# Deploying SAL Gateway using Avaya Aura® System Manager in the VMware® Virtualized Environment

Release 3.0
Issue 2
April 2019

**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.

**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.

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

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

**Support tools**

“AVAYA SUPPORT TOOLS”MEAN THOSE SUPPORT TOOLS PROVIDED TO PARTNERS OR CUSTOMERS IN CONNECTION WITH MAINTENANCE SUPPORT OF AVAYA EQUYIPMENT (E.G., SAL, SLA MON, AVAYA DIAGNOISTIC SERVER, ETC.) AVAYA SUPPORT TOOLS ARE INTENDED TO BE USED FOR LAWFUL DIAGNOSTIC AND NETWORK INTEGRITY PURPOSES ONLY. The customer is responsible for understanding and complying with applicable legal requirements with regard to its network. The Tools may contain diagnostic capabilities that allow Avaya, authorized Avaya partners, and authorized customer administrators to capture packets, run diagnostics, capture key strokes and information from endpoints including contact lists, and remotely control and monitor

end-user devices. The customer is responsible for enabling these diagnostic capabilities, for ensuring users are aware of activities or potential activities and for compliance with any legal requirements with respect to use of the Tools and diagnostic capabilities on its network, including, without limitation, compliance with laws regarding notifications regarding capture of personal data and call recording.

Avaya Support Tools are provided as an entitlement of Avaya Support Coverage (e.g., maintenance) and the entitlements are established by Avaya. The scope of the license for each Tool is described in its License terms and/or the applicable service description document.

**Copyright**

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, 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. Note, unless otherwise stated, that 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, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

**Service Provider**

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

**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.

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

# Contents

# Chapter 1: Introduction

## Purpose

This document contains checklists and procedures for deploying the Secure Access Link (SAL) Gateway virtual appliance in the Avaya Aura® Virtualized Environment by using Avaya Aura® System Manager Solution Deployment Manager. The document includes installation, initial configuration, installation verification, upgrade, and basic maintenance checklist and procedures.

The primary audience of this document is anyone who installs, configures, and verifies SAL Gateway in a virtualization environment at a customer site. The audience includes implementation engineers, field technicians, and solution providers from Avaya, BusinessPartners, and customers.

## Prerequisites

Before you deploy or upgrade the product, ensure that you have the following knowledge, skills, and tools:

### Knowledge

- Avaya Aura® releases
- Linux® operating system
- VMware® and virtualized environment

### Skills

- VMware® and virtualized environment

### Tools

- Avaya supported servers or VMware® supported servers
- Solution Deployment Manager client if System Manager is unavailable or unreachable
- System Manager virtual machine resource requirements for each profile.
- Configuration tools and utilities

# Chapter 2: Avaya Aura architecture overview

## Avaya Aura® Virtualized offers

Avaya Aura® Release 7.0 and later supports the following two Avaya virtualization offers based on VMware:

- Avaya Aura® Virtualized Appliance (VA): Avaya-provided server, Avaya Appliance Virtualization Platform, based on the customized OEM version of VMware® ESXi 5.5.
- Avaya Aura® Virtualized Environment (VE): Customer-provided VMware infrastructure

The virtualization offers provide the following benefits:

- Simplifies IT management using common software administration and maintenance.
- Requires fewer servers and racks which reduces the footprint.
- Lowers power consumption and cooling requirements.
- Enables capital equipment cost savings.
- Lowers operational expenses.
- Uses standard operating procedures for both Avaya and non-Avaya products.
- Deploys Avaya Aura® virtual products in a virtualized environment on Avaya provided servers or customer-specified servers and hardware.
- Business can scale rapidly to accommodate growth and to respond to changing business requirements.

**Related links**

Appliance Virtualization Platform overview on page 7

## Appliance Virtualization Platform overview

From Release 7.0, Avaya uses the VMware®-based Avaya Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya Aura® Virtualized Appliance offer.

Avaya Aura® Virtualized Appliance offer includes:

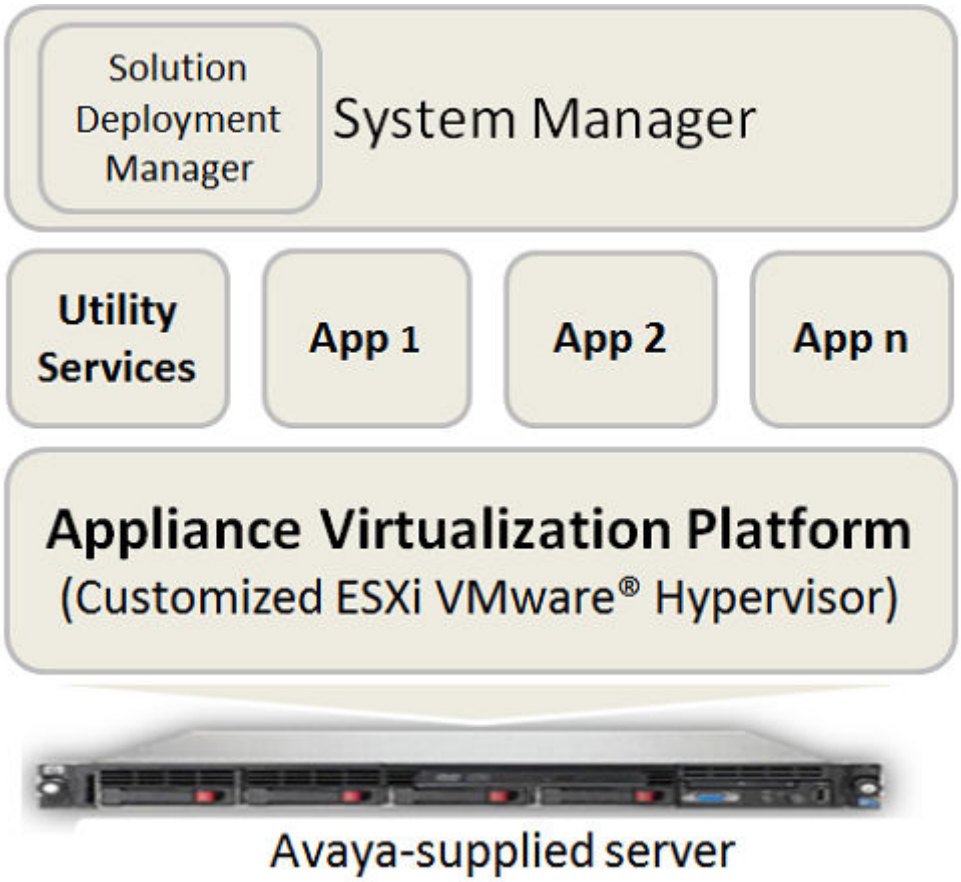
- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360 G7, HP ProLiant DL360p G8, and HP ProLiant DL360 G9

- S8300D and S8300E

**Note:**

With WebLM Release 7.x, you cannot deploy WebLM on S8300D Server or S8300E Server running on Appliance Virtualization Platform.

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.




From Avaya Aura® Release 7.0 and later, Appliance Virtualization Platform replaces System Platform.

You can deploy the following applications on Appliance Virtualization Platform:

- Utility Services 7.1.1
- System Manager 7.1.1
- Session Manager 7.1.1
- Branch Session Manager 7.1.1
- Communication Manager 7.1.1
- Application Enablement Services 7.1.1

- WebLM 7.1.1
- Avaya Breeze™ 3.3 with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0
- Avaya Aura® Device Services 7.0.1
- Avaya Aura® Media Server 7.8
- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

  For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

**Note:**

For deploying Avaya Aura® applications on Appliance Virtualization Platform only use Solution Deployment Manager.

**Related links**

Avaya Aura Virtualized offers on page 7

# Fresh deployment of Avaya Aura® applications

In Avaya Aura® Virtualized Appliance model, for fresh deployments, Avaya Aura® is available to end-users through a set of Avaya-supplied common servers. Avaya Aura® Virtualized Applianceis prepackaged with the virtualization software, and delivered to customers in a ready-to-run state.

In a customer-provided environment, VMware user can install Avaya Aura® applications by using vCenter that VMware provides.

# 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® 7.1.1 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.

In Release 7.1.1, Solution Deployment Manager supports migration of Virtualized Environment-based 6.x and 7.0 applications to Release 7.1.1 in customer Virtualized Environment.

Release 7.1.1 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 is the primary management solution for Avaya Aura® 7.1.1 and later applications.

System Manager with the 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 5.5 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.

With Solution Deployment Manager, you can perform the following operations in Virtualized Environment and Avaya Aura® Virtualized Appliance models:

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.
- Download Avaya Aura® applications.
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications:
  - Communication Manager and associated devices, such as gateways, media modules, and TN boards.
  - Session Manager
  - Branch Session Manager
  - Utility Services
  - Appliance Virtualization Platform, the ESXi host that is running on the Avaya Aura® Virtualized Appliance.

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 7.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

**Related links**

Solution Deployment Manager client on page 11

Capability comparison between System Manager Solution Deployment Manager and the Solution Deployment Manager client on page 15

Solution Deployment Manager on page 15

## Solution Deployment Manager client

For the initial System Manager deployment or when System Manager is inaccessible, you can use the Solution Deployment Manager client. The client can reside on the computer of the technician. The Solution Deployment Manager client provides the functionality to install the OVAs on an Avaya-provided server or customer-provided Virtualized Environment.

A technician can gain access to the user interface of the Solution Deployment Manager client from the web browser.

The Solution Deployment Manager client runs on Windows 7 64-bit, Windows 8 64-bit, and Windows 10 64-bit.

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Avaya appliances and Virtualized Environment.
- Upgrade System Platform-based System Manager.
- Upgrade Virtualized Environment-based System Manager from Release 7.0.x to Release 7.1.
- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.
- Create Appliance Virtualization Platform Kickstart file.
- Install Appliance Virtualization Platform patches.
- Restart and shutdown the Appliance Virtualization Platform host.
- Start, stop, and restart a virtual machine.
- Change the footprint of Avaya Aura® applications that support dynamic resizing. For example, Session Manager and Avaya Breeze™.

**Note:**

You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.

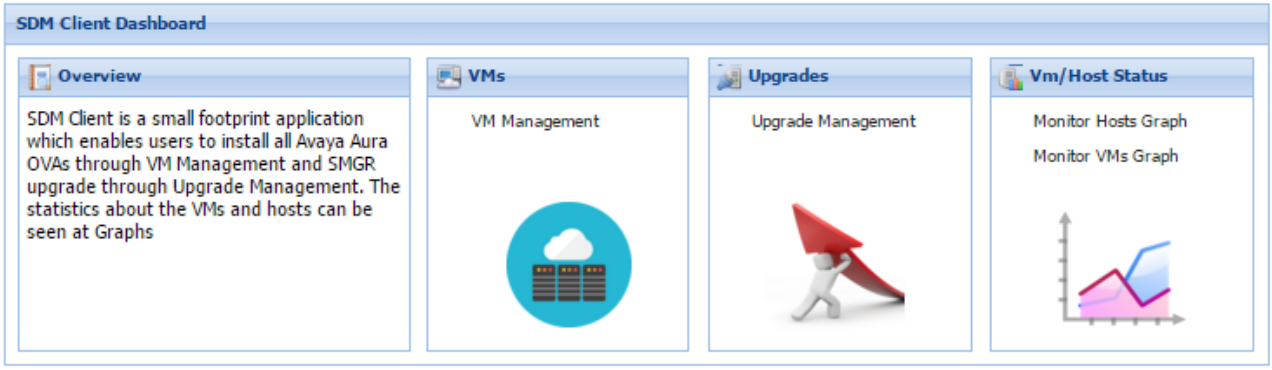



**Figure 1: Solution Deployment Manager client dashboard**

**Related links**

Solution Deployment Manager overview on page 9
Installing the Solution Deployment Manager client on your computer on page 12
Accessing the Solution Deployment Manager client dashboard on page 14

## 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 and hypervisor patches.

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

From Avaya Appliance Virtualization Platform Release 7.1, Solution Deployment Manager is mandatory to upgrade or deploy the Avaya Aura® applications.

### Before you begin

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, or Windows 10 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.

   **Tip:**

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

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.
6. Ensure that ports support Avaya Aura® 7.1.1 supported browsers.
7. Close all applications that are running on your computer.

8. Do not set CATALINA_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

   **Tip:**

   On **Computer**, right-click properties, and perform the following:

   a. In the left navigation pane, click **Advanced system settings**.

   b. On the System Properties dialog box, click Advanced tab, and click **Environment Variables**.

   c. Verify the system variables.

9. Ensure that the computer on which the Solution Deployment Manager client is running is connected to the network.

   Operations that you perform might fail if the computer is not connected to the network.

## Procedure

1. Download the `Avaya_SDMClient_win64_7.1.1.0.xxxxxxx_xx.zip` file from the Avaya Support website at http://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Support by Products** > **Downloads**, and enter the product name as **System Manager**, and version as **7.1**.
3. 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_7.1.1.0.xxxxxxx_45.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, click **Restore Default Folder**.
   - To specify a different location for installation, click **Choose** and browse to an empty folder.
8. Click **Next**.
9. On the Pre-Installation Summary page, review the information, and click **Next**.
10. 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 directory, in Select Location of Software Library Directory, click **Choose** and select a directory.

   The system saves the artifacts in the specified directory. During deployments, you can select the OVA file from the directory.

c. In **Data Port No**, select the appropriate port from the range 1527 through 1627.

d. In **Application Port No**, select the appropriate port from the range 443 through 543.

e. **(Optional)** Click **Reset All to Default**.

11. Click **Next**.
12. 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 system displays an error message. To continue with the installation, make the disk space, memory, and the ports available.

13. Click **Install**.
14. To exit the installer, on the Install Complete page, click **Done**.

    The installer creates a shortcut on the desktop.

15. 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*.

### Related links

Solution Deployment Manager client on page 11

## Accessing the Solution Deployment Manager client dashboard

### About this task

**Note:**

If you perform deploy, upgrade, and update operations from the Solution Deployment Manager client, ignore the steps that instruct you to access System Manager Solution Deployment Manager and the related navigation links.

### Procedure

To start the Solution Deployment Manager client, perform one of the following:

- On your computer, click **Start** > **All Programs** > **Avaya**, and click **SDM Client** > **Avaya SDM Client**.

- On your desktop, click .

**Related links**

Solution Deployment Manager client on page 11

## Capability comparison between System Manager Solution Deployment Manager and the Solution Deployment Manager client

| Centralized Solution Deployment Manager | Solution Deployment Manager client |
|---|---|
| Manage virtual machine lifecycle | Manage virtual machine lifecycle |
| Deploy Avaya Aura® applications | Deploy Avaya Aura® applications |
| Deploy hypervisor patches only for Appliance Virtualization Platform | Deploy hypervisor patches only for Appliance Virtualization Platform |
| Upgrade Avaya Aura® applications<br><br>Release 7.x supports upgrades from Linux-based or System Platform-based to Virtualized Environment or Appliance Virtualization Platform. Release 7.1 and later supports Virtualized Environment to Virtualized Environment upgrades. | Upgrade System Platform-based System Manager |
| Install software patches for Avaya Aura® applications excluding System Manager application | Install System Manager patches |
| Discover Avaya Aura® applications | Deploy System Manager |
| Analyze Avaya Aura® applications | - |
| Create and use the software library | - |

**Related links**

Solution Deployment Manager overview on page 9

## Solution Deployment Manager

The Solution Deployment Manager capability simplifies and automates the deployment and upgrade process.

With Solution Deployment Manager, you can deploy the following Avaya Aura® applications in Release 7.1.1:

- Utility Services 7.1.1
- System Manager 7.1.1
- Session Manager 7.1.1

- Branch Session Manager 7.1.1
- Communication Manager 7.1.1
- Application Enablement Services 7.1.1
- WebLM 7.1.1
- Avaya Breeze™ 3.3 with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0
- Avaya Aura® Device Services 7.0.1
- Avaya Aura® Media Server 7.8
- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

  For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

With Solution Deployment Manager, you can migrate, upgrade, and update the following applications:

- Linux-based Communication Manager 5.x and the associated devices, such as Gateways, TN boards, and media modules.

  **Note:**

  In bare metal Linux-based deployments, the applications are directly installed on the server and not as a virtual machine.

- Hardware-based Session Manager 6.x
- System Platform-based Communication Manager
  - Duplex CM Main / Survivable Core with Communication Manager
  - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- System Platform-based Branch Session Manager
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services

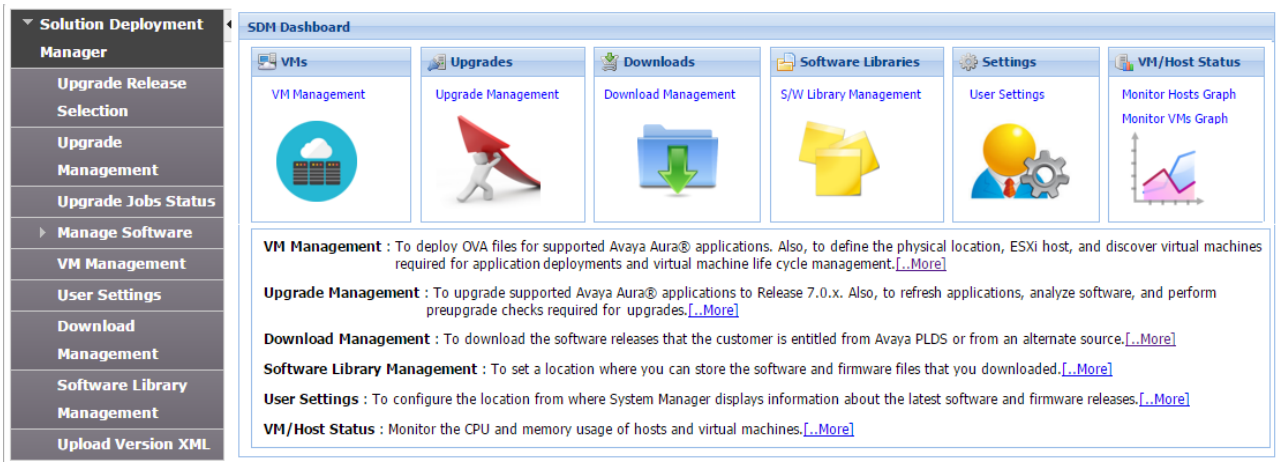
**Note:**

However, you must manually migrate Services virtual machine that is part of the template.

The centralized deployment and upgrade process provide better support to customers who want to upgrade their systems to Avaya Aura® Release 7.1.1. The process reduces the upgrade time and error rate.

## Solution Deployment Manager dashboard

You can gain access to the Solution Deployment Manager dashboard from the System Manager web console or by installing the Solution Deployment Manager client.




## Solution Deployment Manager capabilities

With Solution Deployment Manager, you can perform deployment and upgrade-related tasks by using the following links:

- **Upgrade Release Setting**: To select **Release 7.0** or **6.3.8** as the target upgrade. Release 7.1.1 is the default upgrade target.
- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module (UCM) and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **VM Management**: To deploy OVA files for the supported Avaya Aura® application.
  - Configure Remote Syslog Profile.
  - Generate the Appliance Virtualization Platform Kickstart file.
- **Upgrade Management**: To upgrade Communication Manager that includes TN boards, media gateways and media modules, Session Manager, Communication Manager Messaging, Utility Services, Branch Session Manager, WebLM to Release 7.1.1.
- **User Settings**: To configure the location from where System Manager displays information about the latest software and firmware releases.
- **Download Management**: To download the OVA files and firmware to which the customer is entitled. The download source can be the Avaya PLDS or an alternate source.
- **Software Library Management**: To configure the local or remote software library for storing the downloaded software and firmware files.

- **Upload Version XML**: To save the `version.xml` file to System Manager. You require the `version.xml` file to perform upgrades.

**Related links**

Solution Deployment Manager overview on page 9

# Virtual machine management

The VM Management link from Solution Deployment Manager provides the virtual machine management.

VM Management provides the following capabilities:

- Defines the physical location, Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Supports password change and patch installation of the Appliance Virtualization Platform host. Restart, shutdown, and certificate validation of Appliance Virtualization Platform and ESXi hosts. Also, enables and disables SSH on the host.
- Manages lifecycle of the OVA applications that are deployed on the ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.
- Deploys Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya Aura® Virtualized Appliance environments.
- Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Configures application and networking parameters required for application deployments.
- Supports flexible footprint definition based on capacity required for the deployment of the Avaya Aura® application OVA.

You can deploy the OVA file on the virtual machine by using the System Manager Solution Deployment Manager or the Solution Deployment Manager client.

# Utility Services in the Avaya Aura® Virtualized Appliance offer

From Avaya Aura® Release 7.1.1, Utility Services replaces the console domain (C-dom). Utility Services runs the Services Port connection that was previously run through Dom-0 on System Platform. Therefore, Utility Services with the Services Port is a key component of the Avaya Aura® Virtualized Appliance offer in Release 7.1.1, You must deploy Utility Services on each Appliance Virtualization Platform.

With Services Port, you can connect a laptop directly to Ethernet 1 on an Avaya-supported server, and connect the laptop to any of management interface of applications that run on an Appliance

Virtualization Platform host. On the S8300D and S8300E servers, Services Port is on the front plate. The Services Port virtual machine also supports ASG logins and install of a customer ASG file on to the system. By default, a generic ASG file is available on the system.

The Services Port virtual machine incorporates the Serviceability Agent for alarming and log collection from System Manager.

From Avaya Aura® Release 7.1.1, Utility Services does not include IP Phone firmware. The administrator must download the latest version of the firmware from PLDS and install on Utility Services.

### Utility Services migration

In the Avaya Aura® Virtualized Appliance offer on Appliance Virtualization Platform, you require Utility Services for services static routing. Therefore, you must deploy Utility Services if Utility Services is part of the solution.

In the following two use cases, you might require to deploy Utility Services.

1. Migration of Communication Manager or Session Manager on the Linux® server: Utility Services is mandatory for migration of systems running on the Linux® server. In this case, before you migrate, you must deploy Utility Services from VM Management.
2. Migration of Communication Manager or Session Manager on System Platform: In this case, the template already contains Utility Services. In this case, the process migrates Utility Services, and you do not require to deploy Utility Services separately.

# Chapter 3: Planning and preconfiguration

## Planning checklist

As an Avaya customer, ensure that you complete the following before deploying the SAL Gateway open virtual appliance (OVA):

| No. | Action | Notes | ✔ |
|---|---|---|---|
| 1 | Ensure that a supported server for the Avaya appliance model is installed. | See Supported servers on page 21. | |
| 2 | Ensure that Appliance Virtualization Platform is installed on the supported server. | See *Upgrading and Migrating Avaya Aura® applications to Release 7.1*. | |
| 3 | Ensure that you have all required hardware for the VMware environment. | See Server hardware and resources for VMware on page 22. | |
| 4 | Ensure that the virtualization environment has enough resources to be assigned for the SAL Gateway virtual appliance. | See SAL Gateway virtual appliance resource requirements on page 22. | |
| 5 | Ensure that System Manager 7.1 is available in the environment. | See *Upgrading Avaya Aura® System Manager to Release 7.1* and *Upgrading and Migrating Avaya Aura® applications to Release 7.1*. | |
| 6 | Download the SAL Gateway OVA file from PLDS. | To log on to the PLDS website, use your Avaya Single Sign On (SSO) login, which is associated with the Sold-To number that identifies the location where you want to install SAL Gateway. | |
| 7 | Copy the downloaded SAL Gateway OVA file to a directory on the local System Manager. | Copy the OVA file to the `/swlibrary/staging/sync/` directory. | |
| 8 | Upload the SAL Gateway OVA to the software library of System Manager. | See Uploading a file to the software library on page 25. | |

*Table continues…*

| No. | Action | Notes | ✔ |
|---|---|---|---|
| 9 | (Optional) Install the Solution Deployment Manager client for Windows. | Perform this task if System Manager is unavailable for some reason.<br>See Installing the Solution Deployment Manager client on your computer on page 12. | |
| 10 | Through Solution Deployment Manager, configure a location. | See Adding a location on page 27. | |
| 11 | Through Solution Deployment Manager, configure an ESXi host and associate the host with the location. | See Adding an Appliance Virtualization Platform or ESXi host on page 27. | |
| 12 | (Optional) Obtain the SAL Gateway identifying numbers, Solution Element ID and Product ID, from Avaya. | Obtaining the IDs in advance is not mandatory. You can accept the default IDs during the OVA deployment. After deployment, you can generate the IDs through the SAL Gateway user interface.<br>To obtain the IDs in advance, see Registering SAL Gateway on page 29. | |
| 13 | Ensure that the Appliance Virtualization Platform host and all virtual machines running on the host are on the same subnet mask. | If Out of Band Management is configured in an Appliance Virtualization Platform deployment, you need two subnet masks, one for each of the following:<br>• Public or signaling traffic, Appliance Virtualization Platform, and all virtual machines public traffic.<br>• Management, Appliance Virtualization Platform, and all virtual machine management ports. | |

# Supported servers

In the Avaya appliance model, you can deploy or upgrade to Avaya Aura® Release 7.1.1 applications on the following Avaya-provided servers:

- Dell™ PowerEdge™ R610
- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R630

- HP ProLiant DL360 G9
- S8300D, for Communication Manager and Branch Session Manager
- S8300E, for Communication Manager and Branch Session Manager
- Intel 1006r server. Only to deploy Utility Services and Avaya Aura® Messaging OVA files.

## Server hardware and resources for VMware

VMware offers compatibility guides that list servers, system, I/O, storage, and backup compatibility with VMware infrastructure. For more information about VMware-certified compatibility guides and product interoperability matrices, see http://www.vmware.com/resources/guides.html.

## SAL Gateway virtual appliance resource requirements

Before you deploy the SAL Gateway virtual appliance, you must ensure that the following minimal set of resources is available on the ESXi host. These resources are specified in the SAL Gateway OVA.

| VMware Resource | Value |
|---|---|
| vCPU | 1 |
| CPU speed | 2.3 GHz |
| Memory | 1GB |
| Storage reservation | 10 GB |
| NIC | 2 @ 1000 Mbps |

If you cannot guarantee the availability of the required resources on the ESXi host, do not deploy the SAL Gateway virtual appliance on that host.

You might deploy the SAL Gateway virtual appliance on a host that does not have the resources to allocate to the virtual machine to start. If CPU resources are limited, the system displays the `Insufficient capacity on each physical CPU`, or a similar message after the start-up request. To correct such limitations, you can adjust the virtual machine properties.

Sometimes, the CPU adjustments might not correct the start-up conditions. You might have to adjust other virtual machine resources as required.

**Important:**

Modifying the allocated resources might have a direct impact on the performance, capacity, and stability of the SAL Gateway virtual appliance. To run at full capacity, ensure that the virtual machine meets these resource size requirements. Removing or downsizing reservations might put this requirement at risk.

For SAL Gateway to perform at maximum capacity, maintain the resource allocation of the virtual machine.

# Specifications of bundled software in the OVA

The SAL Gateway OVA contains the application software, operating system, and other required software components, along with preinstalled VMware tools.

The following are the specifications of the software components included as part of the SAL Gateway OVA.

| | |
|---|---|
| **Operating system** | CentOS 7.3, 64-bit |
| **Java** | OpenJDK JRE 1.8 |
| **Application software** | SAL Gateway 3.0 |

# Capacity of SAL Gateway in the virtualized environment

The following table provides the capacity of SAL Gateway in the virtualized environment:

| | |
|---|---|
| Maximum managed elements | 15 |
| Maximum simultaneous remote connections | 6 |
| Maximum alarms per minute | 20 |

SAL Gateway performs at the maximum capacity when:

- The virtual machine meets the required specifications and the resource allocation.
- The alarm flow, remote sessions, and network conditions are normal.

**Note:**

To ensure stable and predictable performance, do not exceed the limit of 15 managed elements. To support more than 15 managed elements, install either a software-only Avaya Diagnostic Server on a standalone server or Avaya Diagnostic Server OVA on your VMware environment.

# Chapter 4: Initial setup and predeployment

## 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 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 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.

# Accessing Solution Deployment Manager

### About this task

You require to start Solution Deployment Manager to deploy and upgrade virtual machines, and install service packs or patches.

### Procedure

Perform one of the following:

- If System Manager is not already deployed, double-click the Solution Deployment Manager client.
- If System Manager is available, on the web console, click **Services** > **Solution Deployment Manager**.

# Uploading a file to the software library

### About this task

Use the procedure to upload software files, such as OVA, images, and firmware that are required during the deployment, migration, upgrade, and update of Avaya Aura® applications.

### Before you begin

- Start an SSH session.
- On Download Management page, click **Refresh Families**.
- When you add or update details in the `versions.xml` file, click **Refresh Families** again to get the updated information.

### Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Software Library Management**.
3. Click **Manage Files**.

4. From the System Manager command line interface, copy the required OVA file to the `/swlibrary/staging/sync/` location that you had created in System Manager.

   **Note:**

   You require admin privileges to access the `/swlibrary/staging/sync/` location.

   The system displays the file that you copied in the Sync Files from directory section.

5. Provide the following information:

   - **MD5 Checksum**: The value mentioned in the source or original location of the file.
   - **Software Library**: The local or remote software library.
   - **Product Family**

     **Note:**

     For SAL, in **Product Family**, **Device Type**, and **Software Type** fields, select **Others**.

   - **Device Type**
   - **Software Type**

   If the file is already in `versions.xml`, the system populates the information.

   If the file does not exist in `versions.xml`, the system does not display the file details. Therefore, you cannot use the file for upgrade in Upgrade Management. You can use the file only for new deployment from VM Management.

6. Select the file.
7. Click **Sync**.

   In File Sync Started Message, the system displays the status of the schedule of the job.

8. Click **OK**.

   When the job completes, the system displays the file in the Software Library Files section.

9. To check the status of the job, click **Services** > **Scheduler** > **Pending Jobs**.

   When the job is complete, the system displays the file in the Software Library Files area and removes from Sync Files from directory.

# Adding the ESXi host details on Solution Deployment Manager

**Note:**

Adding a location and a host are one-time activities on Solution Deployment Manager. If the ESXi host details are already available on Solution Deployment Manager, then you do not need to perform the following procedures.

## 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 System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the Location 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 VM Management Tree section.

## Adding an Appliance Virtualization Platform or ESXi host

### About this task

Use the procedure to add an Appliance Virtualization Platform or ESXi host. You can associate an ESXi host with an existing location.

If you are adding an standalone ESXi host to System Manager Solution Deployment Manager or to the Solution Deployment Manager client, add the standalone ESXi host using its FQDN only.

:

### Before you begin

A location must be available.

### Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section, click **Add**.
4. In the New Host section, provide the Host name, IP address, user name, and password.
5. Click **Save**.
6. On the Certificate dialog box, click **Accept Certificate**.

   The system generates the certificate and adds the Appliance Virtualization Platform host. For the ESXi host, you can only accept the certificate. If the certificate is invalid, to generate certificate, see the VMware documentation.

   In the VM Management Tree section, the system displays the new host in the specified location. The system also discovers applications.
7. To view the discovered application details, such as name and version, establish trust between the application and System Manager using the following:
   a. On the **Virtual Machines** tab, in the VMs for Selected Location <location name> section, select the required virtual machine.
   b. Click **More Actions** > **Re-establish connection**.

      For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
   c. Click **More Actions** > **Refresh VM**.

   **Important:**

   When you change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require Utility Services. To get the Utility Services application name during the IP address or FQDN change, refresh Utility Services to ensure that Utility Services is available.
8. On the **Hosts** tab, select the required host and click **Refresh**.

### Next steps

After adding a new host under VM Management Tree, the refresh host operation might fail to add the virtual machine entry under **Manage Element / Inventory**. This is due to the absence of **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

1. Under VM Management Tree, establish trust for all the virtual machines that are deployed on the host.
2. Ensure that the system populates the **Application Name** and **Application Version** for each of the virtual machines.
3. Once you have performed a trust establishment and refresh host operation on all virtual machines, you can perform refresh operation on the host.

# Registering SAL Gateway

## About this task

Registering a product with Avaya is a process that uniquely identifies the product so that Avaya can service the product. When you register a new SAL Gateway, Avaya assigns a Solution Element ID and a Product ID to the SAL Gateway. SAL Gateway becomes operational only when you configure SAL Gateway with the correct identifiers.

Use this procedure to register SAL Gateway and to generate the SAL Gateway identifiers through Global Registration Tool (GRT) without the use of any material codes.

**Note:**

Registering SAL Gateway before its installation is not mandatory. Since Release 2.5 onwards, an auto-registration feature is available through the SAL Gateway user interface. If you choose to use this feature, you do not need to take any action within GRT to register SAL Gateway.

## Procedure

1. Open the GRT website at https://support.avaya.com/grt.

   The GRT website redirects you to the Avaya single sign-on (SSO) webpage.
2. Log in using your SSO ID and password.
3. On the GRT home page, click **Create New Registration** > **SAL Migration Only**.
4. In the **Sold To/Functional Location** field, enter the Sold To or customer functional location number that identifies the location where you want to deploy SAL Gateway.
5. On the Site Contact Validation page, complete the required contact information fields.

   Provide valid information so that Avaya can contact you to notify you about the registration status.
6. Click **Next**.

   The SAL Gateway Migration List page lists the SAL Gateway instances available for the Sold To number that you provided.
7. Click **Create New SAL Gateway**.

   GRT starts an automatic end-to-end registration of a new SAL Gateway and performs the install base creation process.

   After the install base creation is complete, GRT automatically proceeds to the first step of the technical onboarding process to generate the Solution Element ID and Product ID of SAL Gateway.

   The SAL Onboarding Summary page displays the Solution Element ID and Product ID generated for the new SAL Gateway. You also receive an email notification with the new IDs.

## Next steps

- Complete the SAL Gateway installation process.

- Perform the technical onboarding process for devices that require support through the new SAL Gateway. See *Technical Onboarding Help Document* at https://support.avaya.com/registration.
- Add the devices as managed elements to your SAL Gateway using the SEIDs provided.

# Chapter 5: Deployment process

## SAL Gateway OVA deployment overview

Avaya delivers SAL Gateway 3.0 as a new OVA that you can deploy on an Avaya-provided appliance. The SAL Gateway 3.0 OVA is part of the Avaya Aura® 7.1 solution. For other VMware implementation, you can use the Avaya Diagnostic Server 3.0 OVA.

You can deploy the SAL Gateway 3.0 OVA on VMware Virtualized Environment using one of the following two options:

- Centralized Solution Deployment Manager. A centralized deployment and upgrade capability that System Manager 7.0 and later provide. You can use the centralized Solution Deployment Manager on System Manager to deploy virtual appliances.
- Solution Deployment Manager client. If you cannot access System Manager on the network, you can use the Solution Deployment Manager client to deploy virtual appliances. The client is a lightweight web-based tool that you can install on a Windows-based computer on the network. Both the centralized and the client version of Solution Deployment Manager provide similar web interfaces.

**Note:**

The SAL Gateway OVA does not support the direct ESXi host deployment. You can deploy the SAL Gateway OVA only through Solution Deployment Manager.

## Deployment checklist

Use the following checklist for deploying the SAL Gateway virtual appliance.

| No. | Action | Link/Notes | ✔ |
|---|---|---|---|
| 1 | Ensure that the ESXi host server is ready. | | |
| 2 | Deploy the OVA. | See Deploying the SAL Gateway OVA on page 32. | |

*Table continues…*

| No. | Action | Link/Notes | ✔ |
|---|---|---|---|
| 3 | Change the default passwords of the operating system accounts. | The SAL Gateway virtual appliance has the administrator and the root accounts with default passwords. You must change the passwords of these user accounts immediately after the deployment of the OVA. On the first login to the virtual appliance, The system prompts you to change the passwords.<br>See Password policies on page 63.<br>**Caution:**<br>You must change and control the root and administrator user passwords according to the password control policy of the company. Avaya is not responsible for password control and not liable for any adverse outcomes that might result from inadequate password control and failure to change the default passwords.<br>Note that because the root password belongs to the customer, Avaya cannot reset or recover the root password if lost or forgotten.<br>For information about resetting the account passwords, see Appendix A, Password management. | |

# Deploying the SAL Gateway OVA

## About this task

Use this procedure to deploy the SAL Gateway OVA to your virtualized environment by using Solution Deployment Manager.

## Before you begin

- Ensure that the host location is added and the ESXi host is added to the location.
- Add the OVA file to the software library of System Platform.

## Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **VM Management**.

3. In VM Management Tree, click the ESXi host on which you want to deploy the SAL Gateway OVA.
4. On the **Virtual Machines** tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment section.
5. In the Select Locations and Hosts section, in the **Host FQDN** field, type the name of the virtual machine.
6. In the Select Resource Pool and Data Store section, in the **Data Store** field, click a data store.

   In the Capacity Details section, you can view the capacity of the available data stores.
7. Click **Next**.
8. In the Deploy OVA section, perform the following:
   a. Click **OVA from software library**.
   b. In the **Select Software Library** field, select the local or remote library where the OVA file is available.
   c. In the **Select OVAs** field, select the OVA file that you want to deploy.

   In the Configuration Parameters and Network Parameters sections, Solution Deployment Manager populates fields that are specific to the application that you select to deploy.
9. In the Configuration Parameters section, complete the following fields for the SAL Gateway configuration:
   - **Timezone setting**
   - **Hostname**
   - **Automatic Software Update**
   - **SMTP Hostname / IP Address**
   - **SMTP Port**
   - **Administrator's E-mail Address**
   - (Optional) **SMTP Username**
   - (Optional) **SMTP Password**
   - (Optional) **Secondary E-mail Address**
   - **Solution Element ID**
   - **Alarm ID**

   **Note:**

   If you do not have the Solution Element ID and Alarm ID yet, you can accept the default values to continue. After the deployment, you must configure or generate the correct IDs thought the SAL Gateway user interface.

- (Optional) **Proxy Type**
- (Optional) **Proxy Hostname**
- (Optional) **Proxy Port**
- (Optional) **Proxy User**
- (Optional) **Proxy Password**
- (Optional) **Policy Manager Hostname**
- (Optional) **Policy Manager Port**
- **Master Agent Hostname**
- **Master AgentX Port**
- **Role**

**Important:**

You must replace the default values in most of the fields with correct values that match your environment.

If you plan to migrate the configuration from an existing SAL Gateway virtual appliance, you can keep the default values for the configuration parameters, except the SMTP, Automatic Software Update, and network properties fields.

10. In the Network Properties section, complete the fields according to your network settings:
    - **Default Gateway**
    - **DNS**
    - **Public IP Address**
    - **Public Netmask**
    - **OOBM Selection**
    - **Out of Band Management IP Address**
    - **Out of Band Management Netmask**
11. In the **Network Parameters** tab, complete the following fields:
    - **Public**
    - **Out of Band Management**

    If you want to use an Out-of-Band Management (OOBM) network, select the appropriate networks for NICs in these fields.
12. Click **Deploy**.

    The deployment process takes approximately 5 to 10 minutes to complete depending on the network connectivity quality.

## Next steps

1. (Optional) If you selected to use an OOBM network, configure static routes to direct traffic through the OOBM network interface.

2. Start the SAL Gateway services.

**Important:**

If you want to restore the configurations from an existing SAL Gateway virtual appliance to the new virtual appliance, then *do not* start the SAL Gateway services after the OVA deployment. After you complete the restore operation, the services start automatically.

**Related links**

Configuration Parameters tab field descriptions on page 37
VM Deployment field descriptions on page 35
Starting the SAL Gateway services on page 42
Static routes configuration on page 43

# VM Deployment field descriptions

## Select Location and Host section

| Name | Description |
|---|---|
| **Select Location** | The location name. The field is read only. |
| **Select Host** | The host name of the ESXi host. For example, smgrdev. The field is read only. |
| **Host FQDN** | FQDN of the ESXi host. |
| **Data Store** | The data store from where to allocate the disk space for the virtual appliance.<br>The page displays the capacity details of the selected data store in the Capacity Details section.<br>**Note:**<br>If the host is in a cluster, the system does not display the capacity details. Ensure that the host resource requirements are met before you deploy the virtual appliance. |
| **VM Name** | The name of the virtual machine. |
| **ME Deployment** | The option to perform the Midsize Enterprise deployment.<br>The option is available only while deploying Communication Manager simplex OVA. |

## Deploy OVA section

| Name | Description |
|---|---|
| **URL** | The option to specify the URL from where you can get the OVA file of the virtual appliance. |

*Table continues…*

| Name | Description |
|---|---|
| **Browse** | The option to specify the location of the OVA file of the virtual appliance on the System Manager host. |
| **OVA from software library** | The option to specify the software library from where you can get the OVA file of the virtual appliance. |
| **Select OVA** | The absolute path to the OVA file of the virtual appliance on the system that hosts System Manager.<br>The field is available only when you select **Browse**. |
| **Select Software Library** | The software library where the OVA file is available.<br>The field is available only when you select **OVA from software library**. |
| **Select OVAs** | The OVA file that you want to deploy.<br>The field is available only when you select **OVA from software library**. |
| **Flexi Footprint** | The footprint size supported for the selected host.<br>**Important:**<br>• Ensure that the required memory is available for the footprint sizes that you selected. Upgrades might fail due to insufficient memory.<br>• Ensure that the application contains the footprint size values that are supported.<br>**Note:**<br>The SAL Gateway OVA does not support flexible footprints. |

| Button | Description |
|---|---|
| **Submit File** | Selects the OVA file that you want to deploy, checks for available resources in the data store, and displays the result in the Capacity Details section.<br>The control is available only when you select **Browse**. |

## Configuration Parameters tab

In this tab, the system displays fields according to the selected OVA. The system populates most of the fields depending on the default values that are configured in the OVA file.

For more details about the configuration parameter fields for SAL Gateway, see Configuration Parameters tab field descriptions on page 37.

### Network Parameters tab

| Name | Description |
|---|---|
| **Public** | The network interface or virtual switch (vSwitch) that you want to use for normal in-band traffic. |
| **Out of Band Management** | The network interface you want to use for Out-of-Band Management (OOBM). If you do not want to use an OOBM network for the OVA, select the same network interface for both the public and the OOBM network.<br><br>To use OOBM, you must define a vSwitch for the OOBM network for the ESXi server prior to the OVA deployment. After the OVA deployment, you must enable the OOBM network interface manually. |

| Button | Description |
|---|---|
| **Deploy** | Displays the EULA acceptance screen where you must click **Accept** to start the OVA deployment process. |
| **Cancel** | Cancels the deploy operation and returns to the VMs for Selected Host <host name> section. |

### Related links

Configuration Parameters tab field descriptions on page 37

# Configuration Parameters tab field descriptions

The following table provides the descriptions of the fields available in the Application section of the **Configuration Parameters** tab for the SAL Gateway OVA deployment.

**Important:**

For SAL Gateway to function correctly, you must replace the default values in the fields with correct values that match your environment. In addition, provide correct SMTP details to receive software update notifications from Avaya.

| Name | Description |
|---|---|
| **Timezone setting** | The appropriate time zone for the location where you deploy the SAL Gateway virtual appliance. |
| **Hostname** | The host name or fully qualified domain name of the SAL Gateway virtual appliance. |

*Table continues…*

| Name | Description |
|---|---|
| **Automatic Software Update** | A drop-down list to enable or disable automatic software update for SAL Gateway. You can select one of the following two options:<br>• **Yes**: To enable the Automatic Software Update feature. If you do not install the downloaded software packages within the grace period set for the packages, the packages are applied automatically.<br>• **No**: To disable the Automatic Software Update feature. You must install the downloaded software packages manually. |
| **SMTP Hostname / IP Address** | The host name or the IP address of the Simple Mail Transfer Protocol (SMTP) server that SAL Gateway is to use for sending email notifications. |
| **SMTP Port** | The port number of the SMTP server. |
| **Administrator's E-mail Address** | The administrator email address where you want to receive email notifications about download and installation status of software updates. |
| **SMTP Username** | (Optional) The user name for the SMTP server.<br>The field is mandatory only when the SMTP server is configured to authenticate users. |
| **SMTP Password** | (Optional) The password of the user to be authenticated by the SMTP server.<br>The field is mandatory only when the SMTP server is configured to authenticate users. |
| **Secondary E-mail Address** | (Optional) A secondary email address where you want to receive email notifications. |
| **Solution Element ID** | A unique identifier in the format (nnn)nnn-nnnn, where n is a digit from 0 through 9. Using this ID, Avaya Services or Avaya Partners can uniquely identify and connect to this SAL Gateway.<br>If you do not have the Solution Element ID and Alarm ID yet, you can accept the default values to continue. After the deployment, you must configure or generate the correct IDs thought the SAL Gateway user interface. |
| **Alarm ID** | A unique 10-character ID, also called Product ID, assigned to a device, for example, this SAL Gateway. The Product ID is included in alarms that are sent to alarm receivers from the managed device. Avaya uses the Alarm ID to identify the device that generated the alarm.<br>If you do not have the Solution Element ID and Alarm ID yet, you can accept the default values to continue. After the deployment, you must configure or generate the correct IDs thought the SAL Gateway user interface. |

*Table continues…*

| Name | Description |
|---|---|
| **Proxy Type** | (Optional) The type of channel that the virtual machine uses to communicate with the servers outside your network. This field is required only if you use a proxy server for internet access outside the firewall of your network. The options are:<br>• **HTTP**: For an HTTP proxy without authentication.<br>• **Authenticated HTTP**: For an HTTP proxy with authentication.<br>• **SOCKS**: For a SOCKS proxy without authentication. |
| **Proxy Hostname** | (Optional) The host name or IP address of the proxy server. This field is required only if you have a proxy server for Internet access outside your network. |
| **Proxy Port** | (Optional) The port number of the proxy server. |
| **Proxy User** | (Optional) The user name for the authenticated HTTP proxy. This field is required only if the proxy type is authenticated HTTP. |
| **Proxy Password** | (Optional) The password for the authenticated HTTP proxy. This field is required only if the proxy type is authenticated HTTP. |
| **Policy Manager Hostname** | (Optional) The FQDN of the host where SAL Policy Manager with SSH Proxy is installed on your network.<br>The use of Policy Manager is optional. You can add the Policy Manager information later through the SAL Gateway user interface (UI). |
| **Policy Manager Port** | (Optional) The port number that SALPolicy Manager uses for communication with SAL Gateway. |
| **Master Agent Hostname** | The host name or IP address of the SNMP master agent to which the SNMP subagent must connect.<br>The default value is 127.0.0.1.<br>If you did not configure an SNMP master agent before the OVA deployment, you must update the SNMP master agent information on the SAL Gateway UI after you complete OVA deployment.<br>For information about SNMP master agent configuration, see *Deploying Avaya Diagnostic Server*. |
| **Master AgentX Port** | The AgentX listener port number of the SNMP master agent.<br>The default value is 705.<br>Retain the default value unless another application is already using the port. |

*Table continues…*

| Name | Description |
|---|---|
| **Role** | The role or permission level of the Avaya support personnel to the SAL Gateway UI. Avaya support personnel can have one of the following roles:<br>• **Administrator**: With full permissions to all the SAL Gateway UI pages except a few.<br>• **Browse**: With the read-only access to all pages.<br>• **Deny**: Without access to the SAL Gateway UI. |

The following table provides the descriptions of the fields available in the Network Properties section of the **Configuration Parameters** tab.

| Name | Description |
|---|---|
| **Default Gateway** | The IP address of the default gateway on your network. You can leave this field blank if you plan to use Dynamic Host Configuration Protocol (DHCP). |
| **DNS** | The comma-separated addresses of the Domain Name Servers (DNS) for the virtual machine. You can leave this field blank if you plan to use DHCP. |
| **Public IP Address** | The IP address of the public network interface. You can leave this field blank if you plan to use DHCP. |
| **Public Netmask** | The netmask or prefix for the public network interface. You can leave this field blank if you plan to use DHCP. |
| **OOBM Selection** | The field to indicate whether to use OOBM network for the virtual appliance. You can select one of the following:<br>• **Yes**: To use OOBM network.<br>• **No**: Not to use OOBM network. |
| **Out of Band Management IP Address** | The IP address of the OOBM network interface. |
| **Out of Band Management Netmask** | The netmask or prefix for the OOBM network interface. |

**Note:**

OVA deployment through Solution Deployment Manager does not support DHCP.

# Chapter 6: Initial configuration

## Virtual machine management

### Starting a virtual machine from Solution Deployment Manager

#### Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. From the virtual management tree, select a host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to start.
4. Click **Start**.

   In **VM State**, the system displays `Started`.

### Stopping a virtual machine from Solution Deployment Manager

#### About this task

System Manager is operational and ESXi or vCenter is added to the VM Management page to deploy Avaya Aura® Application OVA on ESXi virtual machines.

#### Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. From the virtual management tree, select a ESXi or vCentre host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to stop.
4. Click **Stop**.

   In **VM State**, the system displays `Stopped`.

## Restarting a virtual machine from Solution Deployment Manager

### Before you begin

- System Manager is operational, and ESXi or vCenter is added to the VM Management page to deploy Avaya Aura® Application OVA on ESXi virtual machines.
- Virtual machines must be in the running state.

### Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. From the virtual management tree, select a host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to restart.
4. Click **More Actions** > **Restart**.

   In **VM State**, the system displays `Stopped` and then `Started`.

## Starting the SAL Gateway services

### About this task

Use this procedure to start all SAL Gateway services.

After the deployment of the SAL Gateway OVA, the SAL Gateway services might remain disabled. Also, when you stop and then start the SAL Gateway virtual machine using the Solution Deployment Manager client, the SAL Gateway services do not start automatically. In such cases, you can start the services using this procedure.

**Important:**

If you want to migrate SAL Gateway configurations from System Platform or an existing SAL Gateway virtual appliance, then *do not* start the SAL Gateway services after the OVA deployment. Start the services only after you complete the migration activities. For a migration activity that involves restoring data through a restore script, the services start automatically.

### Procedure

1. Log on to the SAL Gateway virtual appliance as an administrator, and use the **`su`** command to become the root user.
2. Run the following command:

   ```
   cd /opt/avaya/common_services
   ```

3. Run the following command to start all SAL Gateway services:

   ```
   ./application_control.sh salgateway -enable
   ```

# Static routes configuration

By default, all traffic go through the default gateway you specify for the virtual appliance. Static routes are for traffic that should not go through the default gateway. Because the OOBM network is not reachable through a default gateway, you need to configure static routes to direct traffic through the OOBM network interface.

**Related links**

Adding static routes on page 43
Making static routes persistent on page 43

## Adding static routes

### About this task

If you have devices on an OOB private network, such as 192.168.1.0/24, you must add the necessary static routes to route traffic to that network through the OOBM network interface, eth1.

This procedure uses the **`ip route`** command to add static routes to an example network 192.168.1.0/24. Depending on the network setup, you might have to configure the static routes differently.

### Procedure

1. Log on to the SAL Gateway virtual appliance as an administrator through SSH, and switch to the root user.
2. Run the **`ip route`** command as one of the following to add static routes:
   - `ip route add 192.168.1.0/24 dev eth1`
   - `ip route add 192.168.1.0/24 via <eth1 IP address or next hop address> [dev eth1]`

   The command results in routing the traffic to the 192.168.1.0/24 network through eth1.

   After setting up the static routes, check that you are able reach or ping the devices from the gateway.

## Making static routes persistent

### About this task

The static routes that you set up using the **`ip route`** command are not persistent. The routes cease to exist once you restart the virtual machine. To make the static routes persistent, you must add the route configuration to the `/etc/sysconfig/network-scripts/route-eth1` file.

### Procedure

1. On the virtual appliance, open the `/etc/sysconfig/network-scripts/route-eth1` file in a text editor.
2. In the file, add the arguments you passed to the **`ip route`** command to add the static routes.

   For example, add the following new line to the file:

   ```
   192.168.1.0/24 dev eth1
   ```

   Or

   ```
   192.168.1.0/24 via <eth1 IP address or next hop address> [dev eth1]
   ```

   If you create the file before enabling the OOBM network interface, the static routes become available whenever the interface is enabled. The routes are unloaded whenever the interface is disabled.

# Chapter 7: Postinstallation verification

## Testing the alarming service of SAL Gateway

### About this task

Use this procedure to verify that the alarm transfer service of SAL Gateway is running properly. Through this service, SAL Gateway forwards alarms from Avaya devices to NMS, Avaya, or certified partner to monitor the alarm activities better.

### Procedure

1. Log on to the SAL Gateway virtual appliance as admin, and switch to the root user.
2. Run the following command, and check the outcome of the command:

   ```
   systemctl status spiritAgent
   ```

3. If the service is not running, run the following command to start the service:

   ```
   systemctl start spiritAgent
   ```

   **Note:**

   If you deploy the SAL Gateway OVA with the default Solution Element ID, the service does not start until you configure the correct ID. For information about configuring the correct Solution Element ID through the SAL Gateway UI, see *Administering Avaya Diagnostic Server SAL Gateway*.

4. Check the status again to verify that the service is running properly.

## Testing the SAL Watchdog process

### About this task

The SAL Watchdog process routinely tests the operational state of all SAL Gateway components and restarts the components in case of any abnormal shutdowns. Use this procedure to verify that the Watchdog process is running properly.

**Note:**

Untill Release 2.5, SAL Watchdog used to run as a service. From Release 3.0 onwards, SAL Watchdog is run as a cron job at every 5 minutes.

### Procedure

1. Log on to the host server as root.
2. Run the following command, and check the outcome of the command:

   `cat /var/log/cron`

   Example output of the command:

   ```
   Jan 27 11:25:01 linpubm206 CROND[2816]: (saluser) CMD (/opt/avaya/SAL/gateway/
   SALWatchdog/scripts/SALWatchdog)
   Jan 27 11:30:01 linpubm206 CROND[3452]: (root) CMD (/usr/lib64/sa/sa1 1 1)
   Jan 27 11:30:01 linpubm206 CROND[3453]: (saluser) CMD (/opt/avaya/SAL/gateway/
   SALWatchdog/scripts/SALWatchdog)
   ```

3. Check when the cron job was run the last time.

   If SALWatchdog was run in the last 5 minutes, you can consider that the process is running properly.

## Testing the SAL Gateway UI

### About this task

You can administer the SAL Gateway configurations through the web interface for the remote connectivity and alarm transfer facilities. Use this procedure to ensure that the SAL Gateway web interface is available.

### Procedure

1. From another terminal on the network where SAL Gateway is deployed, open a web browser.
2. In the address bar, type the following URL:

   `https://<IP address of the SAL Gateway virtual appliance>:7443`

   If the host server is registered under DNS, you can replace the host IP with the DNS host name.

   If you configured to use an OOBM network during the OVA deployment, the IP address of SAL Gateway is configured as the OOBM IP address. In such case, use the OOBM IP address in the URL.

   The browser must display the SAL Gateway login page.
3. If the SAL Gateway login page does not open, perform the following:
   a. Log on to the SAL Gateway virtual machine as admin, and switch to the root user.
   b. Run the following command to check the status of the gatewayUI service:

      **`systemctl status gatewayUI`**

   c. If the service is not running, run the following command to start the service:

```
systemctl start gatewayUI
```

d. Check the status again to verify that the service is running properly.

# Chapter 8: Postinstallation customer responsibilities

The customer owns the following postinstallation responsibilities:

- Control and care of the hardware.
- Maintenance of the operating system. Whenever new system updates are available, the customer is responsible to apply the updates that contain bug fixes or resolutions to security issues.
- Maintenance of any third-party software that are not bundled with Avaya Diagnostic Server. Whenever new software updates are available, the customer is responsible to apply the updates that contain bug fixes or resolutions to security issues.

# Chapter 9: Migrating from System Platform to Avaya Aura® Release 7.1 environment

## Overview

You can migrate from the earlier releases of SAL Gateway or Services-VM on System Platform to the SAL Gateway 3.0 virtual appliance in the the Avaya Aura® 7.1 environment. The migration process involves some manual operations of exporting data, deploying the Release 3.0 OVA, and importing the exported data to the new virtual appliance.

You can migrate from the following versions of Services-VM on System Platform:

- Services-VM 1.0
- Services-VM 2.0
- Services-VM 3.0

For information about upgrading other Avaya Aura® applications to Release 7.1, see *Upgrading and Migrating Avaya Aura® applications to Release 7.1*.

## Services-VM migration checklist

The following checklist provides the steps to migrate SAL Gateway data from an earlier release of Services-VM on System Platform to the SAL Gateway 3.0 virtual appliance in the Avaya Aura® Release 7.1 environment:

| No. | Task | Description | ✔ |
|---|---|---|---|
| 1 | Log on to the SAL Gateway user interface that is available for the Services-VM version you want to migrate. | Access the SAL Gateway user interface using one of the following options:<br>• On the System Platform web console, click **Server Management** > **SAL Gateway Management**, and then click **Launch SAL Gateway Management Portal**.<br>• Open the following URL on a web browser:<br>`https://<Services-VM_IP_address>:7443/` | |
| 2 | Through the SAL Gateway user interface, export the managed element data configured on the existing SAL Gateway to a .csv file. | On the Managed Element page, click **Export**, and save the .csv file to a folder on your local computer.<br>For more information about exporting managed element data, see *Administering Avaya Diagnostic Server SAL Gateway*. | |
| 3 | Deploy the SAL Gateway 3.0 OVA in the Avaya Aura® 7.1 virtualized environment. | See Deploying the SAL Gateway OVA on page 32.<br>**Important:**<br>• For an upgrade or migration operation, deploy the target server with the same IP address and host name as in the old server.<br>• Ensure that you do not start the SAL Gateway services after the deployment of the SAL Gateway OVA. Complete the migration activities, and then only start the SAL Gateway services. | |
| 4 | Take the older version of SAL Gateway offline. | You cannot uninstall SAL Gateway on Services-VM. Do one of the following to disable the earlier instance of SAL Gateway:<br>• On the System Platform web console, go to **Server Management** > **Network Configuration**, and clear the **Enable Services VM** check box to disable Services-VM.<br>• Stop all services related to SAL Gateway on Services-VM. | |

*Table continues…*

| No. | Task | Description | ✔ |
|---|---|---|---|
| 5 | Log on to the user interface of the new SAL Gateway 3.0 virtual appliance. | | |
| 6 | Through the SAL Gateway user interface, import the .csv file that contains the managed element data that was exported from the earlier instance of SAL Gateway. | 1. On the Managed Element page, click **Import**, and browse to the saved .csv file on your local computer.<br>2. Click **Upload** and then **Apply** to import the devices to SAL Gateway as managed elements.<br>For more information about importing managed element data, see *Administering Avaya Diagnostic Server SAL Gateway*. | |
| 7 | Verify the configuration details of the imported managed elements. | Do the following as required:<br>• If the model associated with an imported device supports multiple products, ensure that the correct product type is selected for that managed element. When the model supports multiple products, the device is added to SAL Gateway with the default product for that model. For example, if the model assigned to the device is CM_Media_Server_<version>, this model supports more than one product. When imported, the device is added as CM Media Server, which is the default product for the model. Edit the configuration of such managed devices to select the correct product.<br>• Wherever required, make the changes to device configuration related to SNMP v3, inventory collection, and device credentials for inventory collection. | |
| 8 | Start the SAL Gateway services. | See Starting the SAL Gateway services on page 42. | |

# Post upgrade activities

After you complete the upgrade and migration of SAL Gateway and the Avaya Aura® applications from System Platform to Avaya Aura® Release 7.1, complete the following activities on SAL Gateway:

| No. | Task | ✔ |
|---|---|---|
| 1 | Through the SAL Gateway web interface, update the SAL model from DOM0 to the new model, Appliance Virtualization Platform. | |
| 2 | Add Utility Services as a managed element to SAL Gateway. | |

# Chapter 10: Upgrading SAL Gateway virtual appliance to Avaya Aura® 7.1 environment

## SAL Gateway virtual appliance migration checklist

You can migrate the SAL Gateway 2.5 virtual appliance to the Avaya Aura® Release 7.1 environment. Avaya Aura® 7.1 does not support automated upgrade from Virtualized Environment to Virtualized Environment. Therefore, the migration process involves some manual operations of creating a backup, deploying the Release 3.0 OVA, and restoring the backup on the new virtual appliance.

The following checklist provides the high-level steps to migrate from the SAL Gateway 2.5 virtual appliance to the SAL Gateway 3.0 virtual appliance in the Avaya Aura® Release 7.1 environment:

| No. | Task | Description | ✔ |
|---|---|---|---|
| 1 | Back up the SAL Gateway 2.5 virtual appliance. | See Backing up SAL Gateway virtual appliance on page 54. | |
| 2 | Transfer the backup file to a remote server by using `scp` or some other similar file transfer utility. | | |
| 3 | Deploy the SAL Gateway 3.0 OVA in the Avaya Aura® 7.1 virtualized environment. | See Deploying the SAL Gateway OVA on page 32.<br>**Important:**<br>• For a upgrade or migration operation, deploy the target server with the same IP address and host name as in the old server.<br>• Ensure that you do not start the SAL Gateway services after the deployment of the SAL Gateway OVA. Complete the upgrade activities, and then only start the SAL Gateway services. | |

*Table continues…*

| No. | Task | Description | ✔ |
|---|---|---|---|
| 4 | Take the SAL Gateway 2.5 virtual appliance offline. | Through Solution Deployment Manager or vCenter, stop or delete the virtual machine.<br>**Note:**<br>Do *not* use the uninstaller script to uninstall SAL Gateway on a virtualized environment. | |
| 5 | Restore the backup to the new SAL Gateway 3.0 virtual appliance. | See Restoring SAL Gateway data on SAL Gateway 3.0 virtual appliance on page 55. | |
| 6 | Ensure that all configurations are migrated correctly and all services are running properly. | To start the services, see Starting the SAL Gateway services on page 42. | |

# Backing up SAL Gateway virtual appliance

## About this task

Use this procedure to back up data from the SAL Gateway virtual appliance.

## Procedure

1. Log on to the SAL Gateway virtual appliance as an administrator user through SSH, and use the **su** command to become the root user.
2. Navigate to the `/opt/avaya/common_services` directory:

   ```
   cd /opt/avaya/common_services
   ```

3. Run the following command to take the backup:

   ```
   ./backup
   ```

   The system creates the backup file and saves the file in the `/vm-data/backup/archives` directory. The name of the backup file is in the following format:

   `vmbackup_<timestamp in ddMMyyHHmmss format>.tar.gz`

   The system displays a message about the backup file name and the location where the backup file is saved. For example:

   `/vm-data/backup/archives/vmbackup_150817223639.tar.gz`

4. Navigate to the backup directory, and use **scp** to transfer the backup file to a remote server.

# Restoring SAL Gateway data on SAL Gateway 3.0 virtual appliance

### About this task

Use this procedure to restore the backup from an existing SAL Gateway virtual appliance to the SAL Gateway 3.0 virtual appliance.

### Before you begin

Ensure the following:

- The existing SAL Gateway virtual appliance is backed up, and the backup file is transferred to a remote server.
- The SAL Gateway 3.0 virtual appliance is ready after deployment.
- The IP address and the host name of the target server is same as the old server.
- The SAL services on the new SAL Gateway virtual appliance are not started.

### Procedure

1. Log on to the SAL Gateway 3.0 virtual appliance as an administrator user through SSH, and use the **su** command to become the root user.
2. Ensure that the SAL services are in the stopped state.
3. Transfer the backup file from the remote server to a location on the SAL Gateway virtual appliance.
4. Navigate to the `/opt/avaya/common_services` directory:

   ```
   cd /opt/avaya/common_services
   ```

5. Run the following command to restore the backed up SAL Gateway details:

   ```
   ./restore <Archive_file_path_on_VM>
   ```

   After the system completes the restore operation, the services start automatically.
6. Ensure that all configurations are migrated correctly and all services are running properly.

### Related links

Starting the SAL Gateway services on page 42

# Chapter 11: Maintenance procedures

## Backup and restore overview

You can use the backup and restore capabilities of the SAL Gateway virtual machine for the long-term backup and recovery of the SAL Gateway virtual machine that runs on VMware.

As the customer, you have the responsibility to run the backup at periodic intervals. Alternatively, you can schedule a job to run the backup at a periodic interval and copy the backup archive to an external system for preserving the data in the event of a system failure.

The following procedures are for backing up and restoring the SAL Gateway configuration data through the backup and restore scripts available on the virtual appliance.

You can also use the backup and restore features provided by the SAL Gateway user interface. For more details about the backup and restore features provided by the user interface, see *Administering Avaya Diagnostic Server SAL Gateway*.

**Related links**

Backing up the virtual machine on page 56
Restoring a virtual machine on page 57

## Backing up the virtual machine

### About this task

Use this procedure to back up the SAL Gateway virtual machine.

### Procedure

1. Open a virtual machine console, or connect to the virtual machine using an SSH client.
2. Log in as admin, and switch to the root user.
3. Run the following command:

   **`backup`**

   The system displays the directory location where the backup archive is saved.

   You can find the latest backup archive file at the `/vm-data/backup/archives/` directory. The archive file is saved with a file name similar to `vmbackup_xxxxxxxx.tar.gz`.

4. Copy the backup archive to an external host to prevent loss of data in the event of a system failure.

   To copy the file to a remote server, you can use the Linux **scp** command:

   **scp** *<archive_file> <username>@<remote_server_ip>:<directory_path>*

**Related links**

Backup and restore overview on page 56

## Restoring a virtual machine

### About this task

Use this procedure to restore a virtual machine from a backup archive.

### Procedure

1. Deploy the virtual machine.
2. Start the virtual machine.
3. Log in to the virtual machine as admin, and switch to the root user.
4. Copy the backup archive file to a directory on the virtual machine.

   If you are copying the file from a remote system, you can use the following:

   - From a Linux remote system: Use the **scp** command to copy the file back to the virtual machine.

     **scp** *<user>@<SAL_VM_IP_or_hostname>:<directorypath_and_filename_on_remote_system_location> <Archive_file_path_on_VM>*

   - From a Windows remote system: Use WinSCP or a similar file transfer utility to copy the file back to the virtual machine.
5. From the virtual machine console, run the following command:

   **restore** *<Archive_file_path_on_VM>*

**Related links**

Backup and restore overview on page 56

# Redundancy considerations

While creating redundancy for a SAL Gateway 3.0 virtual appliance, consider the following:

- Redundancy should not be with a SAL Gateway instance that supports larger numbers of managed elements.

- Redundancy should be with another SAL Gateway 3.0 virtual appliance or a SAL Gateway instance on Services-VM.

# Chapter 12: Resources

## Documentation

The following table lists the documents related to SAL Gateway and Avaya Aura® Virtualized Environment. Download the documents from the Avaya Support website at http://support.avaya.com.

| Title | Use this document to: | Audience |
|---|---|---|
| **Design and overview** | | |
| *Avaya Aura® Virtualized Environment Solution Description* | Understand the virtualized environment solution from a functional view. Includes a high-level description of the solution, topology diagrams, customer requirements, and design considerations. | Customers, sales engineers, solution architects, and implementation engineers |
| *Avaya Aura® System Manager Overview and Specification* | Understand the high-level solution features and functionalities. | Customers, sales engineers, solution architects, implementation engineers, and support personnel |
| **Implementation** | | |
| *Upgrading Avaya Aura® System Manager to Release 7.1* | Upgrade Avaya Aura® System Manager from earlier releases to Release 7.1 on Avaya-provided appliance and customer-provided Virtualized Environment. | Implementation engineers and support personnel |
| *Deploying Avaya Aura® applications from System Manager* | Install and configure Avaya Aura® applications in Avaya Aura® Virtualized Environment by using System Manager Solution Deployment Manager. | Implementation engineers and support personnel |
| *Upgrading and Migrating Avaya Aura® applications to Release 7.1* | Upgrade and migrate Avaya Aura® applications, including Communication Manager and other associated applications, to Avaya Aura® Release 7.1. | Implementation engineers and support personnel |
| **Administration** | | |

*Table continues…*

| Title | Use this document to: | Audience |
|---|---|---|
| *Administering Avaya Diagnostic Server SAL Gateway* | Configure and administer SAL Gateway for remote servicing and alarm transfer facilities of Avaya products at a customer site. | Implementation engineers, support personnel, and system administrators |
| Administering Avaya Aura® System Manager | Perform administration tasks for System Manager and Avaya Aura® applications that System Manager supports. | System administrators and support personnel |

## Finding documents on the Avaya Support website

### Procedure

1. Navigate to http://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 an appropriate release number.
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 displays the documents only from the selected category.
7. Click **Enter**.

## Training

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

| Course code | Course title | Type |
|---|---|---|
| 2007V/W | What is New in Avaya Aura® Release 7.1 | AvayaLive™ Engage Theory |
| 2011/V/W | What is New in Avaya Aura® Session Manager Release 7.1 and Avaya Aura® System Manager Release 7.1 | AvayaLive™ Engage Theory |
| 2012V | Migrating and Upgrading to Avaya Aura® 7.0 | AvayaLive™ Engage Theory |

*Table continues…*

| Course code | Course title | Type |
|---|---|---|
| 2013V | Avaya Aura® Release 7.1 Solution Management | AvayaLive™ Engage Theory |

# 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.

### Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

**Note:**

Videos are not available for all products.

# Support

Go to the Avaya Support website at http://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 62

## 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.

1. Go to http://www.avaya.com/support.
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 61

# Appendix A: Password management

## Password policies

Adhere to the following rules while you set up a new password:

- The password must be *at least 8 characters long*.
- The passwords must contain:
  - Minimum one English uppercase letter: A, B, C, ... Z
  - Minimum one English lowercase letter: a, b, c, ... z
  - Minimum one numeral: 0, 1, 2, ... 9
  - Minimum one non-alphanumeric special character, such as: ! @ # $ & %
  - Minimum four characters that are different from the previous password

**Note:**

The root user password expires every 90 days. After the password is expired, reset the password to log in to the system.

## Resetting the password of an operating system account

### About this task

Use this procedure to reset the password of an operating system account.

### Procedure

1. Log on to the virtual appliance through the VMware console or SSH as admin.
2. Use the **su -** command to switch to the root user.
3. Run the following command to reset the password of a specific account:

   ```
   passwd <account_name>
   ```

   When the system prompts, type the new password.
4. Run the following command to reset the password of the root user:

   ```
   passwd
   ```

   When the system prompts, type the new password.

**Related links**

Password policies on page 63

# Resetting the password of the admin user

## Procedure

1. Log on to the virtual appliance through the VMware console as root.
2. Run the following command to reset the password of the admin user:

   ```
   passwd admin
   ```

3. When the system prompts, type the new password.

   Henceforth, use the new password to log in as the admin user

# Resetting the password of the root user

## About this task

If you forget the password of the root user, use this procedure to reset the password.

## Procedure

1. Boot the virtual appliance through the VMware console.
2. During the booting process, press **Ctrl**.
3. Select the first entry, and type `e`.
4. Select the second entry, `kernel`, and type `e`.
5. Edit the entry as the following:
   a. Remove `rghb quiet`.
   b. Enter `init=/bin/sh`.
6. Press **Enter**.
7. Press **b**, and let the booting process to continue.
8. When the process stops at the shell prompt sh-4.1#, run the following command:

   ```
   mount -rw -o remount /
   ```

9. Run the following command:

   ```
   passwd
   ```

10. When the system prompts, type the new password.

11. Restart the virtual machine using the VMware console.

# Index

## L



## M



## O



## P



## R



## S

## T



## U



## V