file. Therefore, you must reinstall the license file on System Manager after changing the IP Address of System Manager.</td>
<td>• changeIPFQDN - FQDN &lt;new fully qualified domain name&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• -GATEWAY &lt;new Management interface or Out of Band Management Gateway address for System Manager&gt;</td>
<td></td>
<td>• changeIPFQDN - IP &lt;new IP address&gt; - GATEWAY &lt;new Gateway address for System Manager&gt; - SEARCH &lt;new search list for DNS address&gt;</td>
</tr>
<tr>
<td>#</td>
<td>Command</td>
<td>Parameters</td>
<td>Description</td>
<td>Usage</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>changePublicIPFQDN</td>
<td>• -publicIP &lt;new IP address for System Manager&gt;</td>
<td>Updates the existing Public IP address, FQDN, Gateway, and Netmask with the new value.</td>
<td>• changePublicIPFQDN -publicIP &lt;new Public IP address&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• -publicFQDN &lt;new fully qualified domain name for System Manager&gt;</td>
<td></td>
<td>• changePublicIPFQDN -publicFQDN &lt;new fully qualified domain name for public interface&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• -publicGATEWAY &lt;new Gateway address for System Manager&gt;</td>
<td></td>
<td>• changePublicIPFQDN -publicGATEWAY &lt;new Public Gateway address for System Manager&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• -publicNETMASK &lt;new netmask address for System Manager&gt;</td>
<td></td>
<td>• changePublicIPFQDN -publicNETMASK &lt;new Netmask address for System Manager&gt;</td>
</tr>
<tr>
<td>3</td>
<td>upgradeSMGR</td>
<td>&lt;absolute path to the dmutility.bin&gt; -m -v</td>
<td>Upgrades System Manager using the data migration utility.</td>
<td>upgradeSMGR dmutility *.bin -m -v</td>
</tr>
<tr>
<td>4</td>
<td>SMGRPatchdeploy</td>
<td>&lt;absolute path to the System Manager service pack or the software patch&gt;</td>
<td>Installs the software patch or the service pack for System Manager.</td>
<td>SMGRPatchdeploy &lt;absolute path to SMGRservicepackName&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✴ Note: Copy the System Manager service pack or patches that you must install to /swLibrary.</td>
</tr>
<tr>
<td>5</td>
<td>configureTimeZone</td>
<td>Time zone that you select</td>
<td>Configures the time zone with the value that you select.</td>
<td>configureTimeZone Select a time zone. For example, America/Denver</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>configureNTP</td>
<td>&lt;IP address of NTP server&gt;</td>
<td>Configures the NTP server details.</td>
<td>configureNTP &lt;IP address of NTP server&gt; Separated IP addresses or hostnames of NTP servers with commas (,).</td>
</tr>
<tr>
<td>7</td>
<td>createCA</td>
<td></td>
<td>Creates a new Certificate Authority by using SHA2 signing algorithm and 2048 key size. For more information, see, Creating a new Certificate Authority by using SHA2 signing algorithm and 2048 key size.</td>
<td>createCA You must provide the desired Common Name (CN)</td>
</tr>
<tr>
<td>8</td>
<td>configureOOBM</td>
<td></td>
<td>Enables or disables the Out of Band Management configuration.</td>
<td>• To enable Out of Band Management: configureOOBM -- EnableOOBM • To disable Out of Band Management: configureOOBM -- DisableOOBM</td>
</tr>
<tr>
<td>9</td>
<td>enableOOBMMultiTenancy</td>
<td></td>
<td>If Out of Band Management and MultiTenancy are enabled on system, use this command to provision tenant administrators to available on public interface.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>setSecurityProfile</td>
<td></td>
<td>Enabling the commercial and military grade hardening.</td>
<td>• Enabling commercial grade hardening: setSecurityProfile --enable-commercial-grade • Enabling military grade hardening: setSecurityProfile --enable-military-grade</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
</table>
| 11 | EASGManage          |            | Enables or disables EASG.          | • EASGManage -- enableEASG  
    |                     |            |                                    | • EASGManage -- disableEASG                                         |
| 12 | EASGStatus          |            | Displays the status of EASG.       |                                                                       |
| 13 | EASGProductCert     |            | Displays the EASG certificate details. | EASGProductCert --certInfo                       |
| 14 | EASGSiteCertManage  |            | To manage EASG Certificates.       |                                                                       |
| 15 | editHosts           |            | To modify the /etc/hosts file.     |                                                                       |
| 16 | swversion           |            | Displays the System Manager software information. |                                                                       |
| 17 | changeVFQDN         |            | To change the System Manager Virtual FQDN. | changeVFQDN  
    |                     |            |                                    | Type the System Manager Virtual FQDN.  
    |                     |            |                                    | Note:  
    |                     |            |                                    | When you run the changeVFQDN command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails. To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering-specific Administering document.  
<pre><code>|                     |            |                                    | Table continues...                                                  |
</code></pre>
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
</table>
| 18 | pairIPFQDN |            | Changing the IP address and FQDN on the secondary System Manager server when the secondary is in the standby or active mode. | • If you changed both the IP address and FQDN of primary server, type the following on the secondary server:  
  #sh $MGMT_HOME/utils/ ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the primary server> -NEWIP <New IP of the primary server> -OLDFQDN <Old FQDN of the primary server> -NEWFQDN <New FQDN of the primary server>  
  • If you changed the IP address of primary server, type the following on secondary server:  
  #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the primary server> -NEWIP <New IP of the primary server>  
  • If you changed FQDN of primary server, type the following on secondary server:  
  #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN <Old FQDN of primary server> -NEWFQDN <New FQDN of primary server> |

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>smgr</td>
<td></td>
<td>Starts, stops, and checks the status of Jboss service.</td>
<td>smgr start/stop/status</td>
</tr>
<tr>
<td>20</td>
<td>smgr-db</td>
<td></td>
<td>Starts, stops, and checks the status of postgresql.service.</td>
<td>smgr-db start/stop/status</td>
</tr>
<tr>
<td>21</td>
<td>toggleWeblmOldcert</td>
<td></td>
<td>Replaces identity certificate with old certificate.</td>
<td>toggleWeblmOldcert</td>
</tr>
<tr>
<td>22</td>
<td>getUserAuthCert</td>
<td></td>
<td>Generates a user specific certificate for System Manager to facilitate certificate-based authentication.</td>
<td></td>
</tr>
</tbody>
</table>
| 23 | changeCipherSuiteList  |                     | Configures cipher suite mode for System Manager                            | • To configure strict cipher suite list: changeCipherSuiteList STRICT_CIPHER_SUITE_LIST  
|    |                        |                     |                                                                             | • To configure relax cipher suite list changeCipherSuiteList RELAX_CIPHER_SUITE_LIST |
|    |                        |                     |                                                                             |                                                                     |
| 24 | collectLogs            |                     | Collects the required logs.                                                | • To collect all the logs: collectLogs                                
|    |                        |                     |                                                                             | • To collect all the logs along with backup: collectLogs -Db          
|    |                        |                     |                                                                             | • To collect all the logs along with CND data: collectLogs -CND        |
| 25 | rebootVM               |                     | Reboots the System Manager virtual machine.                               | Type y or n to reboot the System Manager virtual machine.             |

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>powerOffVM</td>
<td></td>
<td>Power off the System Manager virtual machine.</td>
<td>Type y or n to power off the System Manager virtual machine.</td>
</tr>
<tr>
<td>27</td>
<td>sudo /bin/ systemctl (parameter) snmpd</td>
<td>start/stop/restart/status</td>
<td>To start or stop, and to check status of the SNMP service.</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>sudo /bin/ systemctl (parameter) spiritAgent</td>
<td>start/stop/restart/status</td>
<td>To start or stop, and to check status of the Spirit Agent service.</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>sudo /bin/ systemctl (parameter) cnd</td>
<td>start/stop/restart/status</td>
<td>To start or stop, and to check status of the CND service.</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>encryptionPassphrase</td>
<td>[add</td>
<td>change</td>
<td>remove</td>
</tr>
</tbody>
</table>

- **encryptionPassphrase add**: To add encryption passphrase.
- **encryptionPassphrase change**: To change existing encryption passphrase.
- **encryptionPassphrase remove**: To remove encryption passphrase.
- **encryptionPassphrase list**: To display the encryption passphrase and slot assignment.

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>encryptionRemoteKey</td>
<td>[add</td>
<td>remove</td>
<td>list]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• encryptionRemoteKey remove: To remove remote key server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• encryptionRemoteKey list: To display the remote key server and slot assignment.</td>
</tr>
<tr>
<td>32</td>
<td>encryptionLocalKey</td>
<td>[enable</td>
<td>disable]</td>
<td>To enable and disable the local key store.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• encryptionLocalKey disable: To disable local key store.</td>
</tr>
<tr>
<td>33</td>
<td>encryptionStatus</td>
<td></td>
<td>Displays information about encryption on the system.</td>
<td>encryptionStatus displays information about encryption on the system.</td>
</tr>
<tr>
<td>34</td>
<td>updateLogRetention.sh</td>
<td>[-p] [-v] [maxRetentionTime]</td>
<td>Manages the log retention time.</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>pruneAllLogs.sh</td>
<td>[-b] [-t] [-v] [-h] [maxRetentionTime]</td>
<td>Manages the deletion of log files.</td>
<td></td>
</tr>
</tbody>
</table>

## Generating test alarms

### Test alarms

You can generate a test alarm and a clear event corresponding to the generated test alarm. The severity level of the test alarm is minor. The clear event generated has no definite severity level. The clear event updates the status of the test alarms from Raised to Cleared. If Secure Access Link (SAL) Enterprise is configured to forward alarms to Avaya Data Center (ADC), the system also forwards the test alarm and the clear event for the test alarm to the ADC.
### Generating test alarms

**Test Alarm Event**

<table>
<thead>
<tr>
<th>Test Alarm property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm.Message</td>
<td>Test alarm</td>
</tr>
<tr>
<td>Alarm.Severity</td>
<td>Minor</td>
</tr>
<tr>
<td>Alarm.Status</td>
<td>Raised</td>
</tr>
<tr>
<td>Alarm.Log.ProcessName</td>
<td>TESTALARM</td>
</tr>
<tr>
<td>Alarm.Log.EventCode</td>
<td>TEST_ALARM_GEN_0001</td>
</tr>
</tbody>
</table>

**Test Clear Event**

<table>
<thead>
<tr>
<th>Test Clear Event property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm.Message</td>
<td>Clear event for test alarm</td>
</tr>
<tr>
<td>Alarm. Severity</td>
<td>Indeterminate</td>
</tr>
<tr>
<td>Alarm.Status</td>
<td>Cleared</td>
</tr>
<tr>
<td>Alarm.Log.ProcessName</td>
<td>TESTALARM</td>
</tr>
<tr>
<td>Alarm.Log.EventCode</td>
<td>TEST_ALARM_CLR_0000</td>
</tr>
</tbody>
</table>

**Related links**

- Generating the test alarm from the web console on page 65
- Generating the test alarm from CLI on page 66

**Generating the test alarm from the web console**

**About this task**

You can generate test alarms from the System Manager web console for agents, hosts, or elements that are installed with Serviceability Agents running version 6.3.2.4-6706-SDK-1.0 or later.

**Procedure**

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Serviceability Agents**.
3. In the **Agent List** section, select one or more agents for which you want to generate alarms.
4. Click **Generate Test Alarm**.
   
   The system generates the alarm.
5. To view the alarm, click **Events > Alarms**.
   
   To view the details of the alarm, wait until the system displays the alarms on the Alarming page.
Generating the test alarm from CLI

Procedure

1. Log in to the computer on which you installed System Manager.

2. At the command prompt, perform the following:
   a. To check the status of SAL Agent, type `service spiritAgent status` and press Enter.
      
      The system displays SPIRIT Agent is running.
      
      ✷ Note:
      
      If the system displays SPIRIT Agent is not running, then start SAL Agent.
   b. To start SAL Agent, type `service spiritAgent start` and press Enter.

      The `utils` directory contains SAL Agent command line utilities.

3. To navigate to the `utils` directory, at the prompt, type `cd $SPIRIT_HOME/scripts/utils/` and press Enter.

4. Perform one of the following:
   • To generate the test alarm for System Manager, type `sh generateTestAlarm.sh`, and press Enter.
   • To generate the clear alarm for System Manager, type `sh generateTestAlarm.sh -c`, and press Enter.

5. Perform one of the following:
   • To generate the test alarm for a different product, type `sh generateTestAlarm.sh -l LOG_LOCATION -p PRODUCT_TYPE`, and press Enter.
   • To generate the clear alarm for a different product, type `sh generateTestAlarm.sh -c -l LOG_LOCATION -p PRODUCT_TYPE`, and press Enter.

Here, `LOG_LOCATION` is one of the log files that the SAL agent tails for this product, and `PRODUCT_TYPE` is the log product type that you configured for this product in the SAL agent.

Network Management Systems Destinations

The Session Manager serviceability agent can send SNMPv2c/v3 traps or informs for alarms to multiple destinations such as:

• SAL Gateway, mandatory trap destination
• System Manager trap listener
• Third-party NMS
• Avaya SIG server

SAL Gateway is a mandatory trap destination for traps sent to Avaya Services for system maintenance. SAL Gateway converts the traps to alarms and forwards the alarms to the Avaya Data Centre for ticketing purposes. Therefore, after you install or upgrade from release earlier than 6.2 to Session Manager Release 6.2 or later, you must configure the serviceability agent with SAL Gateway as a trap destination. You can configure the serviceability agent by using the System Manager web console. You must also configure Session Manager as a managed device on SAL Gateway.

Optionally, you can configure any third-party Network Management Systems (NMS) as a trap destination. Based on customer requirements, Avaya technicians can also configure the Avaya SIG server as another trap destination.

For upgrades from Release 6.2 or later, the configuration of the serviceability agent persists through the Session Manager upgrade.

You can add an NMS destination using the System Manager web console. To add an NMS destination, you must create a target profile for the NMS destination and then attach the target profile to a serviceability agent. For more information on activating agents and attaching target profiles, see Managing Serviceability Agents in Administering Avaya Aura® System Manager.

---

**Adding Network Management Systems Destination**

You can add an NMS destination using the System Manager web console. To add an NMS destination, you must create a target profile for the NMS destination and then attach the target profile to a serviceability agent. For more information on activating agents and attaching target profiles, see “Managing Serviceability Agents” in Administering Avaya Aura® System Manager.
Chapter 9: Resources

System Manager documentation

The following table lists the documents related to System Manager. Download the documents from the Avaya Support website at [http://support.avaya.com](http://support.avaya.com).

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Avaya Aura® System Manager Overview and Specification</em></td>
<td>Understand high-level product features and functionality.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td><em>Administering Avaya Aura® System Manager</em></td>
<td>Administering System Manager applications and install patches on System Manager applications.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td><em>Avaya Aura® System Manager Certificate Management</em></td>
<td>Understand certificate management.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td><strong>Using</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Using the Solution Deployment Manager client</em></td>
<td>Deploy System Manager applications and install patches on System Manager applications.</td>
<td>System administrators</td>
</tr>
<tr>
<td><em>Avaya Aura® System Manager Solution Deployment Manager Job-Aid</em></td>
<td>Deploy System Manager applications and install patches on System Manager applications.</td>
<td>System administrators</td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Upgrading Avaya Aura® System Manager</em></td>
<td>Upgrade the Avaya Aura® System Manager application to Release 8.1.x.</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td><em>Deploying Avaya Aura® System Manager in Virtual Appliance</em></td>
<td>Deploy System Manager applications in Virtual Appliance</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td><em>Deploying Avaya Aura® System Manager in Virtualized Environment</em></td>
<td>Deploy System Manager applications in Virtualized Environment</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td><em>Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment</em></td>
<td>Deploy System Manager applications in Infrastructure as a Service Environment</td>
<td>Implementation personnel</td>
</tr>
</tbody>
</table>

Table continues…

Comments on this document? infodev@avaya.com
# Deploying Avaya Aura® System Manager in Software-Only Environment

## Description
Deploy System Manager applications in Software-Only Environment

## Audience
Implementation personnel

## Maintenance and Troubleshooting

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avaya Aura® System Manager Fault Management and monitoring using SNMP</strong></td>
<td>Monitor System Manager using SNMP.</td>
<td>System administrators and IT personnel</td>
</tr>
<tr>
<td><strong>Troubleshooting Avaya Aura® System Manager</strong></td>
<td>Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.</td>
<td>System administrators and IT personnel</td>
</tr>
</tbody>
</table>

## Finding documents on the Avaya Support website

**Procedure**

1. Go to [https://support.avaya.com](https://support.avaya.com).
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.
   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.
   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

## Accessing the port matrix document

**Procedure**

1. Go to [https://support.avaya.com](https://support.avaya.com).
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product > Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.

6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**
   The list displays the product-specific Port Matrix document.

7. Click **Enter**.

---

**Avaya Documentation Center navigation**

Customer documentation for some programs is now available on the Avaya Documentation Center website at [https://documentation.avaya.com](https://documentation.avaya.com).

⚠️ **Important:**

For documents that are not available at Avaya Documentation Center, click **More Sites > Support** on the top menu to open [https://support.avaya.com](https://support.avaya.com).

Using the Avaya Documentation Center, you can:

- Search for content using one of the following:
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release.
  - From **Products & Solutions**, select a solution and product, and select the appropriate document from the list.
- Sort documents on the search results page by last updated dated and relevance.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (⭐).

Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

- Add yourself as a watcher by using the **Watch** icon (👁️).

Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.
As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

**Note:**
Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

## Training

The following courses are available on the Avaya Learning website at [http://www.avaya-learning.com](http://www.avaya-learning.com). After you log into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

<table>
<thead>
<tr>
<th>Course code</th>
<th>Course title</th>
</tr>
</thead>
<tbody>
<tr>
<td>20460W</td>
<td>Virtualization and Installation Basics for Avaya Team Engagement Solutions</td>
</tr>
<tr>
<td>20970W</td>
<td>Introducing Avaya Device Adapter</td>
</tr>
<tr>
<td>20980W</td>
<td>What's New with Avaya Aura® Release 8.1</td>
</tr>
<tr>
<td>71200V</td>
<td>Integrating Avaya Aura® Core Components</td>
</tr>
<tr>
<td>72200V</td>
<td>Supporting Avaya Aura® Core Components</td>
</tr>
<tr>
<td>20130V</td>
<td>Administering Avaya Aura® System Manager Release 8.1</td>
</tr>
<tr>
<td>21450V</td>
<td>Administering Avaya Aura® Communication Manager Release 8.1</td>
</tr>
</tbody>
</table>

## Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

**About this task**

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to [https://support.avaya.com/](https://support.avaya.com/) and do one of the following:
  - In **Search**, type **Avaya Mentor Videos**, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.
The Video content type is displayed only when videos are available for that product. In the right pane, the page displays a list of available videos.

• To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

⚠️ Note: Videos are not available for all products.

---

**Support**

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

**Related links**

Using the Avaya InSite Knowledge Base on page 72

---

**Using the Avaya InSite Knowledge Base**

The Avaya InSite Knowledge Base is a web-based search engine that provides:

• Up-to-date troubleshooting procedures and technical tips
• Information about service packs
• Access to customer and technical documentation
• Information about training and certification programs
• Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

2. Log on to the Avaya website with a valid Avaya user ID and password.
   The system displays the Avaya Support page.
3. Click **Support by Product > Product-specific Support**.

4. In **Enter Product Name**, enter the product, and press **Enter**.

5. Select the product from the list, and select a release.

6. Click the **Technical Solutions** tab to see articles.

7. Select relevant articles.

**Related links**

[Support](#) on page 72
Appendix A: System Manager RPMs

- abrt.x86_64
- abrt-addon-ccpp.x86_64
- abrt-addon-kerneloops.x86_64
- abrt-addon-pstoreoops.x86_64
- abrt-addon-python.x86_64
- abrt-addon-vmcore.x86_64
- abrt-addon-xorg.x86_64
- abrt-cli.x86_64
- abrt-console-notification.x86_64
- abrt-dbus.x86_64
- abrt-libs.x86_64
- abrt-python.x86_64
- abrt-tui.x86_64
- acl.x86_64
- aic94xx-firmware.noarch
- aide.x86_64
- alsa-firmware.noarch
- alsa-lib.x86_64
- alsa-tools-firmware.x86_64
- at.x86_64
- atk.x86_64
- attr.x86_64
- audit.x86_64
- audit-libs.x86_64
- audit-libs-python.x86_64
May 2020

Deploying Avaya Aura® System Manager in Software-Only Environment

Comments on this document? infodev@avaya.com
• cracklib-dicts.x86_64
• cronie.x86_64
• cronie-anacron.x86_64
• crontabs.noarch
• cryptsetup.x86_64
• cryptsetup-libs.x86_64
• csync2.x86_64
• cups-libs.x86_64
• curl.x86_64
• cyrus-sasl.x86_64
• cyrus-sasl-lib.x86_64
• cyrus-sasl-plain.x86_64
• dbus.x86_64
• dbus-glib.x86_64
• dbus-libs.x86_64
• dbus-python.x86_64
• dejavu-fonts-common.noarch
• dejavu-sans-fonts.noarch
• dejavu-sans-mono-fonts.noarch
• desktop-file-utils.x86_64
• device-mapper.x86_64
• device-mapper-event.x86_64
• device-mapper-event-libs.x86_64
• device-mapper-libs.x86_64
• device-mapper-persistent-data.x86_64
• dhclient.x86_64
• dhcp-common.x86_64
• dhcp-libs.x86_64
• diffutils.x86_64
• dmidecode.x86_64
• dmraid.x86_64
• dmraid-events.x86_64
• dos2unix.x86_64
• dracut.x86_64
• dracut-config-rescue.x86_64
• dracut-fips.x86_64
• dracut-network.x86_64
• dyninst.x86_64
• e2fsprogs.x86_64
• e2fsprogs-libs.x86_64
• ebtables.x86_64
• elfutils.x86_64
• elfutils-default-yama-scope.noarch
• elfutils-libelf.x86_64
• elfutils-libs.x86_64
• emacs-filesystem.noarch
• ethtool.x86_64
• expat.x86_64
• expect.x86_64
• file.x86_64
• file-libs.x86_64
• filesystem.x86_64
• findutils.x86_64
• fipscheck.x86_64
• fipscheck-lib.x86_64
• firewalld.noarch
• firewalld-filesystem.noarch
• fontconfig.x86_64
• fontpackages-filesystem.noarch
• fprintd.x86_64
• fprintd-pam.x86_64
• freetype.x86_64
• fribidi.x86_64
• fuse.x86_64
System Manager RPMs

- fuse-libs.x86_64
- fxload.x86_64
- gawk.x86_64
- GConf2.x86_64
- gdb.x86_64
- gdbm.x86_64
- gdk-pixbuf2.x86_64
- genisoimage.x86_64
- GeoIP.x86_64
- gettext.x86_64
- gettext-common-devel.noarch
- gettext-devel.x86_64
- gettext-libs.x86_64
- giflib.x86_64
- git.x86_64
- glib2.x86_64
- glibc.x86_64
- glibc-common.x86_64
- gmp.x86_64
- gnupg2.x86_64
- gnutls.x86_64
- gobject-introspection.x86_64
- gpgme.x86_64
- gpm-libs.x86_64
- graphite2.x86_64
- grep.x86_64
- groff-base.x86_64
- grub2.x86_64
- grub2-common.noarch
- grub2-pc.x86_64
- grub2-pc-modules.noarch
- grub2-tools.x86_64
• grub2-tools-extra.x86_64
• grub2-tools-minimal.x86_64
• grubby.x86_64
• gssproxy.x86_64
• gtk2.x86_64
• gtk-update-icon-cache.x86_64
• gzip.x86_64
• hardlink.x86_64
• harfbuzz.x86_64
• haveged.x86_64
• hesiod.x86_64
• hicolor-icon-theme.noarch
• hmaccalc.x86_64
• hostname.x86_64
• hwdata.x86_64
• info.x86_64
• initscripts.x86_64
• insights-client.noarch
• iproute.x86_64
• iprutils.x86_64
• ipset.x86_64
• ipset-libs.x86_64
• iptables.x86_64
• iputils.x86_64
• irqbalance.x86_64
• ivtv-firmware.noarch
• iwl1000-firmware.noarch
• iwl100-firmware.noarch
• iwl105-firmware.noarch
• iwl135-firmware.noarch
• iwl2000-firmware.noarch
• iwl2030-firmware.noarch

Comments on this document? infodev@avaya.com
• iwl3160-firmware.noarch
• iwl3945-firmware.noarch
• iwl4965-firmware.noarch
• iwl5000-firmware.noarch
• iwl5150-firmware.noarch
• iwl6000-firmware.noarch
• iwl6000g2a-firmware.noarch
• iwl6000g2b-firmware.noarch
• iwl6050-firmware.noarch
• iwl7260-firmware.noarch
• iwl7265-firmware.noarch
• jansson.x86_64
• jasper-libs.x86_64
• java-1.8.0-openjdk.x86_64
• java-1.8.0-openjdk-debuginfo.x86_64
• java-1.8.0-openjdk-devel.x86_64
• java-1.8.0-openjdk-headless.x86_64
• javapackages-tools.noarch
• jbigkit-libs.x86_64
• json-c.x86_64
• kbd.x86_64
• kbd-legacy.noarch
• kbd-misc.noarch
• kernel.x86_64
• kernel-tools.x86_64
• kernel-tools-libs.x86_64
• kexec-tools.x86_64
• keyutils.x86_64
• keyutils-libs.x86_64
• kmod.x86_64
• kmod-libs.x86_64
• kpartx.x86_64
May 2020

Deploying Avaya Aura® System Manager in Software-Only Environment

Comments on this document? infodev@avaya.com

- kpatch.noarch
- krb5-libs.x86_64
- ksh.x86_64
- less.x86_64
- libacl.x86_64
- libaio.x86_64
- libassuan.x86_64
- libattr.x86_64
- libbasicobjects.x86_64
- libblkid.x86_64
- libcap.x86_64
- libcap-ng.x86_64
- libcgroup.x86_64
- libcgroup-tools.x86_64
- libcollection.x86_64
- libcom_err.x86_64
- libconfig.x86_64
- libcroco.x86_64
- libcurl.x86_64
- libdaemon.x86_64
- libdb.x86_64
- libdbi.x86_64
- libdb-utils.x86_64
- libdnet.x86_64
- libdrm.x86_64
- libdwarf.x86_64
- libedit.x86_64
- libestr.x86_64
- libevent.x86_64
- libfastjson.x86_64
- libffi.x86_64
- libfontenc.x86_64
System Manager RPMs

- libfprint.x86_64
- libgcc.x86_64
- libgcrypt.x86_64
- libglvnd.x86_64
- libglvnd-egl.x86_64
- libglvnd-glx.x86_64
- libgomp.x86_64
- libgpg-error.x86_64
- libgudev1.x86_64
- libICE.x86_64
- libicu.x86_64
- libIDL.x86_64
- libidn.x86_64
- libini_config.x86_64
- libjpeg-turbo.x86_64
- libmnl.x86_64
- libmodman.x86_64
- libmount.x86_64
- libmspack.x86_64
- libndp.x86_64
- libnetfilter_conntrack.x86_64
- libnfnetwork.x86_64
- libnfsidmap.x86_64
- libnl.x86_64
- libnl3.x86_64
- libnl3-cl outrl x86_64
- libpath_utils.x86_64
- libpcap.x86_64
- libpciaccess.x86_64
- libpipeline.x86_64
- libpng.x86_64
- libproxy.x86_64
• libpwquality.x86_64
• libref_array.x86_64
• libreport.x86_64
• libreport-cli.x86_64
• libreport-filesystem.x86_64
• libreport-plugin-mailx.x86_64
• libreport-plugin-rhtsupport.x86_64
• libreport-plugin-ureport.x86_64
• libreport-python.x86_64
• libreport-rhel.x86_64
• libreport-web.x86_64
• librsync.x86_64
• libseccomp.x86_64
• libselinux.x86_64
• libselinux-python.x86_64
• libselinux-utils.x86_64
• libsemanage.x86_64
• libsemanage-python.x86_64
• libsepol.x86_64
• libSM.x86_64
• libsmartcols.x86_64
• libsmi.x86_64
• libss.x86_64
• libssh2.x86_64
• libssss_idmap.x86_64
• libssss_nss_idmap.x86_64
• libstdc++.x86_64
• libstoragemgmt.x86_64
• libstoragemgmt-python.noarch
• libstoragemgmt-python-clibs.x86_64
• libsysfs.x86_64
• libtalloc.x86_64
System Manager RPMs

• libtar.x86_64
• libtasn1.x86_64
• libteam.x86_64
• libtevent.x86_64
• libthai.x86_64
• libtiff.x86_64
• libtirpc.x86_64
• libtool-ltdl.x86_64
• libunistring.x86_64
• libusal.x86_64
• libusb.x86_64
• libusbx.x86_64
• libuser.x86_64
• libutempter.x86_64
• libuuid.x86_64
• libverto.x86_64
• libverto-tevent.x86_64
• libwayland-client.x86_64
• libwayland-server.x86_64
• libX11.x86_64
• libX11-common.noarch
• libXau.x86_64
• libxcb.x86_64
• libXcomposite.x86_64
• libXcursor.x86_64
• libXdamage.x86_64
• libXext.x86_64
• libXfixes.x86_64
• libXfont.x86_64
• libXft.x86_64
• libXi.x86_64
• libXinerama.x86_64
• libxml2.x86_64
• libxml2-python.x86_64
• libXrandr.x86_64
• libXrender.x86_64
• libxshmfence.x86_64
• libxslt.x86_64
• libXtst.x86_64
• libXxf86vm.x86_64
• libyaml.x86_64
• linux-firmware.noarch
• lksctp-tools.x86_64
• lm_sensors-libs.x86_64
• logrotate.x86_64
• lshw.x86_64
• lsof.x86_64
• lsscsi.x86_64
• lua.x86_64
• lvmp2.x86_64
• lvmp2-libs.x86_64
• lz4.x86_64
• lzo.x86_64
• m2crypto.x86_64
• mailcap.noarch
• mailx.x86_64
• make.x86_64
• man-db.x86_64
• man-pages.noarch
• man-pages-overrides.x86_64
• mariadb-libs.x86_64
• mdadm.x86_64
• mesa-libEGL.x86_64
• mesa-libgbm.x86_64
• mesa-libGL.x86_64
• mesa-libglapi.x86_64
• microcode_ctl.x86_64
• mlocate.x86_64
• mozjs17.x86_64
• ncurses.x86_64
• ncurses-base.noarch
• ncurses-libs.x86_64
• nettle.x86_64
• net-tools.x86_64
• NetworkManager.x86_64
• NetworkManager-config-server.noarch
• NetworkManager-libnm.x86_64
• NetworkManager-team.x86_64
• NetworkManager-tui.x86_64
• newt.x86_64
• newt-python.x86_64
• nfs-utils.x86_64
• nspr.x86_64
• nss.x86_64
• nss-pem.x86_64
• nss-softokn.x86_64
• nss-softokn-freebl.x86_64
• nss-sysinit.x86_64
• nss-tools.x86_64
• nss-util.x86_64
• ntp.x86_64
• ntpdate.x86_64
• ntsysv.x86_64
• numactl-libs.x86_64
• openldap.x86_64
• openssh.x86_64
• openssh-askpass.x86_64
• openssh-clients.x86_64
• openssh-server.x86_64
• openssl.x86_64
• openssl-libs.x86_64
• open-vm-tools.x86_64
• ORBit2.x86_64
• os-prober.x86_64
• p11-kit.x86_64
• p11-kit-trust.x86_64
• pam.x86_64
• pango.x86_64
• parted.x86_64
• passwd.x86_64
• pciutils.x86_64
• pciutils-libs.x86_64
• pcre.x86_64
• pcsc-lite-libs.x86_64
• perl.x86_64
• perl-Business-ISBN.noarch
• perl-Business-ISBN-Data.noarch
• perl-Carp.noarch
• perl-Class-Load.noarch
• perl-Class-Singleton.noarch
• perl-Compress-Raw-Bzip2.x86_64
• perl-Compress-Raw-Zlib.x86_64
• perl-Config-Properties.noarch
• perl-constant.noarch
• perl-Data-Dumper.x86_64
• perl-Data-OptList.noarch
• perl-DateTime.x86_64
• perl-DateTime-Locale.noarch
System Manager RPMs

- perl-DateTime-TimeZone.noarch
- perl-DB_File.x86_64
- perl-DBI.x86_64
- perl-Digest.noarch
- perl-Digest-HMAC.noarch
- perl-Digest-MD5.x86_64
- perl-Digest-SHA.x86_64
- perl-Digest-SHA1.x86_64
- perl-Encode.x86_64
- perl-Encode-Locale.noarch
- perl-Error.noarch
- perl-Exporter.noarch
- perl-File-Listing.noarch
- perl-File-Path.noarch
- perl-File-Temp.noarch
- perl-Filter.x86_64
- perl-Getopt-Long.noarch
- perl-Git.noarch
- perl-HTML-Parser.x86_64
- perl-HTML-Tagset.noarch
- perl-HTTP-Cookies.noarch
- perl-HTTP-Daemon.noarch
- perl-HTTP-Date.noarch
- perl-HTTP-Message.noarch
- perl-HTTP-Negotiate.noarch
- perl-HTTP-Tiny.noarch
- perl-IO-Compress.noarch
- perl-IO-HTML.noarch
- perl-IO-Socket-INET6.noarch
- perl-IO-Socket-IP.noarch
- perl-IO-Socket-SSL.noarch
- perl-IO-Tty.x86_64
• perl-IPC-Run3.noarch
• perl-libs.x86_64
• perl-libwww-perl.noarch
• perl-List-MoreUtils.x86_64
• perl-LWP-MediaTypes.noarch
• perl-macros.x86_64
• perl-Module-Implementation.noarch
• perl-Module-Pluggable.noarch
• perl-Module-Runtime.noarch
• perl-Mozilla-CA.noarch
• perl-Net-Daemon.noarch
• perl-Net-DNS.x86_64
• perl-Net-HTTP.noarch
• perl-Net-LibIDN.x86_64
• perl-Net-SSLeay.x86_64
• perl-Package-DeprecationManager.noarch
• perl-Package-Stash.noarch
• perl-Package-Stash-XS.x86_64
• perl-Params-Util.x86_64
• perl-Params-Validate.x86_64
• perl-parent.noarch
• perl-PathTools.x86_64
• perl-PIRPC.noarch
• perl-Pod-Escapes.noarch
• perl-podlators.noarch
• perl-Pod-Perldoc.noarch
• perl-Pod-Simple.noarch
• perl-Pod-Usage.noarch
• perl-Scalar-List-Utils.x86_64
• perl-Socket.x86_64
• perl-Socket6.x86_64
• perl-Storable.x86_64
System Manager RPMs

- perl-Sub-Install.noarch
- perl-Switch.noarch
- perl-Sys-Syslog.x86_64
- perl-TermReadKey.x86_64
- perl-Text-ASCIITable.noarch
- perl-Text-ParseWords.noarch
- perl-threads.x86_64
- perl-threads-shared.x86_64
- perl-TimeDate.noarch
- perl-Time-HiRes.x86_64
- perl-Time-Local.noarch
- perl-Try-Tiny.noarch
- perl-URI.noarch
- perl-WWW-RobotRules.noarch
- perl-XML-LibXML.x86_64
- perl-XML-NamespaceSupport.noarch
- perl-XML-Parser.x86_64
- perl-XML-SAX.noarch
- perl-XML-SAX-Base.noarch
- perl-XML-Writer.noarch
- pinentry.x86_64
- pixman.x86_64
- pkgconfig.x86_64
- Plymouth.x86_64
- plymouth-core-libs.x86_64
- plymouth-scripts.x86_64
- policycoreutils.x86_64
- policycoreutils-python.x86_64
- polkit.x86_64
- polkit-pkla-compat.x86_64
- popt.x86_64
- postfix.x86_64
• postgresql96.x86_64
• postgresql96-contrib.x86_64
• postgresql96-libs.x86_64
• postgresql96-server.x86_64
• procmail.x86_64
• procps-ng.x86_64
• psacct.x86_64
• psmisc.x86_64
• pth.x86_64
• pygobject2.x86_64
• pygpgme.x86_64
• pyliblzma.x86_64
• pyOpenSSL.x86_64
• python.x86_64
• python2-futures.noarch
• python-augeas.noarch
• python-backports.x86_64
• python-backports-ssl_match_hostname.noarch
• python-chardet.noarch
• python-configobj.noarch
• python-dateutil.noarch
• python-decorator.noarch
• python-dmidecode.x86_64
• python-ethtool.x86_64
• python-firewall.noarch
• python-gobject-base.x86_64
• python-gudev.x86_64
• python-hwdata.noarch
• python-iniparse.noarch
• python-inotify.noarch
• python-ipaddress.noarch
• python-lPy.noarch
• python-javapackages.noarch
• python-libs.x86_64
• python-linux-procfs.noarch
• python-lxml.x86_64
• python-magic.noarch
• python-perf.x86_64
• python-pycurl.x86_64
• python-pyudev.noarch
• python-requests.noarch
• python-schedutils.x86_64
• python-setuptools.noarch
• python-six.noarch
• python-slip.noarch
• python-slip-dbus.noarch
• python-urlgrabber.noarch
• python-urllib3.noarch
• pyxattr.x86_64
• PyYAML.x86_64
• qrencode-libs.x86_64
• quota.x86_64
• quota-nls.noarch
• readline.x86_64
• Red_Hat_Enterprise_Linux-Release_Notes-7-en-US.noarch
• redhat-indexhtml.noarch
• redhat-logos.noarch
• redhat-release-server.x86_64
• redhat-support-lib-python.noarch
• redhat-support-tool.noarch
• rhn-check.x86_64
• rhn-client-tools.x86_64
• rhnlib.noarch
• rhnsd.x86_64
• rhn-setup.x86_64
• rng-tools.x86_64
• rootfiles.noarch
• rpcbind.x86_64
• rpm.x86_64
• rpm-build-libs.x86_64
• rpm-libs.x86_64
• rpm-python.x86_64
• rrdtool.x86_64
• rrdtool-perl.x86_64
• rsync.x86_64
• rsyslog.x86_64
• rsyslog-gnutls.x86_64
• ruby.x86_64
• rubygem-bigdecimal.x86_64
• rubygem-io-console.x86_64
• rubygem-json.x86_64
• rubygem-psych.x86_64
• rubygem-rdoc.noarch
• rubygems.noarch
• ruby-irb.noarch
• ruby-libs.x86_64
• satyr.x86_64
• scl-utils.x86_64
• sdm-api-installer.i386
• sed.x86_64
• selinux-policy.noarch
• selinux-policy-targeted.noarch
• sendmail.x86_64
• setools-libs.x86_64
• setserial.x86_64
• setup.noarch
System Manager RPMs

- sg3_utils.x86_64
- sg3_utils-libs.x86_64
- sgml-common.noarch
- sgpio.x86_64
- shadow-utils.x86_64
- shared-mime-info.x86_64
- slang.x86_64
- smartmontools.x86_64
- smem.noarch
- snappy.x86_64
- sos.noarch
- sqlite.x86_64
- sssd-client.x86_64
- strace.x86_64
- subscription-manager.x86_64
- subscription-manager-rhsm.x86_64
- subscription-manager-rhsm-certificates.x86_64
- sudo.x86_64
- systemd.x86_64
- systemd-libs.x86_64
- systemd-python.x86_64
- systemd-sysv.x86_64
- systemtap-runtime.x86_64
- sysvinit-tools.x86_64
- tar.x86_64
- tcl.x86_64
- tcp_wrappers.x86_64
- tcp_wrappers-libs.x86_64
- tcpdump.x86_64
- tcsh.x86_64
- teamd.x86_64
- time.x86_64
• traceroute.x86_64
• trousers.x86_64
• ttmkfdir.x86_64
• tuned.noarch
• tzdata.noarch
• tzdata-java.noarch
• unzip.x86_64
• usb_modeswitch.x86_64
• usb_modeswitch-data.noarch
• usbutils.x86_64
• usermode.x86_64
• ustr.x86_64
• util-linux.x86_64
• uuid.x86_64
• vim-common.x86_64
• vim-enhanced.x86_64
• vim-filesystem.x86_64
• vim-minimal.x86_64
• virt-what.x86_64
• wget.x86_64
• which.x86_64
• wireshark.x86_64
• wpa_supplicant.x86_64
• xdg-utils.noarch
• xfsdump.x86_64
• xfsprogs.x86_64
• xmlrpc-c.x86_64
• xmlrpc-c-client.x86_64
• xmlsec1.x86_64
• xmlsec1-openssl.x86_64
• xorg-x11-fonts-Type1.noarch
• xorg-x11-font-utils.x86_64
System Manager RPMs

- xz.x86_64
- xz-libs.x86_64
- yajl.x86_64
- yum.noarch
- yum-metadata-parser.x86_64
- yum-rhn-plugin.noarch
- zip.x86_64
- zlib.x86_64
Index

generating test alarms .......................................................... 65

I

InSite Knowledge Base .................................................. 72
install
Application Enablement Services .................................. 26
Avaya Aura applications .................................................. 26
Avaya Aura Media Server ............................................... 26
Avaya Breeze ................................................................. 26
Branch Session Manager ............................................... 26
Communication Manager ................................................. 26
SAL .................................................................................. 26
SDM ............................................................................ 26
Session Manager ............................................................ 26
Solution Deployment Manager client ............................... 26
System Manager ............................................................ 26
System Manager service pack from CLI ......................... 26
WebLM ........................................................................ 26
installing language pack
Canadian French ............................................................ 41
install new license files .................................................... 41
IP address ..................................................................... 53

J

Job History .................................................................. 52

L

latest software patches .................................................. 14
Linux operating system version
Avaya Aura® application OVAs ......................................... 11
Avaya Aura® application Software-only Environment ....... 10
local data backup
create ........................................................................ 47
location
adding ........................................................................ 28

M

My Docs ..................................................................... 70

N

network and configuration
field descriptions ........................................................... 33
network management systems destination ....................... 67
Network Management Systems Destinations ................... 66
new license file ............................................................... 41
NMS destination
add ............................................................................ 67
NMS destinations .......................................................... 66

O

overview ........................................................................ 9

P

patch information .......................................................... 14
perform System Manager tests ......................................... 41
planning checklist .......................................................... 13
PLDS
downloading software .................................................... 15
port matrix .................................................................. 69
postinstall
steps ............................................................................ 41

R

release notes for latest software patches ......................... 14
restore backup
remote server ............................................................... 48
restore backup from remote server ................................ 48
restore data backup ....................................................... 49
restore system backup from local server ....................... 49
RPMs
System Manager .......................................................... 74
WebLM ........................................................................ 74

S

SDM
installation ................................................................. 26
searching for content .................................................... 70
setting up operating system .......................................... 19
sharing content ............................................................. 70
site certificate
add ........................................................................... 44
delete ......................................................................... 44
manage ....................................................................... 44
view ........................................................................... 44
site preparation ............................................................ 14
SNMP traps .................................................................. 66
software details
System Manager ........................................................... 13
software-only ............................................................... 9
software patches ........................................................ 14
Solution Deployment Manager .................................... 24
Solution Deployment Manager client ............................. 24
Solution Deployment Manager Client
prerequisites ................................................................ 25
sort documents by last updated .................................... 70
support ........................................................................ 72
supported applications ................................................. 10
supported browsers ..................................................... 16
System Manager
commands ................................................................... 57
System Manager disk partitioning ................................. 20

Comments on this document? infodev@avaya.com