Upgrading standalone Avaya WebLM
© 2018-2020, Avaya Inc. All Rights Reserved.

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

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

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will necessarily 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=20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

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

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

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

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

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

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

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

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

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

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

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

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

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

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

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

Avaya is a registered trademark of Avaya Inc.
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: 8
- Prerequisites: 8
- Change history: 9

**Chapter 2: Upgrade overview**
- Supported upgrade paths for WebLM: 10
- Solution Deployment Manager: 12

**Chapter 3: Planning and preconfiguration**
- Supported servers: 14
- Supported servers for Avaya Aura® applications: 14
- Supported hardware for VMware: 15
- Software requirements: 15
- Supported ESXi version: 16
- Latest software updates and patch information: 16
- Upgrade order for Avaya components: 16
- Software details of WebLM: 18
- Downloading software from PLDS: 19
- Supported footprints for WebLM Server: 20
- Customer configuration data for WebLM: 20
- Supported browsers: 21

**Chapter 4: Preupgrade tasks**
- Viewing license options: 22
  - Viewing the license capacity and utilization of the product features: 22
  - Viewing peak usage for a licensed product: 23
- Virtual machine management: 24
  - Application management: 24
  - Managing the location: 25
  - Managing the host: 27
  - Downloading the OVA file to System Manager: 34
  - Managing the application: 35
  - Managing vCenter: 40
- Applications pre-upgrade functions: 46
  - Refreshing elements: 46
  - Analyzing software: 47
  - Downloading the software: 47
  - File Download Manager field descriptions: 48
  - Performing the preupgrade check: 49
  - Preupgrade Configuration field descriptions: 50
- Upgrading VMware ESXi version: 51
## Contents

**Chapter 5: Upgrading WebLM to Appliance Virtualization Platform and VMware**
- Upgrading WebLM to Release 8.1.1 by using System Manager Solution Deployment Manager... 53
- Edit Upgrade Configuration field descriptions...................................................................... 56
- Installing a WebLM patch, feature pack, or service pack.................................................... 63
- Upgrading WebLM by using CLI...................................................................................... 63

**Chapter 6: Upgrading WebLM to KVM environment**......................................................... 65
- Migration path for KVM.................................................................................................. 65
- Upgrading to KVM environment...................................................................................... 65

**Chapter 7: Upgrading WebLM to IaaS environment**......................................................... 66
- Migration path for IaaS.................................................................................................. 66
- Upgrading to IaaS environment...................................................................................... 66

**Chapter 8: Upgrading WebLM to Software-only environment**........................................ 67
- Migration path for Software-only environment.................................................................. 67
- Upgrading to Software-only environment using manual backup and restore method........ 67
- Upgrading from AVP or VMware based WebLM to Software-only environment by using System Manager Solution Deployment Manager........................................................................... 67

**Chapter 9: Post-deployment and upgrade verifications**..................................................... 71
- Post-upgrade checklist.................................................................................................... 71
- Logging on to the WebLM web console............................................................................ 71
- Rehosting license files..................................................................................................... 72
- Verifying the WebLM software version........................................................................... 72
- Upgrade job status.......................................................................................................... 73
  - Viewing the Upgrade job status.................................................................................. 73
  - Editing an upgrade job............................................................................................... 74
  - Deleting the Upgrade jobs......................................................................................... 74
- Upgrade Job Status field descriptions............................................................................. 75
- Rollback process............................................................................................................. 75
- Upgrade rollback............................................................................................................ 75
- Rolling back an upgrade............................................................................................... 76
- Enhanced Access Security Gateway overview............................................................... 76
- Enhanced Access Security Gateway (EASG) overview.................................................. 76

**Chapter 10: Maintenance**................................................................................................ 79
- Maintenance.................................................................................................................. 79
  - Changing the IP, FQDN, DNS, Gateway, or Netmask addresses................................. 79
  - Configuring multiple DNS IP addresses..................................................................... 80
  - Configuring the time zone......................................................................................... 81
  - Configuring the NTP server....................................................................................... 81
  - Resetting the WebLM password through CLI............................................................. 81
  - Performing WebLM backup...................................................................................... 82
  - Performing WebLM restore....................................................................................... 82
  - Creating a snapshot backup...................................................................................... 82
  - Creating a snapshot restore...................................................................................... 83

August 2020

Comments on this document? infodev@avaya.com
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebLM CLI operations</td>
<td>84</td>
</tr>
<tr>
<td>Viewing the job history of virtual machine operations</td>
<td>85</td>
</tr>
<tr>
<td>Monitoring a host and virtual machine</td>
<td>86</td>
</tr>
<tr>
<td><strong>Chapter 11: Resources</strong></td>
<td>88</td>
</tr>
<tr>
<td>Avaya WebLM documentation</td>
<td>88</td>
</tr>
<tr>
<td>Finding documents on the Avaya Support website</td>
<td>88</td>
</tr>
<tr>
<td>Accessing the port matrix document</td>
<td>89</td>
</tr>
<tr>
<td>Avaya Documentation Portal navigation</td>
<td>89</td>
</tr>
<tr>
<td>Training</td>
<td>90</td>
</tr>
<tr>
<td>Amazon Web Services documentation</td>
<td>90</td>
</tr>
<tr>
<td>Viewing Avaya Mentor videos</td>
<td>91</td>
</tr>
<tr>
<td>Support</td>
<td>91</td>
</tr>
<tr>
<td>Using the Avaya InSite Knowledge Base</td>
<td>91</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td>93</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

Purpose
This document describes the procedures for upgrading WebLM from Release 6.x and Release 7.x to Release 8.1.1 on:

- Avaya-provided server in Avaya Aura® Virtualized Appliance Environment.
- VMware in customer-provided Virtualized Environment.
- Amazon Web Services, Google Cloud, and Microsoft Azure setup in Infrastructure as a service (IaaS).
- Customer provided software-only environment.

This document:
- includes upgrade checklists and maintenance procedures.
- does not include optional or customized aspects of a configuration.

The primary audience for this guide is anyone who is involved with upgrading and verifying WebLM.

Prerequisites
Before upgrading the Avaya Aura® application, ensure that you have the following knowledge, skills and tools:

Knowledge
- For Appliance Virtualization Platform: Appliance Virtualization Platform virtualized environment.
- For VMware: VMware® vSphere™ virtualized environment.
- For Kernel-based Virtual Machine (KVM): KVM hypervisor set up.
- For Amazon Web Services(AWS): AWS environment.
- For Google Cloud: Google Cloud environment.
- For Azure: Microsoft Azure environment.
• Linux® Operating System.
• System Manager.

Skills
To administer:
• Solution Deployment Manager.
• VMware® vSphere™ virtualized environment.
• KVM hypervisor.
• AWS Management Console.
• Google Cloud.
• Microsoft Azure.

Tools
For information about tools and utilities, see “Configuration tools and utilities”.

---

**Change history**

The following changes have been made to this document since the last issue:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>August 2020</td>
<td>Updated the section: <a href="#">Upgrading from AVP or VMware based WebLM to Software-only environment by using System Manager Solution Deployment Manager</a> on page 67</td>
</tr>
</tbody>
</table>
| 2     | October 2019| For Release 8.1.1, added the following section:  
  • [Upgrading WebLM by using CLI](#) on page 63  
For Release 8.1.1, updated the following sections:  
  • [Software details of WebLM](#) on page 18  
  • [Supported upgrade paths for WebLM](#) on page 10  
  • [Upgrading WebLM to Release 8.1.1 by using System Manager Solution Deployment Manager](#) on page 53  
  • [Upgrading from AVP or VMware based WebLM to Software-only environment by using System Manager Solution Deployment Manager](#) on page 67 |
| 1     | June 2019  | Release 8.1 document.                                                                                                                                  |
Chapter 2: Upgrade overview

Supported upgrade paths for WebLM

The following table displays all the upgrade paths from earlier releases to Release 8.1.x.

⚠️ Important:

- If you are upgrading standalone WebLM by using Solution Deployment Manager on the following supported platform, the system preserves the licenses that are available on old WebLM.
  - Appliance Virtualization Platform to Appliance Virtualization Platform
  - Appliance Virtualization Platform to VMware
  - VMware to VMware
  - VMware to Appliance Virtualization Platform

- If you are upgrading standalone WebLM by using Solution Deployment Manager in Software-only environment, the system does not preserve the licenses that are available on old WebLM.

- If you are upgrading standalone WebLM by using CLI-based procedure without using WebLM, the system does not preserve the licenses that are available on old WebLM as the host id of new WebLM changes. It only restores the users that are available on old WebLM, if supported. You need to rehost licenses on new WebLM.

🌟 Note:

- Before starting the application upgrade, upgrade the platform and hypervisor.

- For upgrading System Manager, use Solution Deployment Manager Client. For upgrading applications other than System Manager, use System Manager Solution Deployment Manager.

- Upgrade or migration using Solution Deployment Manager is only supported with same IP Address of the application in Software-only environment.

Software-only upgrade is supported for VMware, KVM, Nutanix, RHVH, OpenStack, Hyper-V, AWS, GoogleCloud, and Azure.

For information about terms used in the following table, see “Glossary”.
<table>
<thead>
<tr>
<th>From offer</th>
<th>From Release</th>
<th>To Software-only 8.1.x (ISO)</th>
<th>To AVP 8.1.x (OVA)</th>
<th>To VMware 8.1.x (OVA)</th>
<th>To AWS 8.1.x (OVA)</th>
<th>To KVM/OpenStack/Nutanix/RHVH 8.1.x (OVA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVP</td>
<td>7.0.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
<tr>
<td></td>
<td>7.1.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
<tr>
<td></td>
<td>8.0.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
<tr>
<td>VMware</td>
<td>6.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
<tr>
<td></td>
<td>7.0.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
<tr>
<td></td>
<td>7.1.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
<tr>
<td></td>
<td>8.0.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
<tr>
<td>KVM</td>
<td>7.1.x</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
<tr>
<td></td>
<td>8.0.x</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
<tr>
<td>Software-only</td>
<td>8.0.x</td>
<td>Migration using SDM</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>AWS</td>
<td>7.1.x</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
<tr>
<td></td>
<td>8.0.x</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
</tbody>
</table>
Solution Deployment Manager

Solution Deployment Manager simplifies and automates the deployment and upgrade process. With Solution Deployment Manager, you can deploy the following applications:

- AVP Utilities 8.1.1
- System Manager 8.1.1
- Session Manager 8.1.1
- Branch Session Manager 8.1.1
- Communication Manager 8.1.1
- Application Enablement Services 8.1.1
- WebLM 8.1.1
- Communication Manager Messaging 7.0

For information about other Avaya product compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

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

- 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:

You must manually migrate the Services virtual machine that is part of the template.

The centralized deployment and upgrade process provides better support to customers who want to upgrade their systems to Avaya Aura® Release 8.1.1. 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.x Onwards or 6.3.8 as the target upgrade. Release 8.1.1 is the default upgrade target.

- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module, and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.

- **Application 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 Avaya Aura® applications to Release 8.1.1.

- **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 application-specific version.xml file to perform upgrades.
Chapter 3: Planning and preconfiguration

Supported servers

The following servers are supported for deployments and upgrades to Release 8.1 and later:

- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G9
- S8300E, for Communication Manager and Branch Session Manager
- Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640
- Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640

**Note:**

- Avaya Aura® Release 8.0 and later does not support S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.
- Avaya Aura® Release 7.0 and later does not support S8510 and S8800 servers.

For fresh installations, use Avaya Solutions Platform 120 Appliance or Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640.

Supported servers for Avaya Aura® applications

The following table lists the supported servers of Avaya Aura® applications.

<table>
<thead>
<tr>
<th>Supported servers</th>
<th>Avaya Aura® Release</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.0.x</td>
</tr>
<tr>
<td>S8300D</td>
<td>Y</td>
</tr>
<tr>
<td>S8300E</td>
<td>Y</td>
</tr>
<tr>
<td>HP ProLiant DL360 G7</td>
<td>Y</td>
</tr>
<tr>
<td>HP ProLiant DL360p G8</td>
<td>Y</td>
</tr>
<tr>
<td>HP ProLiant DL360 G9</td>
<td>Y</td>
</tr>
</tbody>
</table>

Table continues…

Comments on this document? infodev@avaya.com
Supported servers

<table>
<thead>
<tr>
<th>Supported servers</th>
<th>Avaya Aura® Release</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.0.x</td>
</tr>
<tr>
<td>Dell™ PowerEdge™ R610</td>
<td>Y</td>
</tr>
<tr>
<td>Dell™ PowerEdge™ R620</td>
<td>Y</td>
</tr>
<tr>
<td>Dell™ PowerEdge™ R630</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya Solutions Platform 120</td>
<td></td>
</tr>
<tr>
<td>Appliance: Dell PowerEdge R640</td>
<td></td>
</tr>
<tr>
<td>Avaya Solutions Platform 130</td>
<td></td>
</tr>
<tr>
<td>Appliance: Dell PowerEdge R640</td>
<td></td>
</tr>
</tbody>
</table>

**Note:**

From Avaya Aura® Release 8.0 and later, S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers are not supported.

---

Supported hardware 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](http://www.vmware.com/resources/guides.html).

---

Software requirements

Avaya Aura® supports the following software versions:

- Avaya Aura® Virtualized Appliance offer: Appliance Virtualization Platform 8.1.x
- Customer-provided Virtualized Environment offer supports the following software versions:
  - VMware® vSphere ESXi 6.0, 6.5, or 6.7
  - VMware® vCenter Server 6.0, 6.5, or 6.7


**Note:**

- Avaya Aura® Release 8.0 and later does not support vSphere ESXi 5.0 and 5.5.
- With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware® vSphere Client for ESXi and vCenter administration.
Supported ESXi version

The following table lists the supported ESXi versions of Avaya Aura® applications.

<table>
<thead>
<tr>
<th>ESXi version</th>
<th>Avaya Aura® Release</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.0.x</td>
</tr>
<tr>
<td>ESXi 5.0</td>
<td>Y</td>
</tr>
<tr>
<td>ESXi 5.1</td>
<td>Y</td>
</tr>
<tr>
<td>ESXi 5.5</td>
<td>Y</td>
</tr>
<tr>
<td>ESXi 6.0</td>
<td></td>
</tr>
<tr>
<td>ESXi 6.5</td>
<td></td>
</tr>
<tr>
<td>ESXi 6.7</td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
- With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware vSphere Client for ESXi and vCenter administration.
- Avaya Aura® applications support the ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 6.7 can be VMware ESXi 6.7 Update 3.

Latest software updates and patch information

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

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

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

Upgrade order for Avaya components

You must upgrade Avaya components and solution in the following sequence. If any of the components are not part of your solution, you can skip that particular component and move to the next component.

1. Hard Endpoints (H.323 and SIP)
   You can upgrade endpoints after all Avaya Aura® Platform components are upgraded.
2. Standalone Avaya WebLM
3. Avaya Aura® Appliance Virtualization Platform that hosts System Manager
   Appliance Virtualization Platform of individual components must be upgraded first.
   
   ★ Note:
   • If you are upgrading Appliance Virtualization Platform from Release 7.x to 8.x, Solution Deployment Manager also upgrades Utility Services to AVP Utilities during the Appliance Virtualization Platform upgrade.
   • If you are upgrading Appliance Virtualization Platform from Release 8.0.x to 8.1.x, you need to manually upgrade AVP Utilities after upgrading Appliance Virtualization Platform.

4. AVP Utilities

5. SAL Gateway
   You can choose to upgrade SAL Gateway after all components are upgraded.

6. Avaya Aura® System Manager includes System Manager WebLM and System Manager Solution Deployment Manager
   In the:
   • Non-Geography Redundancy setup, update standalone System Manager.
   • Geography Redundancy setup, update the primary System Manager.
   Avaya recommends that you use System Manager to update Avaya Aura® applications.

7. Avaya Device Adapter Snap-in on Avaya Breeze® platform

8. Avaya Aura® Session Manager (Core Session Managers only)

9. Avaya Breeze® platform and other Snap-ins

10. Avaya Call Management System

11. Avaya Aura® Experience Portal

12. Avaya Oceana® Solution

13. Avaya Aura® Device Services

14. G4XX Media gateways or Avaya Aura® Media Server
   
   ★ Note:
   For S8300E, the Gateway must be on minimum version 33.x.

15. Avaya Aura® Branch Session Manager

16. Avaya Aura® Application Enablement Services

17. Avaya Aura® Communication Manager Survivable Remote Servers (formerly known as Local Survivable Processors)

18. Avaya Aura® Presence Services Snap-in on Avaya Breeze® platform

19. Avaya Aura® Communication Manager Survivable Core Servers (formerly known as Enterprise Survivable Processors)

20. Avaya Aura® Communication Manager feature servers and evolution servers
In duplex configuration, update the:

- Standby Communication Manager server
- Active Communication Manager server

21. Avaya IP Office™ platform
22. Avaya Aura® Messaging or IX Messaging (formerly known as Officelinx)
23. Avaya Aura® Web Gateway
24. Equinox Clients
   Clients are dependent on Avaya Aura® Device Services in Avaya Aura® Platform.
25. Avaya Equinox® Conferencing
26. Avaya Session Border Controller for Enterprise

**Note:**

- System Manager is an integral part of the Avaya Aura® solution.
- System Manager must be on the same or higher release than the application you are upgrading to. For example, you must upgrade System Manager to 8.1 before you upgrade Communication Manager to 8.1.

All the applications that are supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for the version of applications that are supported by System Manager, see Avaya Aura® Release Notes on the Avaya Support website.

- Remove the old Solution Deployment Manager Client and install the latest Solution Deployment Manager Client.

Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 8.1 OVA, Solution Deployment Manager Client version must be on Release 8.1. Solution Deployment Manager Client cannot be on Release 8.0.

- If an application is running on Release earlier than 8.0.x and if it has Utility Services, you must back up Utility Services files and install them on Avaya Aura® Device Services Release 8.0. For migrating data from the legacy Avaya Aura® Utility Services to the Utility Server embedded within Avaya Aura® Device Services Release 8.0, see Administering Avaya Aura® Device Services on the Avaya Support website.

For information about upgrading the application, see the application-specific upgrade guide on the Avaya Support website.

---

**Software details of WebLM**

For Avaya Aura® application software build details, see Avaya Aura® Release Notes on the Avaya Support website at [http://support.avaya.com/](http://support.avaya.com/).
**Downloading software from PLDS**

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

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

*Note:*

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

**Procedure**

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

*Note:*

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

13. If you use Internet Explorer and get an error message, click the **install ActiveX** message at the top of the page and continue with the download.
14. Select a location where you want to save the file and click **Save**.
15. If you used the Download Manager, click **Details** to view the download progress.
Supported footprints for WebLM Server

These footprints are common for Appliance Virtualization Platform, VMware, and KVM.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Profile 1</th>
<th>Profile 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CPU reservation</td>
<td>• Appliance Virtualization Platform and VMware: 2185 MHz</td>
<td>• Appliance Virtualization Platform and VMware: 2185 MHz</td>
</tr>
<tr>
<td></td>
<td>• KVM: 2185 MHz</td>
<td>• KVM: 2185 MHz</td>
</tr>
<tr>
<td>Memory reservation</td>
<td>1GB</td>
<td>2GB</td>
</tr>
<tr>
<td>Storage reservation</td>
<td>40GB</td>
<td>40GB</td>
</tr>
<tr>
<td>Shared NICs</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

☆ Note:
If you use the WebLM server to acquire licenses for more than 5000 clients, use Profile 2.

Customer configuration data for WebLM

The following table identifies the key customer configuration information that you must provide throughout the deployment and configuration process.

<table>
<thead>
<tr>
<th>Required data</th>
<th>Description</th>
<th>Example value for the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The IP address of the WebLM interface.</td>
<td>For IPv4: 192.168.x.x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For IPv6: 2001:0db8::a</td>
</tr>
<tr>
<td>Netmask</td>
<td>The network address mask.</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The default network traffic gateway.</td>
<td>For IPv4: 172.16.x.x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For IPv6: 2001:0db8::1</td>
</tr>
<tr>
<td>DNS IP Address</td>
<td>The IP address of the primary DNS server.</td>
<td>For IPv4: 172.16.x.x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For IPv6: 2001:0db8::5</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The domain name which must be a fully qualified domain name.</td>
<td>abc.mydomain.com</td>
</tr>
<tr>
<td>Short HostName</td>
<td>-</td>
<td>weblm</td>
</tr>
<tr>
<td>Default Search List</td>
<td>The domain name string that is used for default search.</td>
<td>abc.mydomain.com</td>
</tr>
<tr>
<td>NTP Server</td>
<td>The IP address of the NTP server.</td>
<td>For IPv4: 172.16.x.x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For IPv6: 2001:0db8::b</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Required data</th>
<th>Description</th>
<th>Example value for the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone</td>
<td>The time zone you want to choose.</td>
<td>America/Denver</td>
</tr>
<tr>
<td>CLI User details</td>
<td>The command line interface user details.</td>
<td>abcd</td>
</tr>
<tr>
<td>Admin UI password</td>
<td>The admin UI password.</td>
<td></td>
</tr>
<tr>
<td>EASG</td>
<td>Enhanced Access Security Gateway</td>
<td></td>
</tr>
<tr>
<td>Customer root account details</td>
<td>The customer root account details.</td>
<td></td>
</tr>
</tbody>
</table>

### Supported browsers

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

Comments on this document? infodev@avaya.com
Chapter 4: Preupgrade tasks

Viewing license options

Viewing the license capacity and utilization of the product features

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

About this task

Use this procedure to view the license capacity and license utilization of a product for which you installed a license file.

Procedure

1. In the navigation pane, in Licensed products, click the required product.
2. Click View license capacity.

View License Capacity field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License File Host IDs</td>
<td>The host ID of the license file.</td>
</tr>
</tbody>
</table>

Licensed Features

You can view the total number of feature licenses in the license file and the current usage of those licenses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature (License Keyword)</td>
<td>The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The date on which the feature license expires.</td>
</tr>
</tbody>
</table>

Table continues…
### Name | Description
--- | ---
**Licensed capacity** | The number of licenses for each licensed feature. WebLM fetches the number of feature licenses information from the license file.

**Currently Used** | The number of feature licenses that are currently in use by the licensed application. For features of type Uncounted, the column displays *Not counted*.

### Acquired Licenses
The Acquired licenses table displays information about the licenses acquired by the licensed application. You can view the information in the table only if the licensed product has acquired feature licenses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>The feature keyword for each licensed feature that is currently acquired by a licensed application.</td>
</tr>
<tr>
<td>Acquired by</td>
<td>The name of the licensed application that has acquired the license.</td>
</tr>
<tr>
<td>Acquirer ID</td>
<td>The unique identifier of the licensed application that has acquired the license.</td>
</tr>
<tr>
<td>Count</td>
<td>The number of feature licenses that are currently acquired by the licensed application.</td>
</tr>
</tbody>
</table>

---

### Viewing peak usage for a licensed product

**Before you begin**
- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

**Procedure**
1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View peak usage**.

**View Peak Usage field descriptions**
You can view information about the usage of feature licenses of a licensed application at different time intervals.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Feature (License Keyword)</strong></td>
<td>The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.</td>
</tr>
<tr>
<td><strong>Currently Allocated</strong></td>
<td>The number of feature licenses purchased by the organization.</td>
</tr>
</tbody>
</table>
### Virtual machine management

#### Application management

The Application Management link from Solution Deployment Manager provides the application management capabilities that you can use to do the following.

- 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 Appliance Virtualization Platform or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.
Note:
For the Avaya Aura® Messaging element, trust re-establishment is not required.

- Deploys Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya Aura® Virtualized Appliance environment.
- Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Deploys Avaya Aura® application ISOs in Software-only environment.
- 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 or ISO file on the platform by using System Manager Solution Deployment Manager or the Solution Deployment Manager client.

Managing the location

Viewing a location
Procedure
1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. Click the Locations tab.
   The Locations section lists all locations.

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 > Application Management**.
2. On the **Locations** tab, in the Locations section, click **New**.
3. In the New Location section, perform the following:
   a. In the Required Location Information section, type the location information.
   b. In the Optional Location Information section, type the network parameters for the virtual machine.
4. Click **Save**.
   The system displays the new location in the **Application Management Tree** section.
Related links
New and Edit location field descriptions on page 26

Editing the location
Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. On the Locations tab, in the Locations section, select a location that you want to edit.
3. Click Edit.
4. In the Edit Location section, make the required changes.
5. Click Save.

Related links
New and Edit location field descriptions on page 26

Deleting a location
Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. On the Locations tab, in the Locations section, select one or more locations that you want to delete.
3. Click Delete.
4. In the Delete confirmation dialog box, click Yes.
   The system does not delete the applications that are running on the platform and moves the platform to Unknown location Platform mapping.

New and Edit location field descriptions

Required Location Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The location name.</td>
</tr>
<tr>
<td>Avaya Sold-To #</td>
<td>The customer contact number. Administrators use the field to check entitlements.</td>
</tr>
<tr>
<td>Address</td>
<td>The address where the host is located.</td>
</tr>
<tr>
<td>City</td>
<td>The city where the host is located.</td>
</tr>
<tr>
<td>State/Province/Region</td>
<td>The state, province, or region where the host is located.</td>
</tr>
<tr>
<td>Zip/Postal Code</td>
<td>The zip code of the host location.</td>
</tr>
<tr>
<td>Country</td>
<td>The country where the host is located.</td>
</tr>
</tbody>
</table>
Optional Location Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td>The IP address of the virtual machine gateway. For example, 172.16.1.1.</td>
</tr>
<tr>
<td>DNS Search List</td>
<td>The search list of domain names.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>The DNS IP address of the primary virtual machine. For example, 172.16.1.2.</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>The DNS IP address of the secondary virtual machine. For example, 172.16.1.4</td>
</tr>
<tr>
<td>NetMask</td>
<td>The subnet mask of the virtual machine.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the location information and returns to the Locations section.</td>
</tr>
<tr>
<td>Edit</td>
<td>Updates the location information and returns to the Locations section.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the location information, and moves the host to the Unknown location section.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels the add or edit operations, and returns to the Locations section.</td>
</tr>
</tbody>
</table>

Managing the host

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 a 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.

Solution Deployment Manager only supports the Avaya Aura® Appliance Virtualization Platform and VMware ESXi hosts. If you try to add another host, the system displays the following error message:

Retrieving host certificate info is failed: Unable to communicate with host. Connection timed out: connect. Solution Deployment Manager only supports host management of VMware-based hosts and Avaya Appliance Virtualization Platform (AVP).

Before you begin

Add a location.

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. Click Application Management.
3. In Application Management Tree, select a location.
4. On the Platforms tab, in the Platforms for Selected Location <location name> section, click Add.
5. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN or IP address, user name, and password.
      For Appliance Virtualization Platform and VMware ESXi deployment, you can also provide the root user name.
   b. In Platform Type, select AVP/ESXi.
   c. If you are connected through the services port, set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6.
6. Click Save.
7. In 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, Solution Deployment Manager displays the error. To generate certificate, see VMware documentation.
   In the Application Management Tree section, the system displays the new host in the specified location. The system also discovers applications.
8. To view the discovered application details, such as name and version, establish trust between the application and System Manager doing the following:
   a. On the Applications tab, in the Applications for Selected Location <location name> section, select the required application.
   b. Click More Actions > Re-establish connection.
      For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
   c. Click More Actions > Refresh App.
   Important:
      When you change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require AVP Utilities. To get the AVP Utilities application name during the IP address or FQDN change, refresh AVP Utilities to ensure that AVP Utilities is available.
9. On the Platforms tab, select the required platform and click Refresh.

Next steps
After adding a new host under Application Management Tree, the Refresh Platform 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. In Application 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 virtual machine.

**Appliance Virtualization Platform license**

From Appliance Virtualization Platform Release 7.1.2, you must install an applicable Appliance Virtualization Platform host license file on an associated Avaya WebLM server and configure Appliance Virtualization Platform to obtain its license from the WebLM server. WebLM Server can be either embedded System Manager WebLM Server or standalone WebLM Server. Appliance Virtualization Platform licenses are according to the supported server types.

For information about Appliance Virtualization Platform licenses and supported server types, see “Appliance Virtualization Platform licenses for supported servers”.

To configure the Appliance Virtualization Platform license file:

1. Obtain the applicable license file from the Avaya PLDS website.
2. Install the license file on the System Manager WebLM Server or Standalone WebLM Server.

**Note:**

The Appliance Virtualization Platform license file can contain multiple Appliance Virtualization Platform licenses that is for four different server types. One Appliance Virtualization Platform license file contains all the necessary licenses for the complete solution.

3. Configure the applicable **WebLM IP Address/FQDN** field for each Appliance Virtualization Platform host by using either System Manager Solution Deployment Manager, Solution Deployment Manager Client, or Appliance Virtualization Platform host command line interface.

You can view the license status of the Appliance Virtualization Platform host on the **Platforms** tab of the System Manager Solution Deployment Manager or Solution Deployment Manager Client interfaces. The Appliance Virtualization Platform license statuses on the **Platforms** tab are:

- **Normal:** If the Appliance Virtualization Platform host has acquired a license, the **License Status** column displays **Normal**.

- **Error:** If the Appliance Virtualization Platform host has not acquired a license. In this case, the Appliance Virtualization Platform enters the License Error mode and starts a 30-day grace period. The **License Status** column displays **Error - Grace period expires: <DD/MM/YY> <HH:MM>**.

- **Restricted:** If the 30-day grace period of the Appliance Virtualization Platform license expires, Appliance Virtualization Platform enters the License Restricted mode and restricts the administrative actions on the host and associated virtual machines. The **License Status**
column displays **Restricted**. After you install a valid Appliance Virtualization Platform license on the configured WebLM Server, the system restores the full administrative functionality.

**Note:**

Restricted administrative actions for:

- **AVP Host:** AVP Update/Upgrade Management, Change Password, Host Shutdown, and AVP Cert. Management.
- **Application:** New, Delete, Start, Stop, and Update.

**Appliance Virtualization Platform licensing alarms**

If the Appliance Virtualization Platform license enters either License Error Mode or License Restricted Mode, the system generates a corresponding Appliance Virtualization Platform licensing alarm. You must configure the Appliance Virtualization Platform alarming. For information about how to configure the Appliance Virtualization Platform alarming feature, see *Administering Avaya Aura® AVP Utilities*.

**Appliance Virtualization Platform licenses for supported servers**

The following table describes the applicable Appliance Virtualization Platform license type for S8300E and Common Server Release 2 and 3:

<table>
<thead>
<tr>
<th>Server type</th>
<th>Appliance Virtualization Platform license feature keyword</th>
<th>Appliance Virtualization Platform license feature display name</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Avaya S8300E</td>
<td>VALUE_AVP_1CPU_EMBD_SRV R</td>
<td>Maximum AVP single CPU Embedded Servers</td>
</tr>
<tr>
<td>Common Server Release 2</td>
<td>• VALUE_AVP_1CPU_CMN_SRV R</td>
<td>• Maximum AVP single CPU Common Servers</td>
</tr>
<tr>
<td>• HP ProLiant DL360p G8</td>
<td>• VALUE_AVP_2CPU_CMN_SRV R</td>
<td>• Maximum AVP dual CPU Common Servers</td>
</tr>
<tr>
<td>• Dell™ PowerEdge ™ R620</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Server Release 3</td>
<td>• VALUE_AVP_1CPU_CMN_SRV R</td>
<td>• Maximum AVP single CPU Common Servers</td>
</tr>
<tr>
<td>• Dell™ PowerEdge ™ R630</td>
<td>• VALUE_AVP_2CPU_CMN_SRV R</td>
<td>• Maximum AVP dual CPU Common Servers</td>
</tr>
<tr>
<td>• HP ProLiant DL360 G9</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following table describes the applicable Appliance Virtualization Platform license type for Avaya Solutions Platform 120 Server:

<table>
<thead>
<tr>
<th>Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640</th>
<th>Appliance Virtualization Platform license feature keyword</th>
<th>Appliance Virtualization Platform license feature display name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile 2</td>
<td>VALUE_AVP_1CPU_CMN_SRVR</td>
<td>Maximum AVP single CPU Common Servers</td>
</tr>
</tbody>
</table>

*Table continues…*
### Configuring WebLM Server for an Appliance Virtualization Platform host using Solution Deployment Manager

#### Before you begin

1. Add an Appliance Virtualization Platform host.
   
   For information about adding a host, see *Administering Avaya Aura® System Manager*.
2. Obtain the license file from the Avaya PLDS website.
3. Install the license file on the System Manager WebLM Server or Standalone WebLM Server.

#### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section:
   a. Select the Appliance Virtualization Platform host.
   b. Click **More Actions > WebLM Configuration**.
   
   The system displays the WebLM Configuration dialog box.
4. In **WebLM IP Address/FQDN**, type the IP address or FQDN of WebLM Server.
   
   For WebLM configuration, if you select:
   - Only one host then **WebLM IP Address/FQDN** displays the existing WebLM Server IP Address.
   - Multiple hosts then **WebLM IP Address/FQDN** will be blank to assign the same WebLM Server IP Address for all the selected Appliance Virtualization Platform hosts.
5. In **Port Number**, type the port number of WebLM Server.
   
   Embedded System Manager WebLM Server supports both 443 and 52233 ports.
6. Click **Submit**.

---

<table>
<thead>
<tr>
<th>Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640</th>
<th>Appliance Virtualization Platform license feature keyword</th>
<th>Appliance Virtualization Platform license feature display name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile 3</td>
<td>• VALUE_AVP_2CPU_CMN_SRV R</td>
<td>• Maximum AVP dual CPU Common Servers</td>
</tr>
<tr>
<td></td>
<td>• VALUE_AVP_XL_SRVR</td>
<td>• Maximum AVP XL Server</td>
</tr>
<tr>
<td>Profile 4</td>
<td>VALUE_AVP_1CPU_CMN_SRVR</td>
<td>Maximum AVP single CPU Common Servers</td>
</tr>
<tr>
<td>Profile 5</td>
<td>• VALUE_AVP_2CPU_CMN_SRV R</td>
<td>• Maximum AVP dual CPU Common Servers</td>
</tr>
<tr>
<td></td>
<td>• VALUE_AVP_XL_SRVR</td>
<td>• Maximum AVP XL Server</td>
</tr>
</tbody>
</table>
The system displays the status in the **Current Action** column.

The system takes approximately 9 minutes to acquire the Appliance Virtualization Platform host license file from the configured WebLM Server. On the **Platforms** tab, click **Refresh**. When the Appliance Virtualization Platform host acquires the license, on the **Platforms** tab, the **License Status** column displays **Normal**.

### WebLM Configuration field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebLM IP Address/FQDN</td>
<td>The IP Address or FQDN of WebLM Server.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The port number of WebLM Server. The default port is 52233.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submit</td>
<td>Saves the WebLM Server configuration.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Closes the WebLM Configuration dialog box.</td>
</tr>
</tbody>
</table>

### Viewing the Appliance Virtualization Platform host license status using Solution Deployment Manager

**Procedure**

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location `<location name>` section, view the Appliance Virtualization Platform host license status in the **License Status** column.

### Shutting down the Appliance Virtualization Platform host

**About this task**

You can perform the shutdown operation on one Appliance Virtualization Platform host at a time. You cannot schedule the operation.

**Procedure**

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location `<location name>` area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Lifecycle Action** > **Host Shutdown**.

   The Appliance Virtualization Platform host and virtual machines shut down.
Restarting Appliance Virtualization Platform or an ESXi host

About this task
The restart operation fails, if you restart the host on which System Manager itself is running. If you want to restart the host, you can do this either through vSphere Client or through the Solution Deployment Manager client.

Procedure
1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. Click **More Actions > Lifecycle Action > Host Restart**.
5. On the confirmation dialog box, click **Yes**.
   The system restarts the host and virtual machines running on the host.

Removing an Appliance Virtualization Platform or ESXi host

Procedure
1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select one or more platforms that you want to delete.
3. Click **Remove**.
4. On the Delete page, click **Yes**.

Add and Edit platform field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>The location where the platform is available. The field is read only.</td>
</tr>
<tr>
<td>Platform Name</td>
<td>The platform name of OS, Appliance Virtualization Platform or ESXi.</td>
</tr>
<tr>
<td>Platform FQDN or IP</td>
<td>The IP address or FQDN of OS, Appliance Virtualization Platform or ESXi.</td>
</tr>
</tbody>
</table>
### Downloading the OVA file to System Manager

**About this task**

You can download the software from Avaya PLDS or from an alternate source to System Manager. Use the procedure to download the OVA files to your computer and upload the file to System Manager.

**Before you begin**

Set the local software library.

**Procedure**

1. Download the OVA file on your computer.
2. On the System Manager web console, click **Services > Solution Deployment Manager**.
3. In the navigation pane, click **Download Management**.
4. On the Download Management page, perform the following:
   a. In the Select Software/Hardware Types section, select the family name, and click **Show Files**.
   b. In the Select Files Download Details section, in the **Source** field, select **My Computer**.
   c. Click **Download**.
      
      The system displays the Upload File page.
5. In the **Software Library** field, select a local System Manager software library.
6. Complete the details for the product family, device type, and the software type.
7. Click **Browse** and select the OVA file from the location on the system.
8. Provide a valid file type.

This system uploads the OVA file from local computer to the designated software library on System Manager.

☆ Note:

If the file type is invalid, System Manager displays an error.

Managing the application

Editing an application

Before you begin

- Install the Solution Deployment Manager client.
- An ESXi host must be available.
- When you change the IP address or FQDN:
  - AVP Utilities must be available and must be discovered.
  - If AVP Utilities is discovered, the system must display AVP Utilities in the App Name column. If the application name in App Name is empty, click More Actions > Re-establish connection to establish trust between the application and System Manager.

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. In Application Management Tree, select a location.
3. On the Applications tab, in the Applications for Selected Location <location name> section, select an application, and click Edit.
   The system displays the Edit App section.
4. To update the IP address and FQDN of the application in the local Solution Deployment Manager inventory, perform the following:
   a. Click More Actions > Re-establish connection.

☆ Note:

To update IP address or FQDN for AVP Utilities, establish trust on all applications that are running on the host on which AVP Utilities resides.

b. Click More Actions > Refresh App.

☆ Note:

To update IP address or FQDN for AVP Utilities, refresh all applications that are running on the host on which AVP Utilities resides.

c. Click Update IP/FQDN in Local Inventory.
d. Click **Update App IP/FQDN**.
e. Provide the IP address and FQDN of the application.

**Update IP/FQDN in Local Inventory** updates the IP address or FQDN of the application only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the **Platforms** tab to update the IP address or FQDN of the host.

5. Click **Save**.

**Starting an application from Solution Deployment Manager**

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. From the **Application Management Tree**, select a platform to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to start.
4. Click **Start**.

In **Application State**, the system displays **Started**.

**Stopping an application from Solution Deployment Manager**

**About this task**

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

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. From the **Application Management Tree**, select a ESXi or vCenter host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to stop.
4. Click **Stop**.

In **Application State**, the system displays **Stopped**.

**Restarting an application from Solution Deployment Manager**

**Before you begin**

- System Manager is operational, and ESXi or vCenter is added to the Application Management page to deploy Avaya Aura® Application OVA on ESXi applications.
- Applications must be in the running state.
Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. From the application management tree, select a host to which you added applications.
3. On the Applications tab, select one or more applications that you want to restart.
4. Click Restart.
   In Application State, the system displays Stopped and then Started.

Re-establishing trust for Solution Deployment Manager elements

About this task
Use this procedure to re-establish trust with an application using the Solution Deployment Manager client.

Before you begin
• Add a location.
• Add an Appliance Virtualization Platform host to the location.

Procedure
1. To access Solution Deployment Manager, do one of the following:
   • On the System Manager web console, click Services > Solution Deployment Manager.
   • On the desktop, click the Solution Deployment Manager icon.
2. Click Application Management.
3. In Application Management Tree, select a platform.
4. On the Applications tab, in the Applications for Selected Location <location name> area, select an application.
5. Click More Actions > Re-establish connection.
6. Select the release version of the product deployed on the application.
7. Enter the user name and password for applications with the following versions:
   • 7.0
   • others
8. Click Reestablish Connection.
Common causes for application deployment failure

If the application is not reachable from System Manager Solution Deployment Manager or Solution Deployment Manager Client, the OVA deployment fails at the sanity stage, because you might have:

- Provided an IP which is not on the network.
- Provided wrong network values that causes the network configuration for the application to not work properly.
- Chosen a private virtual network.

Following are some examples of wrong network values and configuration that can result in the OVA deployment failure:

- Using an IP which is already there on the network (duplicate IP).
- Using an IP which is not on your network at all.
- Using a DNS value, such as 0.0.0.0.
- Deploying on an isolated network on your VE deployment.

You can check the deployment status in the Current Action Status column on the Applications tab.

Update Static Routing field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>The application name.</td>
</tr>
<tr>
<td>VM IP/FQDN</td>
<td>The IP address or FQDN of the application.</td>
</tr>
<tr>
<td>Utility Services IP</td>
<td>The IP address of AVP Utilities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update</td>
<td>Updates the static IP address for routing.</td>
</tr>
</tbody>
</table>

Reestablish Connection field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>The application name</td>
</tr>
<tr>
<td>VM IP/FQDN</td>
<td>The IP address or FQDN of the application</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name</td>
</tr>
<tr>
<td>Password</td>
<td>The password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reestablish Connection</td>
<td>Establishes connection between System Manager and the application.</td>
</tr>
</tbody>
</table>
Virtual machine report

You can generate a report of virtual machines that are installed on the Appliance Virtualization Platform host.

The script to generate the virtual machine report is in the /swlibrary/reports/generate_report.sh folder.

⚠️ Important:
If you run the report generation script when an upgrade is in progress on System Manager, the upgrade might fail.

generate_report.sh command

The generate_report.sh generates the virtual machine report.

Syntax

sh ./generate_report.sh [-g] [-u <SMGR UI username>] [-p <SMGR UI password>] [-s] [-a]

- The option to generate the report.
- SMGR UI user name
- System Manager Web console user name.
- SMGR UI password
- System Manager Web console password.
- The option to view the status of the generated report.
- The option to abort the generated report.

Generating a virtual machine report

Before you begin

If the application is of prior to Release 7.1, you must establish the trust with all applications before running the Report Generation utility.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the /swlibrary/reports/ directory.
3. Type the ./generate_report.sh -g -u <SMGR UI Username> -p <SMGR UI Password> command:
   For example: ./generate_report.sh -g -u admin -p password
   The system displays the following message: Executing the Report Generation script can cause the failure of upgrade that is running on the System Manager system. Do you still want to continue? [Y/N].
4. To proceed with report generation, type Y, and press Enter.
The system generates the report in the .csv format in the /swlibrary/reports/vm_app_report_DDMMYYYYxxxx.csv folder.

**Note:**
If you re-run the report generation script when the report generation process is in progress, the system displays the following message: **Report Generation Process is Already Running, Kindly try after some time.**

5. **(Optional) To view the logs, go to** /swlibrary/reports/generate_report-YYYYMMDDxxxx.log.

**Viewing the status of the virtual machine report**

**Procedure**

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the /swlibrary/reports/ directory.
3. Type the ./generate_report.sh –s command.

If the virtual machine report generation is in progress, the system displays the following message: **Report Generation Process is Running.**

**Aborting the virtual machine report generation**

**About this task**

If the virtual machine report generation process is in progress and you want to abort the report generation process, use the following procedure.

**Procedure**

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the /swlibrary/reports/ directory.
3. Type the ./generate_report.sh –a command.

The system aborts the virtual machine report generation process.

---

**Managing vCenter**

**Creating a role for a user**

**About this task**

To manage a vCenter or ESXi in Solution Deployment Manager, you must provide complete administrative-level privileges to the user.

Use the following procedure to create a role with administrative-level privileges for the user.
Procedure

1. Log in to vCenter Server.
2. On the Home page, click **Administration > Roles**.
   
   The system displays the Create Role dialog box.
3. In **Role name**, type a role name for the user.
4. To provide complete administrative-level privileges, select the **All Privileges** check box.
5. **(Optional)** To provide minimum mandatory privileges, do the following.
   a. In All Privileges, select the following check boxes:
      - Datastore
      - Datastore cluster
      - Distributed switch
      - Folder
      - Host profile
      - Network
      - Resource
      - Tasks
      - Virtual machine
      - vApp

   Note:

   You must select all the subprivileges under the list of main set of privileges. For example, when you select the **Distributed switch** check box, ensure that you select all the related subprivileges. This is applicable for all the main privileges mentioned above. If you do not select all the subprivileges, the system might not work properly.

   b. In All Privileges, expand **Host**, and select the **Configuration** check box.

   Note:

   You must select all the subprivileges under **Configuration**.

6. Click **OK** to save the privileges.

**Next steps**

Assign this role to the user for mapping vCenter in Solution Deployment Manager. To assign the role to the user, see the VMware documentation.

**Adding a vCenter to Solution Deployment Manager**

**About this task**

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, and 6.7. When you add vCenter, System Manager discovers the ESXi hosts that this
vCenter manages, adds to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository. System Manager displays vCenter, ESXi host, and virtual machines on the Manage Elements page.

Before you begin
Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. In the New vCenter section, provide the following vCenter information:
   a. In **vCenter FQDN**, type FQDN of vCenter.
      - For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
      - The FQDN value must match with the value of the **SAN** field of the vCenter certificate. The FQDN value is case sensitive.
   b. In **User Name**, type the user name to log in to vCenter.
   c. In **Password**, type the password to log in to vCenter.
   d. In **Authentication Type**, select **SSO** or **LOCAL** as the authentication type.
      - If you select the authentication type as **SSO**, the system displays the **Is SSO managed by Platform Service Controller (PSC)** field.
   e. **(Optional)** If PSC is configured to facilitate the SSO service, select **Is SSO managed by Platform Service Controller (PSC)**.
      - PSC must have a valid certificate.
      - The system enables **PSC IP or FQDN** and you must provide the IP or FQDN of PSC.
   f. **(Optional)** In **PSC IP or FQDN**, type the IP or FQDN of PSC.
5. Click **Save**.
6. On the certificate dialog box, click **Accept Certificate**.
   - The system generates the certificate and adds vCenter.
   - In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

Related links
- [Editing vCenter](#) on page 43
Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select a vCenter server and click **Edit**.
4. In the Edit vCenter section, change the vCenter information as appropriate.
5. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.
6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:
   - Select an ESXi host and click the edit icon ().[1]
   - Select one or more ESXi hosts, select the location, click **Bulk Update > Update**.
7. Click **Commit** to get an updated list of managed and unmanaged hosts.

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
4. Click **Yes** to confirm the deletion of servers.

The system deletes the vCenter from the inventory.
### Map vCenter field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the vCenter server.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address of the vCenter server.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The FQDN of the vCenter server.</td>
</tr>
</tbody>
</table>

**Note:**
- Use FQDN to successfully map and log in to vCenter from Solution Deployment Manager. With IP address, the system displays an error message about the incorrect certificate and denies connection.

<table>
<thead>
<tr>
<th>License</th>
<th>The license type of the vCenter server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The license status of the vCenter server.</td>
</tr>
<tr>
<td>Certificate Status</td>
<td>The certificate status of the vCenter server. The options are:</td>
</tr>
<tr>
<td></td>
<td>• 🟢: The certificate is correct.</td>
</tr>
<tr>
<td></td>
<td>• ❌: The certificate is not accepted or invalid.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Displays the certificate status details of the vCenter server.</td>
</tr>
<tr>
<td>Generate/Accept Certificate</td>
<td>Displays the certificate dialog box where you can generate and accept a certificate for vCenter. For vCenter, you can only accept a certificate. You cannot generate a certificate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Displays the New vCenter page where you can add a new ESXi host.</td>
</tr>
<tr>
<td>Edit</td>
<td>Displays the Edit vCenter page where you can update the details and location of ESXi hosts.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the ESXi host.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Updates the list of ESXi hosts in the Map vCenter section.</td>
</tr>
</tbody>
</table>

### New vCenter and Edit vCenter field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter FQDN</td>
<td>FQDN of vCenter.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user name to log in to vCenter.</td>
</tr>
<tr>
<td>Password</td>
<td>The password that you use to log in to vCenter.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>The authentication type that defines how Solution Deployment Manager performs user authentication. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>SSO</strong>: Global username used to log in to vCenter to authenticate to an external Active Directory authentication server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>LOCAL</strong>: User created in vCenter</td>
</tr>
<tr>
<td><strong>Is SSO managed by Platform Service Controller (PSC)</strong></td>
<td>The check box to specify if PSC manages SSO service. When you select the check box, the system enables <strong>PSC IP or FQDN</strong>.</td>
</tr>
<tr>
<td>PSC IP or FQDN</td>
<td>The IP or FQDN of PSC.</td>
</tr>
<tr>
<td><strong>Button</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Save</td>
<td>Saves any changes you make to FQDN, username, and authentication type of vCenter.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the vCenter details.</td>
</tr>
</tbody>
</table>

**Managed Hosts**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP/FQDN</td>
<td>The name of the ESXi host.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The IP address of the ESXi host.</td>
</tr>
<tr>
<td>Location</td>
<td>The physical location of the ESXi host.</td>
</tr>
<tr>
<td>IPv6</td>
<td>The IPv6 address of the ESXi host.</td>
</tr>
<tr>
<td>Edit</td>
<td>The option to edit the location and host.</td>
</tr>
<tr>
<td><strong>Bulk Update</strong></td>
<td>Provides an option to change the location of more than one ESXi hosts.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>You must select a location before you click Bulk Update.</td>
</tr>
<tr>
<td><strong>Update</strong></td>
<td>Saves the changes that you make to the location or hostname of the ESXi host.</td>
</tr>
<tr>
<td><strong>Commit</strong></td>
<td>Commits the changes that you make to the ESXi host with location that is managed by vCenter.</td>
</tr>
</tbody>
</table>
Preupgrade tasks

### Unmanaged Hosts

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP/FQDN</td>
<td>The name of the ESXi host.</td>
</tr>
<tr>
<td>ESXi Version</td>
<td>Displays the versions of the ESXi host linked to vCenter FQDN.</td>
</tr>
<tr>
<td>IPv6</td>
<td>The IPv6 address of the ESXi host.</td>
</tr>
</tbody>
</table>

**Note:** For Release 8.1, do not select the 5.0 and 5.1 versions.

### Button

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commit</td>
<td>Saves all changes that you made to vCenter on the Map vCenter page.</td>
</tr>
</tbody>
</table>

---

### Applications pre-upgrade functions

#### Refreshing elements

**Before you begin**
- On the User Settings page, configure the user settings.

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select one or more devices.
   b. Click **Pre-upgrade Actions > Refresh Element(s)**.
4. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

The **Last Action Status** column displays ✓ and the **Current Version** column displays the current version of the element.

---

August 2020  
Upgrading standalone Avaya WebLM  
Comments on this document? infodev@avaya.com
Analyzing software

About this task

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Custom patching does not require the analyze operation.

Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Perform the Refresh elements operation.

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager.
2. In the navigation pane, click Upgrade Management.
3. On the Upgrade Management page, do the following:
   a. Select a device that you want to analyze.
   b. Click Pre-upgrade Actions > Analyze.
4. On the Job Schedule page, click one of the following:
   - Run Immediately: To perform the job.
   - Schedule later: To perform the job at a scheduled time.
5. If you select Schedule later, select the date, time, and timezone.
6. Click Schedule.

   The Last Action Status column displays a ✔️, the Current Version column displays the current version of the element, and the Entitled Upgrade Version column displays the next version of the element for which the element is entitled to be upgraded.

Downloading the software

About this task

You can download the software releases that you are entitled from Avaya PLDS, or from an alternate source to System Manager.

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager.
2. In the navigation pane, click Upgrade Management.
3. On the Upgrade Management page, select an element from the list.
4. In the left navigation pane, click **Download Management**.

   The system displays the File Download Manager page.

5. To change the display settings, click one of the following:

   - **Tree View**: To view the list of elements in the tree format. The system displays each element with the list of components associated with the element that you selected.
   - **List View**: To view the list of elements in the list format. Every element is displayed individually.

6. In **Select Software/Hardware Types**, select the software or firmware that you want to download.

7. To get the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page, click **Refresh Families**.

   The time to complete the refresh operation depends on the source configuration in **User Settings**.

8. Click **Show Files**.

9. In **Select Files Download Details**, do the following:

   a. In **Source**, click **Avaya PLDS/Alternate Source** or **My Computer** from where you want to download the files.
   b. Select the files that you want to download.
   c. Click **Download**.

   In File Download Status, the system displays the file that you selected for download.

---

**File Download Manager field descriptions**

**Select Software/Hardware Types**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family Name</td>
<td>The name of the device family.</td>
</tr>
<tr>
<td>Hardware/Software</td>
<td>The name of the associated software or hardware.</td>
</tr>
</tbody>
</table>

**Select Files Download Details**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The source from where Download Manager gets the software or firmware files. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Avaya PLDS/Alternate Source</td>
</tr>
<tr>
<td></td>
<td>• My Computer</td>
</tr>
</tbody>
</table>
### Name | Description
---|---
File name | The file name.
Version | The file version.
Entitled | The file entitlements.
Hardware/Software | The name of the hardware or the software.
Family Name | The name of the device family.
Content Type | The type of the content.
Software Library | The status of the file download.
File Description | A description of the file that you download.

| Button | Description |
---|---
Refresh Families | Gets the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page.  
**Note:** When you add or update details in the versions.xml file, you must click Refresh Families to get the updated information.
Show Files | Displays the files associated with the element that you selected.

### File Download Status

| Name | Description |
---|---
File Name | The file name of the software or firmware file.
Job Name | The name of the download job.
Current Step | The current status.
Percentage Completed | The status of completion.
Status | The status of the download activity.
Scheduled By | The user who scheduled the download job.

| Button | Description |
---|---
Delete | Deletes the files that you have selected.

---

**Performing the preupgrade check**

**Procedure**

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

3. On the Upgrade Management page, do the following:
   a. Select an application to upgrade.
   b. Click **Pre-upgrade Actions > Pre-upgrade Check**.

4. On the Pre-upgrade Configuration page, fill in the required information.

   **Note:**
   To upgrade to different server, in **Target Host**, select the target server host.

5. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.

6. Click **Schedule**.

   On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a ✔.

---

**Preupgrade Configuration field descriptions**

**Pre upgrade Configuration Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element name</td>
<td>The name of the application that you want to upgrade.</td>
</tr>
<tr>
<td>Parent name</td>
<td>The parent of the application that you want to upgrade.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the application that you want to upgrade.</td>
</tr>
<tr>
<td>Current Version</td>
<td>The current version of the application that you want to upgrade.</td>
</tr>
<tr>
<td>Target Platform</td>
<td>The Appliance Virtualization Platform or ESXi host of the virtual machine.</td>
</tr>
<tr>
<td>Data Store</td>
<td>The data store.</td>
</tr>
<tr>
<td></td>
<td>When you set the <strong>Target Host</strong> as <strong>Same Box</strong>, the system enables the</td>
</tr>
<tr>
<td></td>
<td><strong>Data Store</strong> field.</td>
</tr>
<tr>
<td>New Target Platform</td>
<td>The Appliance Virtualization Platform or ESXi host to which you want to</td>
</tr>
<tr>
<td></td>
<td>upgrade the virtual machine.</td>
</tr>
<tr>
<td></td>
<td>For upgrades on a different server, add Appliance Virtualization Platform</td>
</tr>
<tr>
<td></td>
<td>or ESXi host from Application Management.</td>
</tr>
<tr>
<td>Upgrade Source</td>
<td>The location where OVA or the software patches are available in the local</td>
</tr>
<tr>
<td></td>
<td>storage or remote server.</td>
</tr>
<tr>
<td>Upgrade/Update To</td>
<td>The OVA file or the software patch to which you want to upgrade.</td>
</tr>
<tr>
<td>Flexi Footprint</td>
<td>The file based on the storage, CPU, and memory capacity of your system.</td>
</tr>
</tbody>
</table>
Upgrading VMware ESXi version

About this task

If the ESXi upgrade is required for upgrading the application to Release 8.1.x, use the following procedure to upgrade the ESXi to a supported ESXi version.

For information about the supported ESXi version, see Supported ESXi version on page 16.

Procedure

1. Shut down all the virtual machines that are hosted on the ESXi.
2. Put the ESXi into maintenance mode.
   For information about performing steps on ESXi, see VMware product documentation website.
3. Upgrade ESXi to supported ESXi version.
   For information about upgrading ESXi, see VMware product documentation website.
4. Reboot the ESXi host.
5. Exit from the ESXi maintenance mode.
Preupgrade tasks

6. Apply the license key for the upgraded ESXi.
7. Power on the virtual machines.
Chapter 5: Upgrading WebLM to Appliance Virtualization Platform and VMware

Upgrading WebLM to Release 8.1.1 by using System Manager Solution Deployment Manager

About this task
Use the procedure to upgrade WebLM to Release 8.1.1 from:
• Release 7.x or 8.0.x on Appliance Virtualization Platform or on VMware.
• Release 6.x on VMware.

Before you begin
• Ensure that Appliance Virtualization Platform and AVP Utilities are running on Release 8.1.1.
• Ensure that System Manager is running on Release 8.1.1.
• Add a location.
  For information, see Adding a location on page 25.
• Add the ESXi, vCenter, or Appliance Virtualization Platform host.
  For information about adding the Appliance Virtualization Platform or ESXi host, see Adding an Appliance Virtualization Platform or ESXi host on page 27.
  For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 41.

Important:
- If application is running on the ESXi version that is not supported with Release 8.1.x, then first upgrade the ESXi to supported ESXi version.
  For information about the supported ESXi version, see Supported ESXi version on page 16.
  For information about upgrading the ESXi, see the VMware product documentation.
- If ESXi is managed by vCenter, ensure that the vCenter version is same or higher than the ESXi version.
If application is running on the server that is not supported with Release 8.1.x, then deploy Appliance Virtualization Platform and AVP Utilities on supported server on latest release.

For information about supported servers, see Supported servers for Avaya Aura applications on page 14.

- Select the WebLM virtual machine and click More Actions > Re-establish connection to establish the trust.

For information, see Re-establishing trust for Solution Deployment Manager elements on page 37.

Note: For WebLM Release 6.x on VMware, trust establishment is not required.

- Obtain the WebLM software. See “Software details of WebLM”.

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager.
2. In the navigation pane, click Upgrade Management.
3. Select WebLM, click Pre-Upgrade Actions > Refresh Element(s).
4. On the next page, click Schedule.
   You can schedule the job now or for a later time.
5. After refresh is done, select Pre-Upgrade Actions > Analyze.
6. On the next page, click Schedule.
   You can schedule the job now or for a later time.
7. After refresh is done, click Pre-Upgrade Actions > Pre-upgrade Check.
8. On the Pre-upgrade Configuration page, do the following:
   a. Do one of the following:
      • For same server, provide the mandatory parameters along with the same target host information.
      • For different server, provide the mandatory parameters along with different target host information.
      For information about parameters, see Preupgrade Configuration field descriptions on page 50.
   b. In the Job Schedule section, click Schedule.
      You can schedule the job now or for a later time.
9. Select WebLM.
10. Click Upgrade Actions > Upgrade/Update.
11. On the Upgrade Configuration page, select the Override preupgrade check check box.
When you select the check box, the upgrade process continues even when the recommended checks fail in preupgrade check.

12. To provide the upgrade configuration details, click **Edit**.

13. On the Edit Upgrade Configuration page, perform the following:

   a. Do one of the following:

      • For same server, provide the mandatory parameters along with same target host information, latest patch file, and credentials

      • For different server, provide the mandatory parameters along with different target host information, latest patch file, and credentials

      For information about parameters, see *Edit Upgrade Configuration field descriptions* on page 56.

   b. Complete the details, and click **Save**.

14. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✔.

   If the field displays ✗, review the information on the Edit Upgrade Configuration page.

15. Click **Save**.

16. To save the configuration, click **Save Configuration**.

   The update configuration is saved as a job in the Upgrade Jobs Status page.

17. On the Upgrade Configuration page, click **Upgrade**.

18. On the Job Schedule page, click one of the following:

   • **Run Immediately**: To perform the job.

   • **Schedule later**: To perform the job at a scheduled time.

19. Click **Schedule**.

20. Click **Upgrade**.


   The **Last Action** column displays **Upgrade**, and the **Last Action Status** column displays ✔.

22. To Commit or Rollback, do the following:

   a. On the Upgrade Management page, select the element.

   b. Click **Upgrade Actions > Commit/Rollback Upgrade**.

      The system displays the Job Schedule page.

   c. Select the action to be performed under the **Upgrade Action** column.

   d. Click **Run Immediately** to perform the job or click **Schedule later** to perform the job at a scheduled time.
e. Click **Schedule**.

When you commit the changes, the system deletes the old virtual machine.

When you rollback, the system deletes the newly created virtual machine and starts the old virtual machine.

23. To view the upgrade status, perform the following:
   a. In the navigation pane, click **Upgrade Job Status**.
   b. In **Job Type**, click **Upgrade**.
   c. Click the upgrade job that you want to view.

**Next steps**

Verify the version of the WebLM to ensure that the upgrade is successful.

**Related links**

- [Verifying the WebLM software version](#) on page 72

---

**Edit Upgrade Configuration field descriptions**

Edit Upgrade Configuration has following tabs:

- **Element Configuration**
- **AVP Configuration**

**Element Configuration: General Configuration Details**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>The system name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the device.</td>
</tr>
<tr>
<td>Operation</td>
<td>The operation that you want to perform on the device. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Upgrade/Migration</td>
</tr>
<tr>
<td></td>
<td>• Update</td>
</tr>
<tr>
<td>ESXi/AVP host/Platform</td>
<td>The host on which you want to run the device. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Same Box</td>
</tr>
<tr>
<td></td>
<td>• Software Only</td>
</tr>
<tr>
<td></td>
<td>• List of hosts that you added from Application Management</td>
</tr>
<tr>
<td>New Target ESXi/AVP host/</td>
<td>The new target host on which you want to run the device.</td>
</tr>
<tr>
<td>Platform</td>
<td></td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrate With AVP Install</td>
<td>The option to migrate System Platform-based Communication Manager Release 6.3.x or 6.4.x to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager.</td>
</tr>
</tbody>
</table>
| Upgrade Source                            | The source where the installation files are available. The options are:  
  • SMGR_DEFAULT_LOCAL  
  • Remote Software Library                                                                                                                                                                                                                                                                                                                                                           |
| Upgrade To                                | The OVA file to which you want to upgrade.  
  When you select the local System Manager library, the system displays the fields and populates most of the data in the Upgrade Configuration Details section.                                                                                                                                                                                                                                           |
| Service/Feature Pack for auto-install after upgrade/migration | The service pack or feature pack that you want to install.                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Element Configuration: Upgrade Configuration Details**

The page displays the following fields when you upgrade Communication Manager and the associated devices. The page displays all values from the existing system. If the system does not populate the values, manually add the values in the mandatory fields.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Commit</td>
<td>The option to automatically commit the upgrade.</td>
</tr>
<tr>
<td>Existing Administrative User</td>
<td>The user name with appropriate admin privileges.</td>
</tr>
<tr>
<td>Existing Administrative Password</td>
<td>The password of the administrator.</td>
</tr>
</tbody>
</table>
| Pre-populate Data                         | The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway.  
  For Communication Manager Messaging, the button is unavailable and you must fill in all details.  
  For Communication Manager Messaging you must provide a new IP address.                                                                                                                                                                                                                                                                                       |
<p>| CM IPv4 Address                           | The IP address of the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| CM IPv4 Netmask                           | The network mask of the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| CM IPv4 Gateway                           | The default gateway of the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| CM IPv6 Address                           | The IPv6 address of the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| CM IPv6 Network Prefix                    | The IPv6 network prefix of the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| CM IPv6 Gateway                           | The IPv6 default gateway of the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                             |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out of Band Management IPv4 Address</td>
<td>The IP address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.</td>
</tr>
<tr>
<td>Out of Band Management Netmask</td>
<td>The subnet mask of the virtual machine for out of band management.</td>
</tr>
<tr>
<td>Out of Band Management IPv6 Address</td>
<td>The IPv6 address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.</td>
</tr>
<tr>
<td>Out of Band Management IPv6 Network Prefix</td>
<td>The IPv6 network prefix of the virtual machine for out of band management.</td>
</tr>
<tr>
<td>CM Hostname</td>
<td>The hostname of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>NTP Servers</td>
<td>The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>The DNS IP address of the virtual machine.</td>
</tr>
<tr>
<td>Search Domain List</td>
<td>The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).</td>
</tr>
<tr>
<td>WebLM Server IPv4 Address</td>
<td>The IP address of WebLM. The field is mandatory.</td>
</tr>
<tr>
<td>CM Privileged Administrator User Login</td>
<td>The login name for the privileged administrator. You can change the value at any point of time.</td>
</tr>
<tr>
<td>CM Privileged Administrator User Password</td>
<td>The password for the privileged administrator. You can change the value at any point of time.</td>
</tr>
<tr>
<td>Flexi Footprint</td>
<td>The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.</td>
</tr>
<tr>
<td>Public</td>
<td>The port number that you must assign to public port group.</td>
</tr>
<tr>
<td>Out of Band Management</td>
<td>The port number that is assigned to the out of band management port group. The field is available only when you select a different host.</td>
</tr>
<tr>
<td>Private</td>
<td>Tan exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.</td>
</tr>
<tr>
<td>Services</td>
<td>The port number that is assigned to the services port. The system displays this field when Utility Services is available.</td>
</tr>
</tbody>
</table>
### Name
#### Description

**Duplication link**
- The port number assigned to a dedicated HA sync links. For example, Communication Manager duplex crossover that is assigned to an exclusive physical NIC. The installer selects free server NIC during the deployment process.
- The field is available only for the Communication Manager duplex configuration and when you select a different host.

**Datastore**
- The datastore on the target ESXi host.
- The field is available only when you select a different host.

---

The page displays the following fields when you upgrade Session Manager.

### Name
#### Description

**Existing Administrative User**
- The user name of the administrator.

**Existing Administrative Password**
- The password of the administrator.

**Pre-populate Data**
- The option to get the configuration data displayed in the fields.

**IP Address**
- The IP address of the virtual machine.

**Short Hostname**
- The hostname of the virtual machine.
- The hostname of the server and is often aligned with the DNS name of the server.

**Network Domain**
- The domain name of the virtual machine.

**Netmask**
- The network mask of the virtual machine.

**Default Gateway**
- The default gateway of the virtual machine.

**DNS Servers**
- The DNS IP address of the virtual machine.

**Timezone**
- The timezone of the virtual machine.

**Login Name**
- The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).

**Enter Customer Account Password**
- Password to log on to the system.

**Primary System Manager IP**
- The IP address of System Manager.

**Enrollment Password**
- The password that is required to establish trust between System Manager and Session Manager.

**Flexi Footprint**
- The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.

**Public**
- The port number that you must assign to public port group.

*Table continues…*
### Element Configuration: End User License Agreement

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Agree to the above end user license agreement</td>
<td>The end user license agreement. You must select the check box to accept the license agreement.</td>
</tr>
</tbody>
</table>

### AVP Configuration: Existing Machine Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>The source IP address.</td>
</tr>
<tr>
<td>Source Administrative User</td>
<td>The source user name with appropriate admin privileges.</td>
</tr>
<tr>
<td>Source Administrative Password</td>
<td>The source password of the administrator.</td>
</tr>
<tr>
<td>Source Root User</td>
<td>The source user name with appropriate root privileges.</td>
</tr>
<tr>
<td>Source Root Password</td>
<td>The source password of the root.</td>
</tr>
</tbody>
</table>

### AVP Configuration: Configuration Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Upgrade Source         | The source where the installation files are available. The options are:  
  - SMGR_DEFAULT_LOCAL  
  - Remote Software Library  
| Upgrade To             | The OVA file to which you want to upgrade.  
When you select the local System Manager library, the system displays the fields and populates most of the data in the Configuration Details section. |
| Dual Stack Setup (with IPv4 and IPv6) | Enables or disables the fields to provide the IPv6 addresses. |
| AVP Management IPv4 Address | IPv4 address for the Appliance Virtualization Platform host. |

Table continues...
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVP IPv4 Netmask</td>
<td>IPv4 subnet mask for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>AVP Gateway IPv4 Address</td>
<td>IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.</td>
</tr>
<tr>
<td>AVP Hostname</td>
<td>Hostname for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td></td>
<td>The hostname:</td>
</tr>
<tr>
<td></td>
<td>• Can contain alphanumeric characters and hyphen</td>
</tr>
<tr>
<td></td>
<td>• Can start with an alphabetic or numeric character</td>
</tr>
<tr>
<td></td>
<td>• Must contain at least 1 alphabetic character</td>
</tr>
<tr>
<td></td>
<td>• Must end in an alphanumeric character</td>
</tr>
<tr>
<td></td>
<td>• Must contain 1 to 63 characters</td>
</tr>
<tr>
<td>AVP Domain</td>
<td>Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.</td>
</tr>
<tr>
<td>IPv4 NTP server</td>
<td>IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com</td>
</tr>
<tr>
<td>Secondary IPv4 NTP Server</td>
<td>Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.</td>
</tr>
<tr>
<td>Main IPv4 DNS Server</td>
<td>Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.</td>
</tr>
<tr>
<td>Secondary IPv4 DNS server</td>
<td>Secondary IPv4 address of customer DNS server. One DNS server entry in each line.</td>
</tr>
<tr>
<td>AVP management IPv6 address</td>
<td>IPv6 address for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>AVP IPv6 prefix length</td>
<td>IPv6 subnet mask for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>AVP gateway IPv6 address</td>
<td>IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.</td>
</tr>
<tr>
<td>IPv6 NTP server</td>
<td>IPv6 address or FQDN of customer NTP server.</td>
</tr>
<tr>
<td>Secondary IPv6 NTP server</td>
<td>Secondary IPv6 address or FQDN of customer NTP server.</td>
</tr>
<tr>
<td>Main IPv6 DNS server</td>
<td>Main IPv6 address of customer DNS server. One DNS server entry in each line.</td>
</tr>
<tr>
<td>Secondary IPv6 DNS server</td>
<td>Secondary IPv6 address of customer DNS server. One DNS server entry in each line.</td>
</tr>
<tr>
<td>Public VLAN ID (Used on S8300E only)</td>
<td>VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use Public VLAN ID only on the S8300E server.</td>
</tr>
<tr>
<td>Enable Stricter Password (14 char pass length)</td>
<td>The check box to enable or disable the stricter password. The password must contain at least 14 characters.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
**AVP Super User Admin Password** | Admin password for Appliance Virtualization Platform. The password must contain at least 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.

**Enhanced Access Security Gateway (EASG)** | **Enable: (Recommended)** By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

**Disable** By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya’s ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.

Enter 1 to Enable EASG (Recommended) or 2 to **Disable** EASG.

**WebLM IP/FQDN** | The IP Address or FQDN of WebLM Server.

**WebLM Port Number** | The port number of WebLM Server. The default port is 52233.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save</strong></td>
<td>Saves the changes that you made to the Edit Upgrade Configuration page.</td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td>Cancels the changes that you made to the Edit Upgrade Configuration page.</td>
</tr>
</tbody>
</table>
Installing a WebLM patch, feature pack, or service pack

Before you begin
- Create backup of WebLM.
- Copy the patch file, feature pack file, or the service pack file to the WebLM server.
- Verify the installed WebLM version.

Procedure
1. Log in to the WebLM command line interface with administrator privilege CLI user credentials.
2. Verify the MD5 checksum of the patch file that you want to install.
3. Type `WebLMPatchdeploy <absolute path to the WebLM feature pack file>`.
   For example, `WebLMPatchdeploy /home/avaya/VEWebLM_8.1.x.0_xxx.bin`.
   The system installs the patch file.
4. To accept the license terms, read the End User License Agreement carefully, and type `Y`.
   The patch installation takes about 10–15 minutes to complete. You can view to monitor the WebLM patch progress status from the `/var/log/Avaya/WebLM_Patch.log` file.
   If the installation is successful, the system displays a warning message on the dashboard and on the command line interface to restart WebLM if kernel is updated.
5. After patch installation is successful, relogin to CLI to check if the updated kernel is running.
6. Restart the standalone WebLM.

Next steps
If the patch or service pack installation fails, perform a snapshot restore to go to the previous version of WebLM.

Note:
Modifying the network or management configuration is not recommended before the patch deployment.

Upgrading WebLM by using CLI

About this task
Use the following procedure to upgrade WebLM manually.
Note:
When you manually upgrade WebLM without using Solution Deployment Manager, the WebLM host id changes.

Procedure
1. Take the backup of the old WebLM server.
   For information about taking the backup, see Performing WebLM backup on page 82.
2. Turn off the old WebLM server in case you are deploying WebLM by using the same IP Address.
4. Apply the latest WebLM patch, if required.
   For information about applying the patch file, see Installing a WebLM patch, feature pack, or service pack on page 63.
5. Restore the backup on the new WebLM server.
   For information about restoring the backup, see Performing WebLM restore on page 82.
6. Generate new licenses and install on new WebLM.
7. Ensure new WebLM is operational.
8. Delete the old version of the WebLM server.

Next steps
After upgrading the system:
• Regenerate the license files because the host ID changes.
• Recreate the users to administrate the WebLM web console, if required.
Chapter 6: Upgrading WebLM to KVM environment

Migration path for KVM

You can migrate to WebLM Release 8.1.1 on KVM from the following:

- Release 8.0.x on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.
- Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment or on AWS.
- Release 6.x on VMware in customer-provided Virtualized Environment.

Upgrading to KVM environment

You can upgrade Standalone WebLM to Release 8.1.x on KVM environment by performing fresh deployment of the application. For detailed information, see the KVM deployment section in Deploying standalone Avaya WebLM in Virtualized Environment document.

For information about upgrading the system using CLI, see Upgrading WebLM by using CLI on page 63.
Chapter 7: Upgrading WebLM to IaaS environment

Migration path for IaaS
You can migrate to WebLM Release 8.1.1 on IaaS from the following:

• Release 8.0.x on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.

• Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment or on AWS.

• Release 6.x on VMware in customer-provided Virtualized Environment.

Upgrading to IaaS environment
You can upgrade Standalone WebLM to Release 8.1.x on IaaS environment by performing fresh deployment of the application. For detailed information, see the Deploying standalone Avaya WebLM in Infrastructure as a Service Environment document.

For information about upgrading the system using CLI, see Upgrading WebLM by using CLI on page 63.
Chapter 8: Upgrading WebLM to Software-only environment

Migration path for Software-only environment

You can migrate to WebLM Release 8.1.1 on Software-only environment from the following:

- Release 8.0.x on Appliance Virtualization Platform on Avaya-provided server or on VMware/KVM in customer-provided Virtualized Environment or on AWS/Google Cloud/Microsoft Azure on IaaS or on Software-only environment.
- Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment or on AWS.
- Release 6.x on VMware in customer-provided Virtualized Environment.

Upgrading to Software-only environment using manual backup and restore method

You can upgrade Standalone WebLM to Release 8.1.x on Software-only environment by performing fresh deployment of the application. For detailed information, see the Deploying standalone Avaya WebLM in Software-Only Environment document.

For information about upgrading the system using CLI, see Upgrading WebLM by using CLI on page 63.

Upgrading from AVP or VMware based WebLM to Software-only environment by using System Manager Solution Deployment Manager

About this task

The procedure describes the steps to upgrade Appliance Virtualization Platform or VMware based WebLM Release 7.x or 8.0.x to WebLM Release 8.1.1 on Software-only environment.
Note:
Follow this procedure to upgrade to Release 8.1 on Hyper-V systems.

Before you begin

• Ensure that System Manager is running on Release 8.1.x.
• Add a location.
  For information, see Adding a location on page 25.
• Add the ESXi, vCenter, or Appliance Virtualization Platform host from the Application Management page.
• Select the WebLM application and click More Actions > Re-establish connection to establish the trust. For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
• Obtain the WebLM application ISO for Software-only environment and the latest service or feature pack file.

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager.
2. In the navigation pane, click Upgrade Management.
3. On the Upgrade Management page, select the WebLM virtual machine.
4. Click Upgrade.
5. On Select Platform, select the Software Only check box.
6. Click Continue.
   Solution Deployment Manager takes the backup and shuts down the virtual machine.
7. Click the Refresh icon until the Upgrade Status changes to Upgrading (PAUSED)...RESUME state.
8. Manually install and configure the RHEL OS with the same IP address of the old WebLM virtual machine.
9. Once the RHEL system is configured and running, access Solution Deployment Manager, and go to Add Platform to add the newly added Software-only platform.
10. On the Add Platform dialog box, configure the following options:
    • Platform Name: Type the name of the platform.
    • Platform FQDN or IP: Type the FQDN or IP address of the platform, that is, the RHEL system created for software-only.
    • User Name: Type the user name to access the platform.
    • Password: Type the password to access the platform.
    • Platform Type: Select platform type as OS for Software-only upgrade.
11. Click Save.
12. Click **Upgrade Management > Upgrade Elements** and, then click **RESUME** displayed under the **Upgrade Status** column.

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

14. Click **Next**.

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

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

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

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

17. Click **Next**.

18. In **Flexi Footprint**, select the footprint size for the application.

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

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

⚠️ **Note:**

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

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

The system displays the Environment Check Output window.

21. Click **Next**.

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

   For a **Software-Only** application upgrade, the **Network Parameters** tab is disabled.

23. Click **Upgrade**.

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

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

25. To continue with the upgrade, click **Accept**.

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

26. To view details, click **Status Details**.
## Chapter 9: Post-deployment and upgrade verifications

### Post-upgrade checklist

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Tasks</th>
<th>Links/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log on to the WebLM web console and verify the WebLM <code>&lt;version_number&gt;</code>.</td>
<td>See <a href="#">Logging on to the WebLM web console</a> on page 71.</td>
</tr>
<tr>
<td>2</td>
<td>Rehost the license file that you generated on the WebLM server.</td>
<td>See <a href="#">Rehosting license files</a> on page 72. For more details, refer <a href="#">Administering Avaya WebLM</a>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you had upgraded the application by using Solution Deployment Manager client, you do not need to rehost the license file separately.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Configure the EASG settings, if required.</td>
<td>See <a href="#">Enhanced Access Security Gateway (EASG) overview</a> on page 76.</td>
</tr>
<tr>
<td>4</td>
<td>Rollback the upgrade in case the upgrade fails.</td>
<td>See <a href="#">Rolling back an upgrade</a> on page 76.</td>
</tr>
<tr>
<td>5</td>
<td>Delete the virtual machine snapshots, if required.</td>
<td>-</td>
</tr>
</tbody>
</table>

### Logging on to the WebLM web console

**About this task**

The WebLM web console is the main interface of Avaya WebLM. You must log on to the WebLM web console to perform any task. The WebLM home page displays the navigation menu that provides access to shared services to perform operations that WebLM supports.
Before you begin
Get a user account to log on to the WebLM web console. To create a new account, go to the Avaya Support website at https://support.avaya.com.

Procedure
1. On a web browser, type the WebLM URL: https://<Fully Qualified Domain Name>>:52233/WebLM.
2. In the User Name field, type the user name.
3. In the Password field, type the password.
4. Click Log On.

WebLM validates the user name and password with the WebLM user account and displays the home page with the WebLM <version_number>. If the match fails, WebLM displays an error message and prompts you to reenter the user name and password.

Rehosting license files
Procedure
2. On the Server Properties page, note the WebLM server host ID.
3. Go to the PLDS website regenerate the license file for your product using the same host ID.
4. Install the license file that you generated on the WebLM server.

For more information about installing a license file, see Administering Avaya WebLM.

Verifying the WebLM software version

About this task
To verify the WebLM version, perform the following procedure after you deploy or upgrade WebLM.

• On the WebLM console, do the following:
  1. Log on to the WebLM web console with administrator privilege credentials.
  2. On the home page, click About.
     The system displays the About WebLM window with the build details.
  3. Verify the software version of WebLM.
On the WebLM command line interface, do the following:

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

2. Type `swversion`.

### StandAlone WebLM Software Information

Standalone WebLM 8.1.x Build Number 8.1.1.xxxx Patch 8.1.x Build Number 8.1.x.x.xxxxx

---

**Upgrade job status**

**Upgrade job status**

The Upgrade Job Status page displays the status of completion of every upgrade job that you performed. Every step that you perform to upgrade an application by using Solution Deployment Manager is an upgrade job. You must complete the following jobs to complete the upgrade:

1. **Refresh Element(s):** To get the latest data like version data for the applications in the system.
2. **Analyze:** To evaluate an application that completed the Refresh Element(s) job.
3. **Pre-Upgrade Check:** To evaluate an application that completed the Analyze job.
4. **Upgrade:** To upgrade applications that completed the Pre-upgrade Check job.
5. **Commit:** To view commit jobs.
6. **Rollback:** To view rollback jobs.
7. **Uninstall:** To view uninstall jobs.

---

**Viewing the Upgrade job status Procedure**

1. On the System Manager web console, click Services > Solution Deployment Manager.
2. In the left navigation pane, click Upgrade Job Status.
3. On the Status of Upgrade Management Jobs page, in the Job Type field, click a job type.
4. Select one or more jobs.
5. Click View.

   The system displays the Upgrade Job Status page.
Editing an upgrade job

Before you begin
You can edit the configuration of an upgrade job that is in pending state.

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager.
2. In the navigation pane, click Upgrade Job Status.
3. On the Upgrade Job Status page, in the Job Type field, click Upgrade.
4. Select a pending upgrade job that you want to edit.
5. Click Edit Configuration.
   The system displays the Upgrade Configuration page.
6. To edit the configuration, see Upgrading Avaya Aura applications.

Deleting the Upgrade jobs

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager.
2. In the left navigation pane, click Upgrade Job Status.
3. On the Upgrade Job Status page, in the Job Type field, click a job type.
4. Select one or more jobs.
5. Click Delete.
   The system updates the Upgrade Job Status page.
Upgrade Job Status field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Type</td>
<td>The upgrade job type. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Refresh Element(s)</strong>: To view refresh elements jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Analyze</strong>: To view analyze jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pre-Upgrade Check</strong>: To view preupgrade check jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Upgrade</strong>: To view upgrade jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Commit</strong>: To view commit jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Rollback</strong>: To view rollback jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Uninstall</strong>: To view uninstall jobs.</td>
</tr>
<tr>
<td>Job Name</td>
<td>The upgrade job name.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time when the system started the job.</td>
</tr>
<tr>
<td>End Time</td>
<td>The time when the system ended the job.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the upgrade job. The status can be: SUCCESSFUL, PENDING_EXECUTION, PARTIAL_FAILURE, FAILED.</td>
</tr>
<tr>
<td>% Complete</td>
<td>The percentage of completion of the upgrade job.</td>
</tr>
<tr>
<td>Element Records</td>
<td>The total number of elements in the upgrade job.</td>
</tr>
<tr>
<td>Successful Records</td>
<td>The total number of times that the upgrade job ran successfully.</td>
</tr>
<tr>
<td>Failed Records</td>
<td>The total number of times that the upgrade job failed.</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the upgrade job.</td>
</tr>
<tr>
<td>Re-run Checks</td>
<td>Performs the upgrade job again.</td>
</tr>
<tr>
<td>Edit Configuration</td>
<td>Displays the Upgrade Configuration page where you can change the upgrade configuration details.</td>
</tr>
</tbody>
</table>

Rollback process

Upgrade rollback

The upgrade rollback is initiated in two cases:

• Upgrade process of an element fails: Administrator need not rollback upgrade of all the elements. When the element upgrade fails, the system stops the entire upgrade process and
displays the failure status on the Upgrade Management page. The entire upgrade process does not roll back. Only the failed element upgrade rolls back.

- Upgrade process of the entire system fails: Admin specifies rollback all when the system upgrade fails. The system stops the upgrade and rolls back the overall upgrade process.

### Rolling back an upgrade

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Click the Avaya Aura® application that you want to rollback.
   
   The system selects the parent of the application that you select and all child applications of the parent. For example, the page displays the message **Selected System Platform or child of System Platform, and System Platform and all child applications**.
4. Click **Upgrade Actions > Rollback**.

---

### Enhanced Access Security Gateway overview

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

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

### Managing EASG from CLI

**About this task**

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

**Before you begin**

Log in to the application CLI interface.

**Procedure**

1. To view the status of EASG, run the command: **EASGStatus**.
The system displays the status of EASG.

2. To enable EASG, do the following:

   a. Run the command: `EASGManage --enableEASG`.

      The system displays the following message.
      
      By enabling Avaya Services Logins you are granting Avaya access to your system. This is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.
      
      The product must be registered using the Avaya Global Registration Tool (GRT, see https://grt.avaya.com) to be eligible for Avaya remote connectivity. Please see the Avaya support site (https://support.avaya.com/register) for additional information for registering products and establishing remote access and alarming.
      
   b. When the system prompts, type `yes`.

      The system displays the message: EASG Access is enabled.

3. To disable EASG, do the following:

   a. Run the command: `EASGManage --disableEASG`.

      The system displays the following message.
      
      By disabling Avaya Services Logins you are denying Avaya access to your system. This is not recommended, as it can impact Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Services Logins should not be disabled.
      
   b. When the system prompts, type `yes`.

      The system displays the message: EASG Access is disabled.

Viewing the EASG certificate information

   Procedure

   Log in to the application CLI interface.

EASG site certificate

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

Before you begin

1. Obtain the site certificate from the Avaya support technician.

2. You must load this site certificate on each server that the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to /home/cust directory, where cust is the login ID. The directory might vary depending on the file transfer tool used.

3. Note the location of this certificate and use in place of installed_pkcs7_name in the commands.

4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

Procedure

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

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

3. To delete the site certificate, run the following command:
   - sudo EASGSiteCertManage --delete <installed_pkcs7_name>: To delete the specified site certificate.
   - sudo EASGSiteCertManage --delete all: To delete all the site certificates that are currently installed on the system.
Chapter 10: Maintenance

Maintenance

This chapter describes the procedures to change the WebLM IP address, FQDN, and other parameters from Command Line Interface (CLI). This chapter also provides information about performing backup and restore of WebLM.

Note:
The existing license files become invalid when you:

- change the WebLM IP address
- perform a WebLM update
- clone a virtual machine

When you redeploy the WebLM, then you must reinstall a new license file to match the new Host ID generated in the WebLM server.

Changing the IP, FQDN, DNS, Gateway, or Netmask addresses

Before you begin
Log in to the WebLM command line interface with administrator privilege CLI user credentials.

Important:
Ensure that WebLM maintenance is not in progress.

Procedure

1. Type `changeIPFQDN -IP <IP Address> -FQDN <FQDN> -GATEWAY <Gateway address> -NETMASK <Netmask address> -dns <dns address> -SEARCH <search list for DNS>`.

Warning:
Do not change the IP address settings from VMware tools when WebLM is in the Power Off state.
Note:
After a WebLM IP/FQDN change, the licenses become invalid. You must re-host the licenses. The license data varies based on the installed license as part of the license re-host.

2. To add more than one IP address for the DNS server, type `changeIPFQDN -dns primary_DNS_IPaddress, secondary_DNS_IPaddress, DNS_N_IPadress....` to “changeIPFQDN -dns primary_DNS_IPaddress, secondary_DNS_IPaddress, ..., DNS_N_IPadress.

You must separate each DNS IP address by a comma (,). For example, `changeIPFQDN -dns 10.14.16.2, 14.17.13.5`.

The system takes a few seconds to apply the DNS changes to the network.

Note:
The command to configure multiple DNS IP addresses overrides all the previous DNS IP address entries.

Related links
- [Rehosting license files](#) on page 72
- [WebLM CLI operations](#) on page 84

---

### Configuring multiple DNS IP addresses

**Before you begin**
- Deploy the WebLM OVA file.
- Start the WebLM virtual machine.

When you turn on WebLM for the first time after you deploy the OVA file, the system applies the network configurations that you provided during the deployment of the WebLM OVA file.

**Note:**
The command to configure multiple DNS IP addresses overrides all the previous DNS IP address entries.

**Procedure**

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

    **Important:**
    Ensure that WebLM maintenance is not in progress.

2. Check the existing DNS IP address of WebLM.

3. To add more than one IP address for the DNS server, type `changeIPFQDN -dns primary_DNS_IPaddress, secondary_DNS_IPaddress, DNS_N_IPadress....`
to "changeIPFQDN -dns primary_DNS_IPaddress,
secondary_DNS_IPaddress, ...; DNS_N_IPadress.

You must separate each DNS IP address by a comma (,). For example, changeIPFQDN -

The system takes a few seconds to apply the DNS changes to the network.

4. Log on to the WebLM web console with administrator privilege credentials.
5. Ensure that the system displays the multiple DNS IP addresses.

Related links
WebLM CLI operations on page 84

---

**Configuring the time zone**

**Procedure**

1. Log in to the WebLM command line interface with administrator privilege CLI user credentials.
2. Type `configureTimeZone`.
3. Select the time zone from the list.
   For example, America/Denver.

Related links
WebLM CLI operations on page 84

---

**Configuring the NTP server**

**Procedure**

1. Log in to the WebLM command line interface with administrator privilege CLI user credentials.
2. Type `configureNTP <IP address of the NTP server>`.
   The system configures the NTP server.

Related links
WebLM CLI operations on page 84

---

**Resetting the WebLM password through CLI**

**Procedure**

1. Log in to the WebLM command line interface with administrator privilege CLI user credentials.
2. Type the `weblm_password <reset|restore>` command.

Using password reset you can back up the existing user configuration and apply the predefined password. By resetting the password, you can restore the backed up configuration.

---

### Performing WebLM backup

**Procedure**

1. Log in to the WebLM command line interface with administrator privilege CLI user credentials.
2. Type `WebLMBackup <backup_location>` and provide the backup location as a parameter.

In this case, the WebLM backup is stored at the location you specify as a parameter.

Copy the backup files to a remote computer or to an external storage device.

---

### Performing WebLM restore

**Procedure**

1. Log in to the WebLM command line interface with administrator privilege CLI user credentials.
2. Depending on your restore requirement, perform one of the following:
   - Type `WebLMRestore full <backup_location>` to restore all the WebLM files by picking up the backup file at the specified location.
   - Type `WebLMRestore selective <backup_location>` to restore a set of files necessary for the functionality of the WebLM server from the specified backup location.

---

### Creating a snapshot backup

**About this task**

⚠️ **Important:**

Do not perform any activity on WebLM until the snapshot backup is complete.

To create the snapshot backup, use the vCenter client or the vSphere client.

**Procedure**

1. From the list of virtual machines, right-click the required WebLM virtual machine, and select **Snapshot**.
2. Click **Take Snapshot**.
3. In the Name and Description fields, enter a name and the description for the snapshot.

4. Set the following Snapshot options:
   a. Enable Snapshot the virtual machine’s memory.
   b. Enable Quiesce guest file system (Needs VMware Tools installed).

   **Note:**
   Quiescing indicates pausing or altering the state of running processes, particularly the processes that might modify the information stored on disk during a backup. Quiescing ensures a consistent and usable backup.

5. Click OK.

6. In the Recent Tasks window, ensure that the status of the Create virtual machine snapshot task is Completed.

**Creating a snapshot restore**

**About this task**

**⚠ Important:**
Do not perform any activity on WebLM until the snapshot restore is complete.

Performing the VMware snapshot restore is not the same as application specific restore.

To restore the snapshot backup, use the vCenter client or the vSphere client.

**Procedure**

1. From the list of virtual machines, select the deployed WebLM virtual machine, and right-click and select Snapshot.
2. Open Snapshot Manager.
3. Select the snapshot version that you want to restore.
4. Click Go to.
5. In the Recent Tasks window, verify whether the Status of the Revert snapshot task is Completed.
## WebLM CLI operations

<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>changeIPFQDN</td>
<td>• IP &lt; new IP address for WebLM &gt; &lt;br&gt;• FQDN &lt; new fully qualified domain name of WebLM &gt; &lt;br&gt;• GATEWAY &lt; new gateway address for WebLM &gt; &lt;br&gt;• NETMASK &lt; new netmask address for WebLM &gt; &lt;br&gt;• dns &lt; new DNS address for WebLM &gt; &lt;br&gt;• SEARCH &lt; new search list for DNS addresses &gt;</td>
<td>Updates the IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value.</td>
<td>• changeIPFQDN -IP &lt; new IP address &gt; &lt;br&gt;• changeIPFQDN -FQDN &lt; new fully qualified domain name &gt; &lt;br&gt;• changeIPFQDN -GATEWAY &lt; new gateway address for WebLM &gt; -SEARCH &lt; new search list for DNS addresses &gt;</td>
</tr>
<tr>
<td>2.</td>
<td>configureNTP</td>
<td>&lt; IP address of the NTP server &gt;</td>
<td>Configures the NTP server details.</td>
<td>configureNTP &lt; IP address of the NTP server &gt; &lt;br&gt;Separate the IP addresses or the host names of the NTP servers with commas (,).</td>
</tr>
<tr>
<td>3.</td>
<td>configureTimezone</td>
<td>&lt; Time zone that you want to select &gt;</td>
<td>Configures the time zone with the value that you select.</td>
<td>configureTimezone &lt; Time zone that you want to select &gt; &lt;br&gt;Select a time zone. For example, America/Denver</td>
</tr>
<tr>
<td>4.</td>
<td>WebLMPatchdeploy</td>
<td>&lt; absolute path to the WebLM service pack, feature pack, or the software patch &gt;</td>
<td>Installs the software patch, the service pack, or the feature pack for WebLM.</td>
<td>WebLMPatchdeploy &lt;absolute path to home/admin/&lt; WebLM FeaturepackName &gt; &lt;br&gt;Note: &lt;br&gt;Copy the WebLM feature pack or patches that you install to /home/admin/.</td>
</tr>
</tbody>
</table>

Table continues...
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>weblm_password</td>
<td>&lt;reset&gt;</td>
<td>Reset option backs up the existing user configuration and applies the predefined password.</td>
<td>weblm_password reset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;restore&gt;</td>
<td>Restore option restores the backed-up user configuration. The utility also supports the non-root user, such as admin.</td>
<td>weblm_password restore</td>
</tr>
<tr>
<td>6.</td>
<td>configureTLS</td>
<td>&lt;TLSv1.2&gt;</td>
<td>Configures the TLS support.</td>
<td>Type one of the following option:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;TLSv1.1&gt;</td>
<td></td>
<td>• enable TLSv1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;TLSv1&gt;</td>
<td></td>
<td>• enable TLSv1.2 and TLSv1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• enable TLSv1.2, TLSv1.1 and TLSv1.0</td>
</tr>
</tbody>
</table>

**Viewing the job history of virtual machine operations**

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.

2. On the desktop, click the SDM icon (SDM), and then click **Application Management**.

3. In the lower pane, click **Job History**.

4. On the Job History page, in **Operation**, select one or more operations.

5. Click **Submit**.

   The page displays the details of jobs that you selected.
Job History field descriptions

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

History

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

Monitoring a host and virtual machine

Monitoring a platform

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. Click **Monitor Platforms**.
3. On the Monitor Hosts page, do the following:
   a. In **Hosts**, click a host.
   b. Click **Generate Graph**.

The system displays the graph regarding the CPU/memory usage of the host that you selected.
Monitoring an application

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. Click **Monitor Applications**.
3. In the Monitor VMs page, do the following:
   a. In **Hosts**, click a host.
   b. In **Virtual machines**, click a virtual machine on the host that you selected.
4. Click **Generate Graph**.
   The system displays the graph regarding the CPU/memory usage of the virtual machine that you selected.
Chapter 11: Resources

Avaya WebLM documentation

The following table lists the documents related to Avaya WebLM. Download the documents from the Avaya Support website at http://support.avaya.com.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploying standalone Avaya WebLM in Virtual Appliance</td>
<td>Deploy the application in virtual appliance environment by using Solution Deployment Manager</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying standalone Avaya WebLM in Virtualized Environment</td>
<td>Deploy the application in virtualized environment.</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying standalone Avaya WebLM in Infrastructure as a Service Environment</td>
<td>Deploy the application on cloud services.</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying standalone Avaya WebLM in Software-Only Environment</td>
<td>Deploy the application in software-only environment.</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Upgrading standalone Avaya WebLM</td>
<td>Upgrade the application.</td>
<td>Implementation personnel</td>
</tr>
</tbody>
</table>

Administering

| Administering standalone Avaya WebLM             | Perform administration tasks                                               | System administrators       |

Finding documents on the Avaya Support website

Procedure

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**.

---

**Accessing the port matrix document**

**Procedure**

1. Go to [https://support.avaya.com](https://support.avaya.com).
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product > Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.

7. Click **Enter**.

---

**Avaya Documentation Portal navigation**

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

⚠️ **Important:**

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

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
• Publish a PDF of the current section in a document, the section and its subsections, or the entire document.

• Add content to your collection by using My Docs (🌟).
  Navigate to the My Content > My Docs menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.

• Add yourself as a watcher by using the Watch icon (💬).
  Navigate to the My Content > Watch list menu, and do the following:
  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.
  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

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

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

---

Training

The following courses are available at http://www.avaya-learning.com/. To search for the course, enter the course code in the Search field and click Go.

<table>
<thead>
<tr>
<th>Course code</th>
<th>Course title</th>
</tr>
</thead>
<tbody>
<tr>
<td>71200V</td>
<td>Integrating Avaya Aura® Core Components</td>
</tr>
</tbody>
</table>

---

Amazon Web Services documentation

For information about the Amazon Web Services documentation, go to the AWS documentation website at https://aws.amazon.com/documentation/.
Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In Search, type Avaya Mentor Videos, click Clear All and select Video in the Content Type.
  - In Search, type the product name. On the Search Results page, click Clear All and select Video in the Content Type.

  The Video content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

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

⚠️ Note:

Videos are not available for all products.

Support

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

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
Resources

- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

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

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

2. Log on to the Avaya website with a valid Avaya user ID and password. The system displays the Avaya Support page.
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.
Glossary

Fully automated upgrade using Solution Deployment Manager

The fully automated upgrade process includes upgrading a product from earlier release to the latest release by using either Solution Deployment Manager Client or System Manager Solution Deployment Manager. In fully automated upgrade all subsequent steps are executed as a single process, including tasks such as backup, deploy, and post upgrade tasks such as applying patches or service packs.

For fully automated upgrade using Solution Deployment Manager, the system does not allow to change the IP Address of the application. Alternatively, you can use the Migration using CLI method.

For upgrading System Manager, use Solution Deployment Manager Client. For upgrading applications other than System Manager, use System Manager Solution Deployment Manager.

Migration

The migration process includes changing the hypervisor or hardware while upgrading the application.

- **Migration using SDM:** Migration using Solution Deployment Manager is supported using same IP Address.
  
  For example, from:
  
  - System Platform to AVP/VMware
  - AVP to VMware
  - VMware to AVP

  For upgrading System Manager, use Solution Deployment Manager Client. For upgrading applications other than System Manager, use System Manager Solution Deployment Manager.

  If you want to migrate using different IP Address for the application, use the CLI method.

Update

The update process includes installing patches of an application. For example, kernel patches, security patches, hotfixes, service packs, and feature packs.

Upgrade using CLI

The upgrade process includes upgrading a product from earlier release to the latest release without the need to change the server hardware or hypervisor.
Index

A
aborting
  virtual machine report generation ........................................... 40
accessing port matrix ..................................................................... 89
actual license usage ........................................................................ 22
adding
  Appliance Virtualization Platform host ........................................ 27
  AVP host .................................................................................. 27
  ESXi host .................................................................................. 27
  location .................................................................................... 25
  vCenter to SDM .......................................................................... 41
adding ESXi host ........................................................................... 27
adding location .............................................................................. 25
adding location to host ................................................................... 43
adding vCenter to SDM ................................................................... 41
Add Platform .................................................................................. 33
analyze inventory
  SDM ............................................................................................ 47
analyze job status ........................................................................... 73
Appliance Virtualization Platform
  license file .................................................................................. 29
  restarting ..................................................................................... 33
  shutting down ............................................................................. 32
  WebLM Configuration .................................................................... 29
Appliance Virtualization Platform license
  supported servers .......................................................................... 30
Appliance Virtualization Platform licenses for servers ...................... 30
Application deployment failure ...................................................... 74
application
  edit ............................................................................................. 35
  monitoring ................................................................................ 87
  re-establishing trust ..................................................................... 37
  restart .......................................................................................... 36
  start ............................................................................................. 36
  stop .............................................................................................. 36
Application management .................................................................. 24
applications
  preupgrade check ................................................................-------- 49
Avaya Aura® application
  ESXi version .............................................................................. 16
  supported servers ....................................................................... 14
Avaya support website ..................................................................... 91
AVP license status .......................................................................... 32

B
backup through CLI ........................................................................... 82
browser requirements ........................................................................ 21

C
Change IP FQDN ............................................................................... 35
changing DNS .................................................................................. 79

D
deleting
  location ....................................................................................... 26
  upgrade jobs ................................................................................. 74
deleting a location .......................................................................... 26
deleting vCenter .............................................................................. 43
deploy application ............................................................................ 24
documentation
  WebLM ........................................................................................ 88
documentation portal ....................................................................... 89
  finding content ............................................................................ 89
  navigation .................................................................................... 89
downloading software
  using PLDS ................................................................................. 19
download software .......................................................................... 34, 47

E
EASG
  certificate information .................................................................. 77
  disabling ...................................................................................... 76
  enabling ...................................................................................... 76
  status .......................................................................................... 76
  EASG site certificate ..................................................................... 77
edit application .......................................................... 35
edit application .......................................................... 35
edit location ................................................................. 26
edit vCenter ................................................................. 43
editing the location ...................................................... 26
editing upgrade configuration ...................................... 74
editing vCenter ............................................................ 43
Edit Location ............................................................... 26
Edit Platform ............................................................... 33
Edit Upgrade Configuration
  AVP Configuration .................................................... 56
  Element Configuration ................................................. 56
Edit vCenter ................................................................. 44
  elements refresh .......................................................... 46
Enhanced Access Security Gateway
  EASG overview .......................................................... 76
ESXi host
  adding ........................................................................... 27
  removing ....................................................................... 33
  restarting ...................................................................... 33
ESXi version
  Avaya Aura® application ............................................. 16

F
field descriptions
  Add Platform ............................................................... 33
  Edit Location ............................................................. 26
  Edit Platform ............................................................. 33
  Job History ................................................................. 86
  Map vCenter .............................................................. 44
  New Location .............................................................. 26
  Preupgrade configuration .......................................... 50
  View License Capacity ............................................... 22
  View Peak Usage ........................................................ 23
  WebLM Configuration .................................................. 32
file download manager .................................................. 48
finding content on documentation portal ....................... 89
finding port matrix ....................................................... 89

G
General Configuration Details .......................................... 56
generate_report.sh ......................................................... 39
generating virtual machine report .................................. 39

H
hardware supported
  System Manager .......................................................... 14

I
InSite Knowledge Base ................................................... 91
installing a patch ......................................................... 63
installing a service pack ............................................... 63
installing WebLM feature pack ....................................... 63
inventory
  refresh elements .......................................................... 46

J
Job History ..................................................................... 85, 86

L
latest software patches .................................................. 16
license files
  rehost ......................................................................... 72
Life cycle management .................................................... 24
location
  adding ......................................................................... 25
  deleting ........................................................................ 26
  editing ........................................................................ 26
  view ........................................................................... 25
logging on
  WebLM web console .................................................... 71

M
Map vCenter ................................................................... 41, 43, 44
migration path
  IaaS ............................................................................ 66
  software-only environment .......................................... 67
monitoring
  application ................................................................... 87
  platform ....................................................................... 86
  multiple DNS IP addresses ......................................... 79, 80
My Docs ......................................................................... 89

N
New Location ................................................................. 26
New vCenter .................................................................. 44
NTP server
  configure ..................................................................... 81

P
patch information ........................................................... 16
PCN .............................................................................. 16
peak usage; view .......................................................... 23
peak usage for a licensed product .................................... 23
performing WebLM backup ............................................ 82
performing WebLM restore ............................................. 82
platform
  monitoring ................................................................... 86