



# **Implementing Avaya Aura<sup>®</sup> Application Enablement Services on Avaya Aura<sup>®</sup> System Platform**

## Notices

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

## Link disclaimer

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

## Warranty

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

## Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) 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. 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 Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed, or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "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 on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

**Database License (DL).** End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.

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

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

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

## Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express

written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

### **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 Documentation or on Avaya's website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

### **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: <http://support.avaya.com> or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: [securityalerts@avaya.com](mailto:securityalerts@avaya.com).

### **Trademarks**

Avaya Aura is a registered trademark of Avaya.

All non-Avaya trademarks are the property of their respective owners.

PuTTY is copyright 1997-2009 Simon Tatham.

### **Downloading Documentation**

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

### **Contact Avaya Support**

See the Avaya Support website: <http://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: <http://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

# Contents

<b>Chapter 1: Introduction</b> .....	11
Purpose.....	11
Intended audience.....	11
Document changes since last issue.....	11
Resources.....	11
Documentation.....	11
Training.....	13
Viewing Avaya Mentor videos.....	14
Support.....	14
Warranty.....	15
<b>Chapter 2: Installation overview</b> .....	16
About the Application Enablement Services on System Platform offer.....	16
Application Enablement Services on System Platform High Availability Failover.....	16
Network interfaces for the server.....	19
Application Enablement Services Ethernet interfaces.....	20
Single NIC configuration.....	21
Dual NIC configuration.....	21
Network interface (NIC) settings.....	22
Network latency requirements.....	23
Client workstation provisioning.....	23
Communication Manager and media server requirements.....	24
Downloading the AE Services release notes.....	24
Installation process overview.....	25
<b>Chapter 3: Installation prerequisites</b> .....	27
Application Enablement Services on System Platform installation overview.....	27
What Avaya provides.....	28
What customer provides.....	29
Installation worksheet for AES on System Platform.....	29
<b>Chapter 4: Preinstallation tasks for System Platform</b> .....	33
Preinstallation checklist for System Platform.....	33
Registering the system.....	34
Registering for PLDS.....	35
Downloading software from PLDS.....	36
Verifying the downloaded ISO image.....	36
Verifying the ISO image on a Linux-based computer.....	36
Verifying the ISO image on a Windows-based computer.....	37
Writing the downloaded software to DVD.....	37
DVD requirements.....	37
Writing the ISO image to DVD or CD.....	38

<b>Chapter 5: Installing the Dell PowerEdge R620 Server</b> .....	39
Dell R620 Server overview.....	39
Downloading Dell documentation.....	40
Dell R620 documentation set.....	41
Front view of Dell R620 Server.....	41
Back view of Dell R620 Server.....	43
Dell R620 Server specifications.....	44
Dell R620 altitude and air pressure requirements.....	45
Dell R620 temperature and humidity requirements.....	46
Dell R620 Server power specifications.....	46
Installing the server in the rack.....	47
Installing a 10 Gb network-interface card.....	48
<b>Chapter 6: Installing the HP DL360 G7 server</b> .....	49
HP DL360 document set.....	49
Downloading HP documentation.....	49
Specifications for HP DL360 G7 server with P410i RAID controller.....	50
HP DL360 G7 Server physical specifications.....	50
HP DL360 G7 Server power specifications.....	50
HP DL360 G7 Server environmental specifications.....	51
Front view of HP DL360 G7 Server.....	51
Back view of HP DL360 G7 Server.....	52
Installing the server in the rack.....	53
Installing a 10 Gb network-interface card.....	55
<b>Chapter 7: Installing the Dell R610 server</b> .....	58
Specifications for Dell R610 server with H700 RAID controller.....	58
Installing a 10 Gb network-interface card.....	59
<b>Chapter 8: Installing System Platform</b> .....	64
Installation methods.....	64
Server requirements.....	64
Installation checklist for System Platform.....	65
Connecting your laptop to the server.....	68
Configuring the laptop for direct connection to the server.....	68
Disabling proxy servers in Microsoft Internet Explorer.....	69
Disabling proxy servers in Mozilla Firefox.....	70
Starting the installation.....	70
Starting the installation from your laptop.....	70
Starting the installation from the server console.....	71
Selecting the type of keyboard.....	72
Verifying the System Platform server hardware.....	73
Verifying the System Platform image on the DVD.....	74
Configuring network settings for System Domain.....	74
System Domain Network Configuration field descriptions.....	76
Configuring network settings for Console Domain.....	77

System Platform Console Domain Network Configuration field descriptions.....	78
Installing the Services virtual machine.....	79
Services VM Network Configuration field descriptions.....	81
Configuring the time zone for the System Platform server.....	81
Configuring the date and time for the System Platform server.....	82
Configuring System Platform passwords.....	82
Passwords field descriptions.....	85
Verifying installation of System Platform.....	85
Accessing System Platform.....	87
Connecting to the server through the services port.....	87
Enabling IP forwarding to access System Platform through the services port.....	88
Browser support for System Platform Web Console.....	88
Accessing the System Platform Web Console.....	88
Accessing the command line for System Domain.....	89
Accessing the command line for Console Domain.....	90
<b>Chapter 9: Installing Feature Pack software on System Platform.....</b>	<b>92</b>
Feature packs.....	92
Feature Pack installation.....	93
Managing patches.....	93
Patch management.....	93
Patch commit and rollback.....	93
Downloading patches.....	95
Configuring a proxy.....	96
Installing patches.....	96
Installing System Platform patches on High Availability systems.....	97
Committing patches.....	98
Rolling back patches.....	99
Removing patches.....	99
Search Local and Remote Patch field descriptions.....	100
Patch List field descriptions.....	102
Patch Detail field descriptions.....	102
<b>Chapter 10: Configuring System Platform High Availability.....</b>	<b>105</b>
About System Platform High Availability.....	105
Template administration during High Availability operation.....	105
Prerequisites for High Availability configuration.....	106
Introduction to High Availability prerequisites.....	106
Common prerequisites for all High Availability modes.....	106
Prerequisites for locally redundant High Availability.....	107
Configuring System Platform High Availability.....	108
Configuring locally redundant High Availability.....	108
High Availability field descriptions.....	110
Configure HA field descriptions.....	110
High Availability start/stop.....	113

Starting System Platform High Availability.....	113
Stopping System Platform High Availability.....	114
Manually switching High Availability server roles.....	115
Removing the High Availability configuration.....	115
<b>Chapter 11: Installing Application Enablement Services.....</b>	<b>117</b>
Prerequisites for installing the AES template.....	117
Configuring a proxy.....	117
Installing Application Enablement Services template.....	118
Search Local and Remote Template field descriptions.....	119
Reinstalling or replacing the Avaya Access Security Gateway default authentication file.....	121
<b>Chapter 12: Configuring SAL Gateway on System Platform.....</b>	<b>123</b>
SAL Gateway.....	123
Configuration prerequisites.....	124
Changing the Product ID for System Platform.....	125
System and browser requirements.....	125
Starting the SAL Gateway user interface.....	126
Configuring the SAL Gateway.....	126
Gateway Configuration field descriptions.....	127
Configuring a proxy server.....	129
Proxy Server field descriptions.....	129
Configuring SAL Gateway communication with a Concentrator Core Server.....	131
Core Server field descriptions.....	131
Configuring SAL Gateway communication with a Concentrator Remote Server.....	132
Remote Server field descriptions.....	133
Configuring NMS.....	133
Network Management Systems field descriptions.....	134
Managing service control and status.....	134
Applying configuration changes.....	135
Managed element worksheet for SAL Gateway.....	136
Adding a managed element.....	136
Managed Element field descriptions.....	137
Using a stand-alone SAL Gateway.....	139
Adding an SNMP trap receiver.....	139
Disabling SAL Gateway.....	139
<b>Chapter 13: Upgrading System Platform.....</b>	<b>141</b>
Introduction.....	141
Determining whether the WebLM license will be removed during an upgrade.....	141
Upgrades to System Platform 6.3.4.....	143
Service continuity.....	143
System Platform upgrades on High Availability systems.....	144
SAL deployment on the Services Virtual Machine.....	144
Checklists for upgrading System Platform.....	145
System Platform upgrade paths, service packs, and patches.....	148

About System Platform upgrade files.....	148
Upgrade paths to System Platform 6.3.4.....	150
System Platform release history and upgrade information.....	151
System Platform releases.....	155
Solution template patches.....	155
Preupgrade tasks.....	155
Preupgrade checklist.....	155
Preupgrade checklist for System Platform on High Availability systems.....	157
Stopping System Platform High Availability.....	158
System Platform backup.....	159
Cdom and SAL Gateway address assignments.....	160
Upgrading System Platform.....	165
Feature packs.....	165
Feature Pack installation.....	166
Platform upgrade process in different System Platform deployments.....	166
Upgrading a System Platform server.....	167
Verifying an upgrade.....	170
Commit and Rollback.....	172
Committing an upgrade.....	173
Rolling back an upgrade.....	173
Platform Upgrade field descriptions.....	173
Upgrading System Platform on High Availability Systems.....	175
High Availability during platform upgrades.....	175
Installing System Platform patches on High Availability systems.....	176
Removing the High Availability configuration.....	176
Upgrading System Platform on both servers.....	177
Starting System Platform High Availability.....	178
Postupgrade tasks.....	179
SNMP configuration overview.....	179
Configuring SNMP version support on the Services VM.....	180
Licensing change in System Platform 6.3.4.....	181
Password hashing.....	182
Upgrading the Services virtual machine.....	182
Upgrade of the Services virtual machine.....	182
Upgrading Services-VM on System Platform.....	182
Verifying the Services-VM installation and upgrade.....	186
Enabling SAL Gateway.....	187
Committing the template upgrade.....	188
Enabling Services-VM.....	188
Upgrading the standby and active servers when Geographical Redundancy High Availability feature is enabled.....	189
<b>Chapter 14: Upgrading Application Enablement Services.....</b>	<b>190</b>
Upgrading Application Enablement Services template.....	190



Using RPM Only installer for installing the Application Enablement Services 6.3.3 feature pack from the System Platform Web Console.....	192
Using RPM Only installer for uninstalling the AE Services 6.3.3 feature pack from the System Platform Web Console .....	193
Using RPM Only installer for installing AE Services 6.3.3 feature pack from the AE Services shell console.....	193
Using RPM Only installer for uninstalling AE Services 6.3.3 feature pack from the AE Services shell console.....	194
<b>Chapter 15: Troubleshooting the installation.....</b>	<b>196</b>
Template DVD does not mount.....	196
Cannot ping Console Domain or get to the Web Console.....	196
Troubleshooting steps.....	196
SAL does not work.....	197
Multiple reinstallations can result in an out of memory error.....	199
<b>Appendix A: Preinstallation checklist for System Platform.....</b>	<b>200</b>
<b>Appendix B: Installation worksheet for System Platform.....</b>	<b>202</b>
<b>Appendix C: Managed element worksheet for SAL Gateway.....</b>	<b>213</b>
<b>Appendix D: Managing license entitlements from PLDS.....</b>	<b>214</b>
Activating license entitlements.....	214
Searching for license entitlements.....	215
Moving activated license entitlements.....	217
Regenerating a license file.....	218
<b>Appendix E: Enterprise-wide licensing.....</b>	<b>220</b>
Overview of enterprise-wide licensing.....	220
Comparison of standard licensing and enterprise-wide licensing.....	220
Licensing configuration examples.....	221
Standard licensing.....	221
Enterprise-wide licensing — allocating licenses or features.....	222
Enterprise-wide licensing — pointing to a master license on a remote server.....	223
Setting up a configuration for allocating licenses.....	224
Installing the license file and configuring the master WebLM server.....	224
Adding a local WebLM server.....	226
Setting up the Local WebLM Server in your configuration.....	227
Changing the allocations of a license file.....	228
Verifying the license allocations on the Local WebLM Server.....	229
<b>Appendix F: Installing and connecting the S8800 server.....</b>	<b>230</b>
Overview of the Avaya S8800 Server.....	230
Avaya S8800 Server overview.....	230
Front of server.....	230
Back of server.....	232
Avaya S8800 1U Server specifications.....	233
Server components.....	234
S8800 Server environmental requirements.....	235

## Contents

Safety instructions.....	235
Avaya-provided equipment.....	236
Customer-provided equipment.....	237
Clearance requirements.....	237
Server installation checklist.....	238
Installing the Avaya S8800 Server.....	238
Rack installation components.....	238
Attaching the rails to the rack.....	239
Installing the server in the rack.....	242
Installing the cable management arm.....	243
Turning on the server.....	248
Connecting the server to the network.....	249

# Chapter 1: Introduction

---

## Purpose

This document describes implementing of the tested product, characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.

---

## Intended audience

This document is intended for people who want to gain a high-level understanding of the product features, functions, capacities, and limitations.

---

## Document changes since last issue

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

- Updated the IP settings for local WebLM server configuration to [Adding a local WebLM server](#) on page 226
  - Added steps for uninstalling the AE Services 6.3.3 feature pack from the System Platform Web Console, using RPM Only installer to [Using RPM Only installer for uninstalling the Application Enablement Services 6.3.3 feature pack from the System Platform Web Console](#) on page 193
  - Updated the guide to remove all references to VMware offer.
- 

## Resources

---

### Documentation

The following table lists the related documents for Avaya Aura<sup>®</sup> Application Enablement Services. Most of the documents listed are Release 6.3.3. Those listed that are for earlier releases have not required an update and remain compatible with AE Services 6.3.3. Obtain the related documents

and documents about other Avaya products mentioned in this guide from the Avaya Support website: [Avaya support site](#).

	<b>Document title</b>	<b>Number</b>	<b>Release</b>
1	<i>Avaya Application Enablement Services Overview and Specification</i>	02-300360	6.3.3
2	<i>Implementing Avaya Application Enablement Services on Avaya Aura® System Platform</i>	02-603468	6.3.3
3	<i>Implementing Avaya Application Enablement Services in a Software-Only Environment</i>	02-300355	6.3.3
4	<i>Implementing Avaya Application Enablement Services for a Bundled Server Upgrade</i>	02-300356	6.3.3
5	<i>Avaya Application Enablement Services using VMware® in the Avaya Aura® Virtualized Environment Deployment Guide</i>	Not applicable	6.3.3
6	<i>Avaya Application Enablement Services Administration and Maintenance Guide</i>	02-300357	6.3.3
7	<i>Avaya Application Enablement Services Implementation Guide for Microsoft® Live Communications Server 2005, Microsoft Office Communications Server 2007, and Microsoft Lync® Server 2010 and 2013</i>	02-601893	6.3.3
8	<i>Avaya Application Enablement Services Integration Guide for IBM Lotus Sametime</i>	02-602818	6.3
9	<i>Avaya Application Enablement Services Online Help (packaged with Application Enablement Services software and not available on the Web)</i>	Not applicable	6.3.3
10	<i>Avaya Application Enablement Services TSAPI Exerciser Help (Online, packaged with the AE Services TSAPI Client SDK software and not available on the Web)</i>	Not applicable	6.3.3
11	<i>Avaya Application Enablement Services Web Services Programmer's Guide</i>	02-300362	5.2
12	<i>Avaya Application Enablement Services Device, Media and Call Control API .NET Programmer's Guide</i>	02-602658	6.3.3
13	<i>Avaya Application Enablement Services Device, Media, and Call Control .NET Programmer's Reference (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)</i>	Not applicable	6.3.3
14	<i>Avaya Application Enablement Services Device, Media, and Call Control XML Programmer's Guide</i>	02-300358	6.3.3
15	<i>Avaya Application Enablement Services Device, Media, and Call Control XML Programmer 's Reference (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)</i>	Not applicable	6.3.3
16	<i>Avaya Application Enablement Services Device, Media, and Call Control Java Programmer 's Guide</i>	02-300359	6.3.3

Table continues...

	<b>Document title</b>	<b>Number</b>	<b>Release</b>
17	<i>Avaya Application Enablement Services Device, Media, and Call Control Java Programmer's Reference</i> (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)	Not applicable	6.3.3
18	<i>Avaya Application Enablement Services Device, Media, and Call Control Media Stack API Reference</i> (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)	Not applicable	6.3.3
19	<i>Avaya Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide</i>	02-300543	6.3.3
20	<i>Avaya Application Enablement Services TSAPI for Avaya Communication Manager Programmer's Reference</i>	02-300544	6.3.3
21	<i>Avaya Application Enablement Services TSAPI Programmer's Reference</i>	02-300545	4.1
22	<i>Avaya Application Enablement Services CVLAN Programmer's Reference</i>	02-300546	4.1
23	<i>Avaya Application Enablement Services JTAPI Programmer's Guide</i>	02-603488	5.2
24	<i>Avaya Application Enablement Services JTAPI Programmer's Reference</i> (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)	Not applicable	5.2
25	<i>Avaya Application Enablement Services ASAI Technical Reference</i>	03-300549	4.1
26	<i>Avaya Application Enablement Services ASAI Protocol Reference</i>	03-300550	3.1

---

## Training

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

<b>Course code</b>	<b>Course title</b>
ATI02595AEN	Application Enablement Services Implementation and Administration (Assessment)
AVA00962WEN	Application Enablement Services 4.0 Overview
1U00223O	Avaya Aura Application Enablement Services (AES) 6.2 - L2
1U00222O	Avaya Aura Application Enablement Services (AES) 6.2 - L1
3U00127O	Designing Avaya Aura Application Enablement Services (AES) - Technical Sales L1
10U00030E	Knowledge Access: AIPS - Avaya Aura Application Enablement Services Implementation

*Table continues...*

Course code	Course title
4100	Avaya Aura(R) Application Enablement Services Implementation Test
9Z04481V	Application Enablement Services

---

## Viewing Avaya Mentor videos

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

### About this task

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

### Procedure

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

 **Note:**

Videos are not available for all products.

---

## Support

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

---

## Warranty

Avaya provides a 90-day limited warranty on Application Enablement Services. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Application Enablement Services in the warranty period is available on the Avaya Support website at <https://support.avaya.com/> under **Help & Policies > Policies & Legal > Warranty & Product Lifecycle**. See also **Help & Policies > Policies & Legal > License Terms**.

# Chapter 2: Installation overview

---

## About the Application Enablement Services on System Platform offer

Avaya Aura® Application Enablement Services (AE Services) on Avaya Aura® System Platform (System Platform) was first offered in Release 5.2. The Application Enablement Services on Avaya Aura® System Platform 6.3.4 offer includes a hardware platform (Dell™ PowerEdge™ R620, HP DL360 G7, or Dell™ PowerEdge™ R610), the Red Hat Linux operating system, the Avaya Aura® System Platform 6.3.4 software, and the Application Enablement Services 6.3.3 software.

**\* Note:**

System Platform 6.3.4 is an RPM-based feature pack and installed on System Platform 6.3, which is an ISO image.

Application Enablement Services on System Platform provides the High Availability Failover feature for customers who want to take advantage of the high availability failover capability. (See [Application Enablement Services on System Platform High Availability Failover](#) on page 16).

This book covers:

- installation of the 6.3 ISO release of System Platform software and the 6.3.4 feature pack of System Platform software
- installation of the Application Enablement Services 6.3.3 software
- upgrade of an existing version of System Platform software to release 6.3.4
- upgrade of an existing version of Application Enablement Services to release 6.3.3

---

## Application Enablement Services on System Platform High Availability Failover

With the High Availability Failover feature, you can install two identical servers that can be addressed and administered as a single entity. If one server fails, the second server quickly and automatically becomes available to client applications. To use the Application Enablement Services on System Platform High Availability feature, you must have purchased the high availability option when ordering Application Enablement Services 6.3.



System Platform 6.3 supports multiple modes of High Availability operation, facilitating efficient failover from a primary node to a secondary node with little or no interruption in system services. For Application Enablement Services 6.3, System Platform supports the following modes:

- Fast Reboot High Availability (FRHA)
- Machine Preserving High Availability (MPHA)

**!** **Important:**

Application Enablement Services 6.3 does not support Live Migration High Availability (LMHA) mode.

**\*** **Note:**

Avaya Aura System Platform High Availability does not support:

- IPv6 networking and cannot be configured with IPv6 address.
- Customer provided servers.

### **Fast Reboot High Availability (FRHA)**

System Platform FRHA mode was available in Application Enablement Services 6.1. This High Availability configuration consists of a dual server platform, which includes an active server and a standby server. Only the active server provides service. The standby server monitors the active server and then quickly takes over when a failure in the active server occurs. The interchange will appear to applications as a brief loss of the network connection. When an interchange occurs, the TSAPI, CVLAN, JTAPI, and DLG services lose all existing associations and data in transit. The DMCC service preserves its associations when an interchange occurs. With FRHA mode, a virtual machine reboot occurs after the failover.

The FRHA mode requires a pair of the following servers connected by an Ethernet crossover cable:

- S8800
- Dell R620 with H710 RAID controller
- HP DL360 G7 with P410i RAID controller
- Dell R610 with H200 RAID controller
- Dell R610 with H700 RAID controller

There will be a single license file for the server pair.

### **Machine Preserving High Availability (MPHA)**

System Platform MPHA mode is a new mode that implements a new Virtual Server Synchronization Technology (VSST) offering on System Platform. As with FRHA mode, the MPHA High Availability configuration consists of a dual server platform, which includes an active server and a standby server. Only the active server provides service. With MPHA mode, the standby server monitors the active server and then quickly takes over when one of the following conditions occur in the active server:

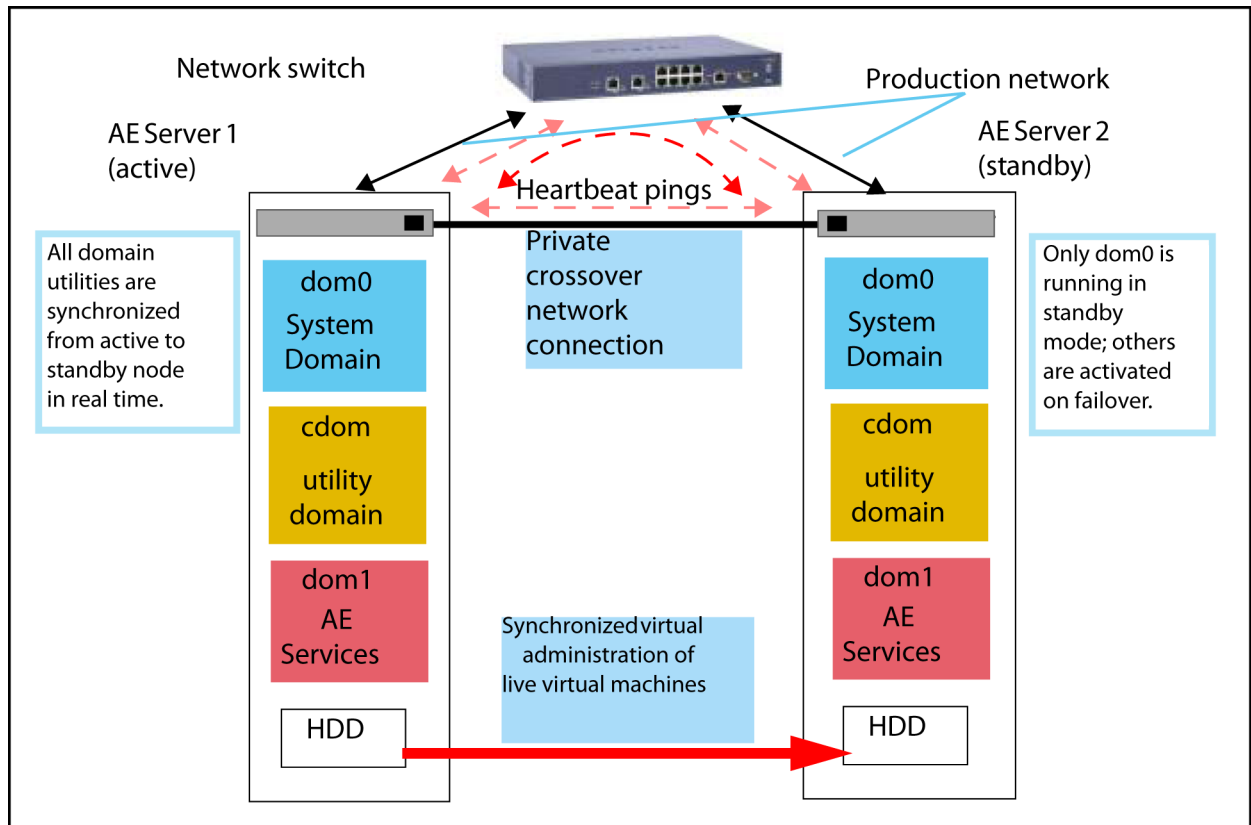
- faulty hardware is detected
- a network failure is detected
- the administrator issues a reboot/shutdown of the active server (by mistake)

Unlike in FRHA mode, failovers from the active server to the standby server in MPHA mode are not service affecting. (No reboot is required following the failover.) The failover from the active server to the standby server is transparent.

MPHA mode requires one of the following configurations:

- a pair of Dell R620 servers with H710 RAID controllers and connected back-to-back by a Category 6 cable on a 10 Gigabit NIC port. There will be a single license file for the Dell R620 pair.
- a pair of HP DL360 G7 servers with P410i RAID controllers and connected back-to-back by a Category 6 cable on a 10 Gigabit NIC port. There will be a single license file for the HP DL360 G7 pair.
- a pair of Dell R610 servers with H700 RAID controllers and connected back-to-back by a Category 6 cable on a 10 Gigabit NIC port. There will be a single license file for the Dell R610 pair.

The following diagram shows an MPHA configuration. For more information about MPHA configurations, see the whitepaper *Avaya Aura® Application Enablement Services R6.2 Machine Preserving High Availability (MPHA)* on the Avaya Support website.



**! Important:**

Starting with Application Enablement Services 6.3.3, if you want to use the GRHA feature, the use of MPHA mode is optional.

---

## Network interfaces for the server

The network interfaces, sometimes referred to as NICs (network interface cards), used by System Platform and AE Services use standard IEEE 802.3 Ethernet connections.

AE Services runs on System Platform as a guest domain. As a guest domain, AE Services is responsible for configuring its virtual Ethernet interfaces. That is, when you install the Application Enablement Services software, you will need to provide the network configuration for the virtual Ethernet interfaces (eth0 and eth1 ).

- If your configuration uses only one network interface (referred to as a single NIC configuration), you only need to provide an IP address for eth0.
- If your configuration uses two network interfaces (referred to as a dual NIC configuration), you need to provide an IP address for eth0 and eth1.

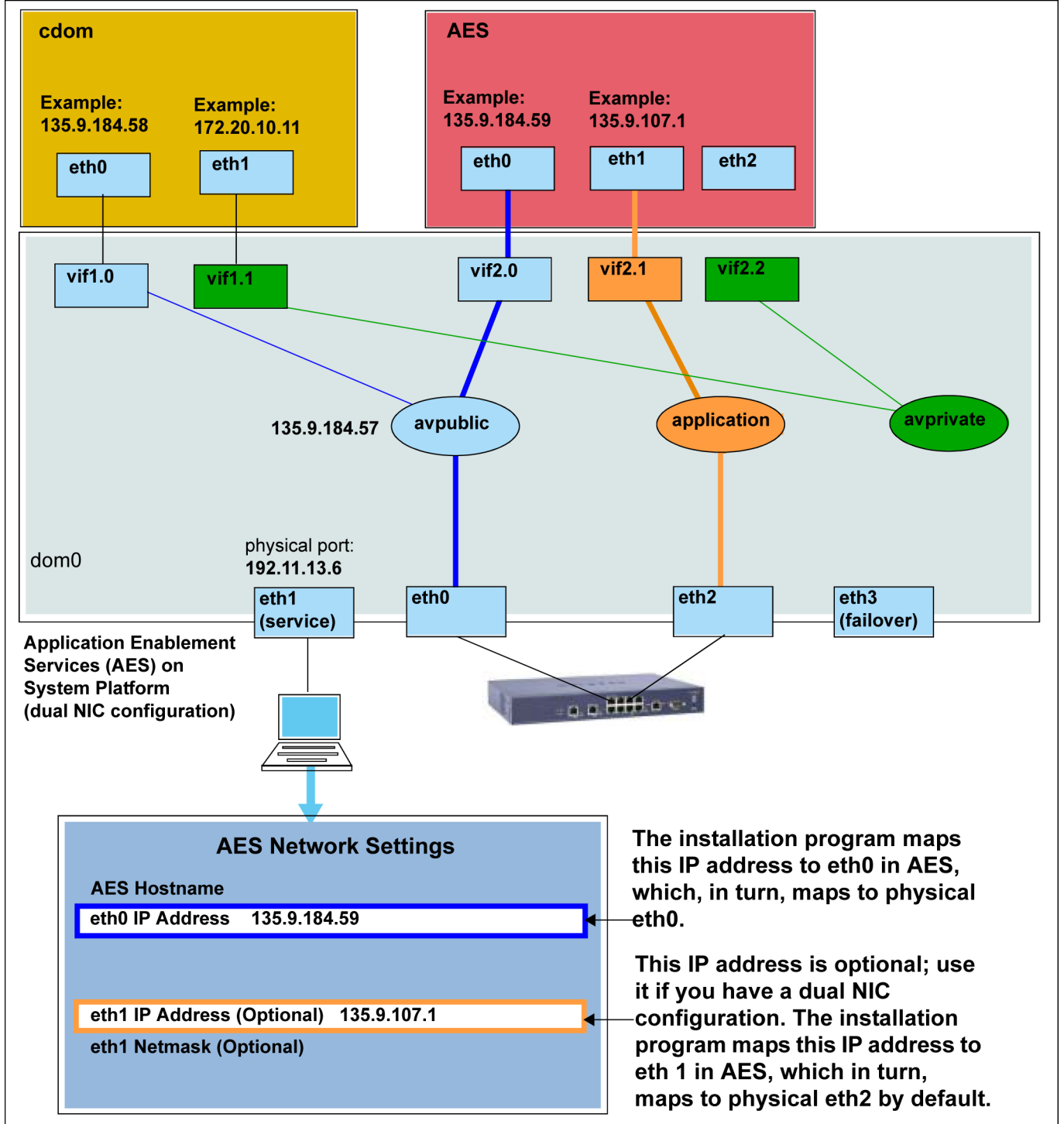
Keep in mind that these “eth” settings refer to virtual Ethernet interfaces. The installation program maps these virtual ethernet IP addresses to physical Ethernet interface ports, which are designated in the software as eth0, eth1, eth2, eth3. Virtual eth0 maps to physical eth0. Virtual eth1 maps to physical eth2 by default and can be configured to any other available port through the System Platform web console.

 **Note:**

In previous System Platform versions, physical eth2 was reserved for High Availability Failover, and the application bridge (virtual eth1) was assigned to physical eth3. From System Platform 6.0 and on, High Availability Failover can be configured on any free physical port through the System Platform web console.

All network configuration can be performed from the Avaya Aura® System Platform web console. For more information, see the *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02-300357.

# Application Enablement Services Ethernet interfaces



---

## Single NIC configuration

In a single NIC configuration, you use one network interface. That is, the AE Services server uses one NIC for client, switch, and media connectivity. The AE Services server, Communication Manager, and the client application computer must reside on a private LAN, a virtual LAN (VLAN), or a WAN.

In a single NIC configuration, you must configure the IP interface for the AE Services server to be accessible over the public Internet for the registration of IP endpoints.

The HP DL360 G7 server has six physical network interfaces: eth0, eth1, eth2, eth3, eth4, and eth5. The Dell R610 server and S8800 server have four physical network interfaces: eth0, eth1, eth2, and eth3. The eth1 interface is reserved for Avaya technicians to use for remote access.

### Important:

When you install the AE Services software, always use eth0 for a single NIC configuration.

### Note:

Eth0 and eth1 are virtual network interfaces in the AE Services virtual machine.

AE Services recommends a single NIC configuration for connectivity to most S8300, S8400, and S8500c Communication Manager media servers.

See [Required network interface \(NIC\) settings](#) on page 22 for more information.

---

## Dual NIC configuration

In a dual NIC configuration, you use two network interfaces for connectivity to two separate network segments. One network segment is used for switch connectivity to Communication Manager, and the other network segment for is used for client and media connectivity (LAN, VLAN, or WAN). The NICs must be on separate networks or network segments. In a dual NIC configuration, the client network is referred to as the production (or public) network, and the Communication Manager segment is referred to as the private network segment.

### Important:

When you install the AE Services software, always use the following settings for a dual NIC configuration:

- Use eth0 for the IP address of the AE Services server (production network).
- Use eth1 for the IP address of the private network.

### Note:

Eth0 and eth1 are virtual network interfaces in the AE Services virtual machine.

AE Services supports using a dual NIC configuration for S8400, S8500c, S8700, and S8800 Communication Manager media servers.

The Dell R610 server and the S8800 server have four physical network interfaces: eth0, eth1, eth2, and eth3. You can choose two of the three available network interfaces (eth0, eth2, or eth3). AE Services recommends that you use eth0 and eth2. The eth1 interface is reserved for Avaya technicians to use for remote access.

See [Required network interface \(NIC\) settings](#) on page 22 for more information.

---

## Network interface (NIC) settings

The NIC choices for all network interfaces are as follows:

- Auto-Negotiate:

- Gigabit interfaces: Auto-negotiation (auto-neg) - on

In this case, you must administer 1000-Mbps / full / auto-neg at each end of the Ethernet link.

- 100-Mbps interfaces: Auto-negotiation (auto-neg) - on

In this case, you must administer 100-Mbps / full / auto-neg at each end of the Ethernet link.

- Lockdown: 100-Mbps interfaces

100-Mbps interfaces: Lockdown (auto-neg) - off

In this case, you must administer 100-Mbps / full / Lockdown at each end of the Ethernet link.

 **Important:**

AE Services defaults to auto-negotiation mode; it negotiates the network speed and duplex mode with the Ethernet switch. Both ends of the Ethernet link must be set to the same mode. Otherwise, a duplex mismatch will occur. Verify that both ends of the Ethernet link operate at the same desired speed and duplex settings.

Keep in mind the following:

- Auto-neg is highly desired for Gigabit links.
- Auto-neg or Lockdown is acceptable for 100-Megabit links.
- Lockdown for Gigabit links is highly discouraged.
- 10-Megabit and/or half-duplex operation is never acceptable and should be corrected.

For detailed information about using auto-negotiation and Lockdown, see Ethernet Link Guidelines at <https://support.avaya.com/css/P8/documents/100121639>.

See “Editing the NIC configuration (optional)” in the *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02-300357, to set up the NICs with the recommended settings.

**\* Note:**

In AE Services 6.3.3, the NIC speed 1000, full duplex with auto-negotiate is supported if AE Services is connected to Communication Manager Processor Ethernet that has the same NIC settings.

---

## Network latency requirements

Regardless of the type of network used (LAN, VLAN or WAN), set up the TCP/IP links (CTI links) between the AE Services server and Communication Manager with the following network latency characteristics:

- No more than a 200 ms average round-trip packet delivery time, as measured with `ping` over every one-hour time period
- Periodic spiked delays of no more than 2 seconds while maintaining the 200 ms average round-trip delivery time, as measured with `ping` over every one-hour time period

These requirements are necessary to maintain the AE Services communication channel with each Communication Manager C-LAN over a LAN/VLAN or WAN. Considerations include:

- If the CTI application issues route requests, the associated vector “wait” step must have a value greater than the largest “periodic spiked delay”. With a maximum delay of 2 seconds, the wait step must be greater than 2 seconds. If you can guarantee “periodic spiked delays” of less than 2 seconds, you can reduce the wait step time-out accordingly.
- If the switch receives no response to a route select, the call will follow the remaining steps in this specific vector, so you must program the vector to deal with this condition. If you encounter “periodic spiked delays” greater than 2 seconds, messages are either:
  - Stored and retransmitted after recovering from a short network outage, or
  - Dropped during a long network outage

**\* Note:**

The communication channel between the AE Services server and the Communication Manager requires a hub or data switch. Avaya does not support the use of a crossover cable.

---

## Client workstation provisioning

Although client workstations are not a requirement for installing the AE Services software, you will need to provide workstations for the AE Services client applications.

- Device, Media, and Call Control (DMCC) clients: You can develop and run Device, Media, and Call Control applications on any computer that is capable of running the Java Platform, Standard Edition (Java SE) 1.7 or openJDK 7 client, a .NET client API for Windows, and an XML client API.

- TSAPI and CVLAN clients: See the *Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide (02-300543)* for hardware and software requirements.

---

## Communication Manager and media server requirements

To use AE Services 6.3.3, you must have the official Release 5.2.1, 6.0.x, 6.2 Service Pack 2, 6.3, 6.3.2, or 6.3.6 software running on an IP-enabled media server.

**\* Note:**

Communication Manager 5.2.1 or later provides link bounce resiliency for the Application Enablement Protocol (AEP) transport links that AE Services uses.

- AE Services supports all media servers and gateways that support Communication Manager Release 5.2.1, 6.0.x, 6.2 Service Pack 2, 6.3, or 6.3.2.
- AE Services 6.3.3 supports both CLAN interfaces and Processor Ethernet connections when implementing Enterprise Survivable Server (ESS) and Local Survivable Processor (LSP) configurations.
- AE Services DMCC applications that use the High Availability Failover feature require the Communication Manager H.323 Time-to-Service registration feature. These features are available only on Communication Manager 5.2.1 or later.

---

## Downloading the AE Services release notes

### About this task

Make sure you read the AE Services release notes before you install the software.

**\* Note:**

AE Services provides release notes as .PDF documents. Make sure you have the Adobe Acrobat Reader installed on your computer.

### Procedure

1. Using your web browser, go to <https://support.avaya.com>.
2. On the top of the Welcome to Avaya Support page, click **DOWNLOADS & DOCUMENTS**.
3. In the Enter Your Product Here box on the Downloads & Documents page, type `Application Enablement Services`.
4. From the drop-down list, select **AES**.
5. From the Choose Release box, select **6.3.x**.
6. In the Filters area, click **Release Notes & Software Update Notes**.
7. Click the title of the release notes.



Your browser displays the release notes as a .PDF document.

8. (Optional) Save the .PDF document to your computer.

---

## Installation process overview

### About this task

Installation of System Platform consists of the following tasks:

### Procedure

1. Install the server hardware.
2. Connect the server to the customer network.

This step is for best practice, although it is possible to install the System Platform software without an initial connection to the customer network.

3. Connect the two servers if using a System Platform High Availability option.

 **Note:**

Cable interconnection requirements depend typically on the configured System Platform HA mode, Ethernet specifications, restrictions on the use of layer-2 switches to extend maximum cable distance, and in a small percentage of site-specific scenarios, ambient electrical and signal noise (RFI) affecting the choice of Ethernet cable types (for example, CAT5E, CAT5A, CAT6A). For more details, see topics associated with System Platform HA cable requirements in your Avaya Solution documentation.

4. Install the System Platform software, service packs, and any required Feature Pack on the server. If using the High Availability Failover option, also install the System Platform software, service packs, and any required Feature pack on the standby server.
5. Configure the Secure Access Link (SAL) Gateway for remote support and alarming. You can use the SAL Gateway that is included with System Platform or installed on a standalone SAL Gateway.

 **Note:**

On systems using High Availability operation, configure the SAL Gateway only on the primary server. When you enable High Availability operations, SAL Gateway will propagate to the standby server.

6. Install the solution template.

 **Important:**

If you have a System Platform High Availability configuration, do not install a template on the standby node. If you do, you will be unable to start High Availability operation. If you are using a bundled System Platform installation (with a solution template), disable the

template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability operation.

7. Configure High Availability if using that option.

# Chapter 3: Installation prerequisites

---

## Application Enablement Services on System Platform installation overview

The Avaya Aura® Application Enablement Services on System Platform installation has many parts to it. It requires:

- installing the server (or servers) hardware
- connecting the server to the customer's network
- connecting two servers if using the high availability failover option
- installing the System Platform software on the server
- installing the System Platform 6.3.4 feature pack on the server
- installing the Application Enablement Services software on the server
- configuring the Secure Access Link (SAL) gateway included in System Platform for remote support and alarming

### Server hardware installation and connectivity

Application Enablement Services on System Platform is installed on a Dell R620 server, an HP DL360 G7 server, or a Dell R610 server. The server arrives at the customer's site with all the appropriate components and memory. Nothing needs to be added to the server on site.

The server (or servers) require CAT5 Ethernet cables to connect to the customer's network. For FRHA mode, both servers must be connected back-to-back with a gigabit-crossover cable on the ports identified as the High Availability Failover configured port on the System Platform. For MPHA mode, both servers must be connected back-to-back with a CAT6 Ethernet cable on a 10 Gigabit NIC port identified as the High Availability Failover configured port on the System Platform.

### Application Enablement Services on System Platform software

You can install Application Enablement Services on System Platform using two different methods:

- A laptop connected to the Services port on the server (this port is identified as eth1 in the server).
- A video monitor, keyboard, and mouse connected to the appropriate ports on the server.

Access the System Platform installer and the Application Enablement Services installer through DVDs. You must burn the ISO images to blank DVDs. Avaya recommends that you verify that the ISO images are not corrupted before starting each installation.

A worksheet that identifies information required at time of installation is provided. Complete this worksheet prior to installation. See [Installation worksheet for AES on](#) on page 29.

### Product Licensing and Delivery System (PLDS)

The Application Enablement Services on System Platform downloadable software and the licenses for installing Application Enablement Services on System Platform are available in the PLDS Web site (<https://plds.avaya.com>).

**\* Note:**

A license can not be generated for Application Enablement Services on System Platform until the MAC address on the Console domain (Cdom) is determined. This address is not known until after AE Services is installed.

### Secure Access Link (SAL)

Application Enablement Services on System Platform includes the Avaya Secure Access Link (SAL) gateway to manage service delivery (alarming and remote access). SAL requires upload bandwidth (customer to Avaya) of at least 90kB/s (720kb) with latency no greater than 150 ms (round trip.)

You must configure SAL with the customer's network and register during the installation process. For Avaya to provide support, Business Partners and/or their customers need to ensure that SAL is configured and registered properly. Avaya support will be delayed or not possible if SAL is not properly implemented.

Business Partners without a SAL Concentrator must provide their own B2B VPN connection (or other IP-based connectivity) to deliver remote services. SAL does not support modem connections.

---

## What Avaya provides

Avaya provides the following items for installing System Platform:

- One or two servers. One is for a standard configuration, and two are for High Availability Failover configuration.
- Slide rails to mount the servers in a standard 19-inch, 4-post rack that have square holes.
- System Platform installation software.
- Other hardware as ordered, such as an uninterruptible power supply (UPS). UPS is a required component.
- Product registration form. The form is available on <http://support.avaya.com>. Click **More Resources > Avaya Equipment Registration**. Under **Non-Regional (Product) Specific Documentation**, click **Universal Install/SAL Product Registration Request Form**. For more information, see [Registering the system](#) on page 34.

**\* Note:**

Avaya provides the System Platform installation software. The customer must either buy the System Platform DVD or download the ISO image and write that image to a DVD.

---

## What customer provides

The customer must provide the following items for installing System Platform.

- Standard equipment rack correctly installed and solidly secured.
- USB keyboard, USB mouse, and VGA monitor or laptop with an Ethernet crossover cable.

**\* Note:**

Some laptop computer Network Interface Cards (NICs) provide an internal crossover option that makes it possible to use a straight-through Ethernet cable for this connection. See the documentation for your laptop computer to determine whether this option is available.

The supported keyboard types are sg-latin1, sk-qwerty, slovene, sv-latin1, trq, uautf, uk, and us.

- Gigabit-certified Ethernet cable for High Availability Failover.
- DVDs written with the software for installing.
- A computer that can route to the System Platform server and has a supported version of Internet Explorer or Firefox installed. Internet Explorer versions 7 through 9 are supported. Firefox versions 3.6 through 19 are supported.
- Filled-out worksheets with the system and network information needed for installation and configuration.
- (Optional) Electronic preinstallation worksheet (EPW) and Avaya Bulk Import Tool (ABIT) files.
- Access to the customer network.
- (Optional) VPN Gateway for providing remote access to Avaya Partners.

**\* Note:**

Avaya Partners must arrange for their own IP-based connectivity (for example, B2B VPN) to provide remote services. Modem connectivity is unsupported.

**\* Note:**

Secure Access Link (SAL) Gateway is required for remote service and alarming. System Platform includes an embedded SAL Gateway, or you can use a standalone SAL Gateway.

---

## Installation worksheet for AES on System Platform

The Application Enablement Services installer and System Platform installer require you to fill in several fields. Having the information available at the time of installation makes it go faster and ensures accuracy.

Print out the following tables and work with your network administrator to fill in the rows.

### System Domain (Dom-0) network

Field	Value	Notes
IP address		
Hostname		This is the hostname for System Domain (Dom 0).

### Console Domain network

Field	Value/requirement	Notes
IP address		The Console Domain does not have a physical interface. It has a virtual interface that uses the physical interface in System Domain (Domain-0). Because System Domain acts like a bridge, the IP address that you enter here must be a valid IP address. Further, the Console Domain must be on the same network as System Domain (Domain-0).
Hostname		This is the hostname for Console Domain.

### General network settings

Field	Value/requirement	Notes
Network mask		
Default gateway		This will be the default gateway for all the virtual machines, if you do not configure gateways for them.
Primary DNS		
Secondary DNS		Optional
NTP Server 1		Use of NTP server is optional. However, Avaya recommends its use.
NTP Server 2		Optional
NTP Server 3		Optional

### Ethernet interface that connects to the customer network

This field displays the physical Ethernet interface (NIC) that connects to the customer network. You must configure this interface for IP.

The specific Ethernet interface number depends on the server model being used.

Field	Value/requirement	Notes
Static IP		The static IP address for the Ethernet interface that connects to the customer network.
Subnet mask	255.255.255.0 (default)	
Default gateway IP		

### Services Virtual Machine Configuration

Name	Value	Description
<b>Enable Services VM</b>		<p>Enables or disables remote access. Also supports local or centralized alarm reporting.</p> <p>Default value: <b>Enabled</b></p> <p>Leave the <b>Enable services VM</b> option enabled (checkmark) for remote access and local SAL support, or disabled (no checkmark) if you have a separate server dedicated for independent/centralized remote access and SAL support.</p> <p>In a System Platform High Availability configuration, the active node automatically propagates to the standby node, any change in the setting for this field</p>
<b>Hostname</b>		The name assigned to the Services Virtual Machine
<b>Static IP address</b>		The IP address assigned to the Services Virtual Machine. The address must be on the same subnet assigned to the Domain 0 (dom0) and Console Domain (cdom) virtual machines.
<b>Virtual devices</b>		The virtual device (port) assigned to the Services Virtual Machine. Default value (eth0) automatically assigned. No user input necessary.

### Passwords

Default passwords are provided. You should change these default passwords.

Field	Value/requirement	Notes
root		
admin		
cust		
ldap		

### Application Enablement Services template installation

These fields are on the Template Details page.

Field	Value/requirement	Notes
AES hostname		
ETH0 IP address of the AES		
ETH1 IP address of the AES		
ETH1 network mask		



# Chapter 4: Preinstallation tasks for System Platform

## Preinstallation checklist for System Platform

Before starting System Platform installation, ensure that you complete the tasks from the following preinstallation checklist.

No.	Task	Notes	✓
1	Complete and submit the Universal Install/SAL Product Registration Request form. When opening the Excel based form, click <b>Enable Macros</b> ; otherwise, the form automation will not work. Submit the completed form using the built in email button. See <a href="#">Registering the system</a> on page 34.	<b>!</b> <b>Important:</b> Submit the registration form three weeks before the planned installation date.	
2	Gather the required information about installation, such as IP configuration information, DNS addresses, and address information for Network Time Protocol (NTP) servers.  See <a href="#">Installation worksheet for System Platform</a> on page 202.		
3	Register for PLDS unless you have already registered. See <a href="#">Registering for PLDS</a> on page 35.		
4	Download the System Platform installer ISO image file from PLDS.  See <a href="#">Downloading software from PLDS</a> on page 36.		
5	Download the appropriate solution template and licenses from PLDS.  See <a href="#">Downloading software from PLDS</a> on page 36.		
6	Verify that the downloaded ISO images match the images on the PLDS website.		

*Table continues...*

No.	Task	Notes	✓
	See <a href="#">Verifying the ISO image on a Linux-based computer</a> on page 36 and <a href="#">Verifying the ISO image on a Windows-based computer</a> on page 37.		
7	Write the ISO images to separate DVDs. See <a href="#">Writing the ISO image to DVD or CD</a> on page 38.	<p><b>* Note:</b></p> <p>If the software files you are writing on media are less than 680 Mb in size, you can use a CD instead of a DVD.</p>	

## Registering the system

### About this task

Registering System Platform and applications in the solution template ensures that Avaya has a record of the system and it is ready for remote support if needed.

Avaya assigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway and managed device that is registered. In System Platform, managed devices are the components of System Platform and of the applications in the solution template. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely. The Product ID is in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

**\* Note:**

- For a description of any elements you must register with your Solution Template, see your Avaya Aura<sup>®</sup> solution documentation.
- For solutions being deployed in a System Platform High Availability configuration, you must register two VSP solution elements, one for the primary server and one for the secondary server in the HA pair. For a description of any other solution elements you must register for the various System Platform High Availability deployments, see your Avaya Aura<sup>®</sup> solution documentation.

Registrations are performed in two stages: before installation of System Platform, the solution template, and SAL Gateway and after installation. The first stage of registration provides you with the SE IDs and Product Identifications required to install the products. The second stage of the registration makes alarming and remote access possible.

### Procedure

1. Gain access to the registration form and follow the instructions. The SAL registration form is available at <http://support.avaya.com>. In the Help & Policies section, click **More Resources**. The system displays the More Resources page. Click **Avaya Equipment Registration**, and search for *SAL Universal Install Form Help Document*.

2. Complete the Universal Install Product Registration page and submit it at least three weeks before the planned installation date.

Provide the following:

- Customer name
- Avaya Sold-to Number (customer number) where the products will be installed
- Contact information for the person to whom the registration information should be sent and whom Avaya can contact if any questions come up
- Products in the solution template and supporting information as prompted by the form

Avaya uses this information to register your system. When processing of the registration request is complete, Avaya sends you an email with an ART install script attached. This script includes instructions for installation and the SE IDs and Product IDs that you must enter in SAL Gateway to add managed devices.

3. Complete and submit the Universal Install Alarm Registration page after the installation is complete.

#### Related links

[Configuration prerequisites](#) on page 124

[SAL Gateway](#) on page 123

[Gateway Configuration field descriptions](#) on page 127

---

## Registering for PLDS

### Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com>.

The PLDS website redirects you to the Avaya single sign-on (SSO) webpage.

2. Log in to SSO with your SSO ID and password.

The PLDS registration page is displayed.

3. If you are registering:

- as an Avaya Partner, enter the Partner Link ID. If you do not know your Partner Link ID, send an email to [pradmin@avaya.com](mailto:pradmin@avaya.com).
- as a customer, enter one of the following:
  - Company Sold-To
  - Ship-To number
  - License authorization code (LAC)

4. Click **Submit**.

Avaya will send you the PLDS access confirmation within one business day.

---

## Downloading software from PLDS

### About this task

**\* Note:**

You can download product software from <http://support.avaya.com> also.

### Procedure

1. Type <http://plds.avaya.com> in your Web browser to go to the Avaya PLDS website.
  2. Enter your Login ID and password to log on to the PLDS website.
  3. On the Home page, select **Assets**.
  4. Select **View Downloads**.
  5. Search for the available downloads using one of the following methods:
    - By download name
    - By selecting an application type from the drop-down list
    - By download type
- After entering the search criteria, click **Search Downloads**.
6. Click the download icon from the appropriate download.
  7. When the system displays the confirmation box, select **Click to download your file now**.
  8. If you receive an error message, click the message, install Active X, and continue with the download.
  9. When the system displays the security warning, click **Install**.

When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

---

## Verifying the downloaded ISO image

---

### Verifying the ISO image on a Linux-based computer

#### About this task

Use this procedure to verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

Use this procedure if you downloaded ISO images to a Linux-based computer.

## Procedure

1. Enter `md5sum file name`, where *file name* is the name of the ISO image. Include the .iso file name extension.
2. Compare the md5 checksum of the ISO image to be used for installation with the md5 checksum that is displayed for the ISO image on the PLDS Web site.
3. Ensure that both numbers are the same.
4. If the numbers are different, download the ISO image again and reverify the md5 checksum.

---

## Verifying the ISO image on a Windows-based computer

### About this task

Use this procedure to verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

Use this procedure if you downloaded ISO images to a Windows-computer.

### Procedure

1. Download a tool to compute md5 checksums from one of the following Web sites:
  - <http://www.md5summer.org/>
  - <http://code.kliu.org/hashcheck/>

 **Note:**

Avaya has no control over the content published on these external sites. Use the content only as reference.

2. Run the tool on the downloaded ISO image and note the md5 checksum.
3. Compare the md5 checksum of the ISO image to be used for installation with the md5 checksum that is displayed for the ISO image on the PLDS Web site.
4. Ensure that both numbers are the same.
5. If the numbers are different, download the ISO image again and reverify the md5 checksum.

---

## Writing the downloaded software to DVD

---

### DVD requirements

Use high-quality, write-once, blank DVDs. Do not use multiple rewrite DVDs which are prone to error.

When writing the data to the DVD, use a slower write speed of 4X or a maximum 8X. Attempting to write to the DVD at higher or the maximum speed rated on the disc is likely to result in write errors.

 **Note:**

If the software files you are writing on media are less than 680 Mb in size, you can use a CD instead of a DVD.

---

## Writing the ISO image to DVD or CD

### Before you begin

1. Download any required software from PLDS.
2. Verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

### About this task

If you are writing to a DVD, this procedure requires a computer or server that has a DVD writer and software that can write ISO images to DVD. If you are writing to a CD, this procedure requires a computer or server that has a CD writer and software that can write ISO images to CD.

 **Important:**

When the ISO image is writing to the DVD, do not run other resource-intensive applications on the computer. Any application that uses the hard disk intensively can cause a buffer underrun or other errors, which can render the DVD useless.

### Procedure

Write the ISO image of the installer to a DVD or CD.

# Chapter 5: Installing the Dell PowerEdge R620 Server

---

## Dell R620 Server overview

The Avaya Common Servers category includes the Dell™ PowerEdge™ R620 1U server that supports several Avaya software solutions, some requiring additional hardware and memory requirements beyond the standard configuration. This book covers the standard configuration only—consult specific Avaya product documentation for application-specific or solution-specific server configurations.

- Avaya Common Servers are supplied under an OEM relationship and Avaya servers are treated differently than commercially available servers from the vendors.
- Neither customers, business partners, distributors, nor Avaya Associates interacting with customers and business partners, should get BIOS or other firmware updates for any third party OEM servers forming part of Avaya's turnkey appliance offers. Only consult Avaya-provided downloads, information and support. Send questions to the Server Product Management mailbox at [svrprodmgmt@avaya.com](mailto:svrprodmgmt@avaya.com).
- Avaya Common Servers are turnkey appliances. No servers designed for a particular application can be repurposed for use with another application. The only exception to this is when an application has provided an upgrade or migrate path from an existing server state to a different server state with the appropriate kits, tools, documentation, and training materials. For example, Avaya Aura Messaging is providing a kit plus documentation for migrating a server running Modular Messaging to Avaya Aura Messaging.
- Remote access and use of Dell iDRAC hardware management tools for the Dell R620 server are not supported by any Avaya application (Dell iDRAC).
- Do not contact Dell for Service; all support, warranty, repair, and maintenance are through the Avaya processes.
- Avaya strongly recommends that all servers are protected with an Uninterruptible Power Supply for power surge and interruption protection. Avaya is not responsible for servers damaged by power surges, brown outs, black outs etc. when the server is connected to standard power mains and has no protection.
- Substitution of a DC power supply in a server must be approved by the Application Product Manager before any substitution is made. If there is a significant demand for a turnkey solution with a DC power supply, an Avaya GRIP (Global Requirements Integration Process) request must be submitted. Partners registered to use this process can submit a GRIP request at <https://portal.avaya.com/apps/grip/partner.asp>. Avaya Associates may assist and can find

information about this process at <http://spark4.avaya.com/grip> Note, a GRIP request must be made for the Avaya application product, not the server model. The decision on whether to include a turnkey offer with a DC power supply is the responsibility of each Avaya application Product Manager. The name of the Product Managers for each application can be found at the bottom of the application page on the Avaya Global Sales portal.

- Dell's RAID battery is a consumable item that can be purchased as a part without a Service ticket. Customers are responsible for installing them, the procedure for which is in the Maintaining and troubleshooting document or in appropriate OEM vendor documentation. The Avaya Service Notice about the RAID battery as consumable is Service Bulletin SB000130.
- Product labels on the servers themselves have the 9-digit base server codes for Avaya Services in service and support. These 9-digit codes differ from the 6-digit orderable codes under which servers are ordered. On every server package, there is a Packing Label and a Hierarchy Label. The Hierarchy Label itemizes the stock list in the box of the 6-digit orderable code and Avaya recommends retaining them for reference.
- Quality assurance - product integrity testing/environmental international restrictions/ has been completed by Dell and verified with Avaya through the use of Design for Environmental Checklists. These lists include: batteries, printed wiring boards, plastic parts, product packaging, RoHS, green requirements, and energy efficiency.

---

## Downloading Dell documentation

Use this procedure to find and download the Dell™ PowerEdge™ R620 documentation from Dell.

### Procedure

1. Open a browser and to go <http://www.support.dell.com>.
2. On the Welcome to Dell Support page click on the `Start Here` button in the Support for Work section.
3. On the Support for Work page click on `Servers, Storage and Networking` in the "choose a product category" section.
4. On the next page click on `PowerEdge`.
5. On the Choose your Dell PowerEdge page, click on `PowerEdge R620`.
6. On the Product Support for PowerEdge R620 page click on `Manuals and Documentation`.
7. Click the link that corresponds to the document that you want to download.
8. Download the documents in the *Dell R620 document set > Documents to download* section below.



## Dell R620 documentation set

Refer to the documents listed below for Dell R620 server installation information and procedures.

**\* Note:**

Download the documents listed in the *Documents to download* section below. Printed copies of the documents listed in the *Documents included in the shipping container* section below ship with the server.

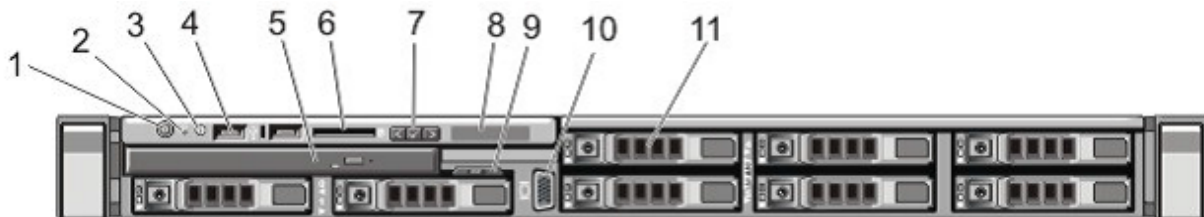
### Documents to download

Title
Getting Started Guide
Owner's Manual
Technical Guide

### Documents included in the shipping container

Title
Product Information Guide
Rack Installation Instructions

## Front view of Dell R620 Server



**\* Note:**

Most Avaya servers ship with 2–4 hard disk drives, depending upon product requirements. The remaining hard drive bays (slots 4–7) will not be operable. A plate will be covering the 4 slots on the right side of the server.

No.	Item	Icon	Description
1	Power-On Indicator, Power Button		The power-on indicator lights when the system power is on. The power button controls the power supply output to the system.

*Table continues...*

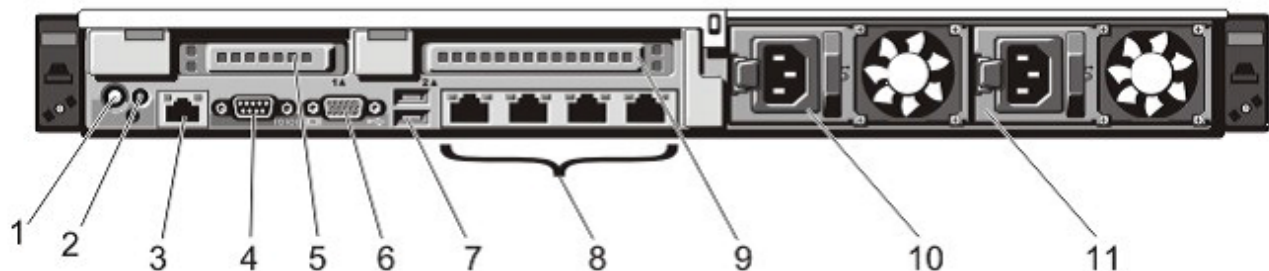
			<p><b>* Note:</b></p> <p>On ACPI-compliant operating systems, turning off the system using the power button causes the system to perform a graceful shutdown before power to the system is turned off.</p>
2	NMI Button		<p>Used to troubleshoot software and device driver errors when running certain operating systems. This button can be pressed using the end of a paper clip.</p> <p>Use this button only if directed to do so by qualified support personnel or by the operating system's documentation.</p>
3	System Identification Button		<p>The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the LCD panel on the front and the system status indicator on the back flashes blue until one of the buttons are pressed again.</p> <p>Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode.</p>
4	USB Connectors (2)		<p>Allows you to insert USB devices to the system. The ports are USB 2.0-compliant.</p>
5	Optical Drive		<p>One optional SATA DVD-ROM drive or DVD+/-RW drive.</p> <p><b>* Note:</b></p> <p>DVD devices are data only.</p>
6	vFlash Media Card Slot (Not populated for Avaya)		<p>Allows you to insert a vFlash media card.</p>
7	LCD Menu Buttons		<p>Allows you to navigate the control panel LCD menu.</p>
8	LCD Panel		<p>Displays system ID, status information, and system error messages. The LCD lights blue during normal system operation. The LCD lights amber when the system needs attention, and the LCD panel displays an error code followed by descriptive text.</p> <p><b>* Note:</b></p> <p>If the system is connected to AC power and an error is detected, the LCD lights amber regardless of whether the system is turned on or off.</p>

*Table continues...*

9	Information Tag		A slide-out label panel, which allows you to record system information, such as Service Tag, NIC, MAC address, and so on as per your need.
10	Video Connector		Allows you to connect a VGA display to the system.
11	Hard Drives		A typical Avaya configuration has up to four 2.5 inch hot-swappable hard drives. The other hard drive bays will not be operable. High density HDD Avaya products will ship with 8 slots.

More information can be found in the Dell Owner’s Manual, in the Front Panel Features and Indicators section.

## Back view of Dell R620 Server



No.	Item	Icon	Description
1	System Identification Button		<p>The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the LCD panel on the front and the system status indicator on the back blink until one of the buttons are pressed again.</p> <p>Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode.</p> <p>To reset iDRAC (if not disabled in F2 iDRAC setup) press and hold for more than 15 seconds.</p>
2	System Identification Connector		Allows you to connect the optional system status indicator assembly through the optional cable management arm.
3	iDRAC Enterprise Port		Dedicated management port.

*Table continues...*

			<p><b>* Note:</b> The port is available for use only if the iDRAC7 Enterprise license is installed on your system. (Not normally used in Avaya systems)</p>
4	Serial Connector		Allows you to connect a serial device to the system.
5	PCIe Expansion Card Slot 1 (riser 2)		Allows you to connect a PCIe expansion card.
6	Video Connector		Allows you to connect a VGA display to the system.
7	USB Connectors (2)		Allows you to connect USB devices to the system. The ports are USB 2.0-compliant.
8	Ethernet Connectors (4)		<p>Four integrated 10/100/1000 Mbps NIC connectors (Avaya Standard)</p> <p><b>* Note:</b> Dell R620 NIC port numbers are read from <b>left to right</b>, starting with Port 1, then continuing 2, 3 and port 4.</p>
9	PCIe expansion card slot 2 (riser 3)		Allows you to connect a PCIe expansion card.
10	Power Supply (PSU1)		AC 495W, 750W
11	Power Supply (PSU2)		AC 495W, 750W

More information can be found in the Dell Owner’s Manual, in the Back Panel Features and Indicators section.

## Dell R620 Server specifications

Base unit	Baseline	Options
R620	1U chassis, dual socket	Listed below
Processor	<p>Intel E5-2630, Six Core 2.3GHz (Sandybridge)</p> <p>4 memory channels per CPU with up to 3 DIMMs per channel (most applications use 1 or 2 DIMMs per channel to optimize memory speed)</p>	<ul style="list-style-type: none"> <li>Intel E5-2667 six Core/2.9 GHz (Sandybridge)</li> <li>Upgradable to dual processors for either E5-2630 or E5-2667</li> </ul>
Memory	4GB DDR3 RDIMMs	Max Capacity for memory: RDIMM – up to 96GB (2 cpus)
HW RAID	H710 RAID controller with 512MB Cache and battery backup. Optioned as RAID 1 or 5	Other RAID configurations available

*Table continues...*

Base unit	Baseline	Options
Hot-Plug disk drive cage	8 Small Form Factor 2.5" hot-plug hard drive bays are available when an optical drive is installed. A typical Avaya configuration has up to four 2.5 inch hot-swappable hard drives.	High density HDD Avaya products will ship with 8 slots.
Disk drive	300GB SAS 2.5" 10K RPM 6G DP Hard Drive. Two base configurations: <ul style="list-style-type: none"> <li>• 299.96GB total: RAID 1, 2 x 300GB drives</li> <li>• 599.93GB total: RAID 5, 3 x 300GB drives</li> </ul>	<ul style="list-style-type: none"> <li>• Additional 300GB 10K RPM SAS drive</li> <li>• High performance 300GB 15K SAS drives</li> <li>• High capacity 600GB 10K SAS drives</li> </ul>
NICs	4 integrated ENET Gigabit NIC ports with TCP offload engine (included on motherboard)	Broadcom 5720 Dual Port 1GbE NIC (430-3261)
PCI slots	2 PCIe risers (left and center)	<p>(Riser 2, Slot 1) One half-height, half-length x8 link or one half-height, half-length x16 link</p> <p><b>* Note:</b></p> <p>Both processors must be installed to use the slots on the x16 link on riser 2.</p> <p>(Riser 3, Slot 2) One full-height, three fourth-length x16 link or one half-height, half-length x16 link</p>
Removable media	Slim line SATA DVD-RW optical drive (used in all Avaya configurations)	No additional options supported.
Power supply	495W AC Hot Plug Power Supplies	<ul style="list-style-type: none"> <li>• 750W AC power supply</li> <li>• Single and dual power supply configurations</li> </ul>
Fans	7 Fan modules	7 Fan modules
Additional items	2 front USB, 4 back USB, and 1 internal USB port  Front Video Connector	

## Dell R620 altitude and air pressure requirements

A table listing the altitude and air pressure requirements for the Dell R620 server.

	Altitude
Operating	–15.2 m to 3048 m (–50 to 10,000 ft)  * <b>Note:</b> For altitudes above 2,950 ft, the maximum operating temperature is de-rated 1°F per 550 ft.
Storage	–15.2 m to 10,668 m (–50 ft to 35,000 ft)

## Dell R620 temperature and humidity requirements

This is a table of the temperature and humidity requirements for the Dell R620 server.

Specification	Value
<b>Temperature range</b>	
Operating	10° to 35 °C (50° to 95 °F) with no direct sunlight on the equipment.  * <b>Note:</b> For altitudes above 2950 ft, the maximum operating temperature is derated 1 °F / 550 ft.
Storage	–40° to 65° C (–40° to 149° F) with a maximum temperature gradation of 20 °C per hour
<b>Relative humidity</b>	
Operating	20% to 80% (non-condensing) at a maximum wet bulb temperature of 29 °C (84.2 °F)
Non-operating	5% to 95% at a maximum wet bulb temperature of 38 °C (100.4 °F)

## Dell R620 Server power specifications

Specification	Value
BTU	1057.8 BTU/hr
Voltage	110 VAC (100–240 VAC auto-ranging 50/60 Hz)
Plug Type	NEMA 5-15P
Circuit Breaker	15 amp
Pole	1
AMP Draw	2.8 amps (based on 110 voltage)

**\* Note:**

The above power configuration is based on the following example:

- 2qty – E5-2630 Processors
- 2qty – 495W power supplies
- 2qty – 300GB HDDs
- CPU load 100%
- 8qty – 4GB 1600mHz RDIMMs

---

## Installing the server in the rack

### About this task

**\* Note:**

Although not used frequently, Avaya customers are required to have a monitor, USB keyboard, and USB mouse available for use by installation and/or servicing technicians.

### Procedure

1. Examine contents of shipping container (Avaya provided equipment), and ensure that the 6-digit material code on the order matches the 6-digit material code on the shipping container.
2. Verify that the rack is installed according to the manufacturer's instructions and in accordance with all local codes and laws. Verify that the rack is grounded in accordance with local electrical code.

See the *Rack Installation Instructions* that are shipped with the hardware for more information.

3. Remove the cabinet doors, if necessary.
4. Attach the rails to the rack

The rails included with the server will accommodate most square-hole racks. If these rails do not fit the rack, the customer must provide rails or a shelf for rack installation. Also, the rails included with the server might not work with round-hole racks. The customer can obtain rails and/or a shelf from any distributor, for example <http://www.racksolutions.com/>. The customer-provided rails and rack must be on site prior to the first day of installation.

**\* Note:**

The customer is responsible for any rack screws.

5. Attach the server to the rack.
6. Connect the power cord(s).

See the *Getting Started Guide* sections: “connecting the power cables” and “securing the power cord” for more information.

---

## Installing a 10 Gb network-interface card

### Before you begin

- Take an inventory of the network-interface cards on site.
- Ensure connectivity.
- Always follow safe electrostatic discharge (ESD) practices.

### About this task

Use this procedure to install a 10 Gb network-interface card in a Dell R620 server.

#### **Note:**

- Install network-interface cards before mounting and cabling.
- You must install the 10 Gb network-interface card in PCIe slot #1 of the server.

### Procedure

1. Power down the server.
  - a. Back up the AE Services database.
  - b. Shut down the operating system as directed by the operating system documentation.
  - c. Power down the server.
  - d. Disconnect the power cords.

2. Open the system.

#### **Warning:**

To prevent damaging the system, follow safe electrostatic discharge (ESD) practices.

3. Locate PCIe slot #1, which is located on riser 2.
4. Open the expansion card latch and remove the filler bracket (if applicable) for PCIe slot #1.
5. Holding the 10 Gb network-interface card by its edges, position the card so that the card-edge connector aligns with the expansion-card connector for slot #1.
6. Insert the card-edge connector firmly into the expansion-card connector until the card is fully seated in slot #1.
7. Slide the expansion-card latch into position.
8. Close the system.
9. Reconnect all peripheral cables and power cords.
10. Connect the CAT6A crossover cable to the port on the 10 Gb network-interface card you just installed.
11. Power up the server.



# Chapter 6: Installing the HP DL360 G7 server

---

## HP DL360 document set

See the following documents for HP DL360 server information and procedures.

### Documents

- HP ProLiant Servers Safety Information
- HP ProLiant DL360 G7 Server Maintenance and Service Guide
- HP ProLiant Servers Troubleshooting Guide
- HP ProLiant DL360 G7 Server User Guide

### Documents included in the shipping container

Abbreviation	Title	Part number
1URH	1U Rack Hardware Installation Instructions	365 494–004
PCS	Power Cord Strain Relief Kit	407 454–021

---

## Downloading HP documentation

Use this procedure to find and download the HP ProLiant DL360 G7 documentation.

### Procedure

1. Open a browser and go to <http://support.avaya.com>.
2. Expand **Documentation** in the left hand menu.
3. Click **View All Documents**.
4. Click **C** in the alphabetical list along the top of the screen.
5. Scroll down to **Common Servers** in the C products.
6. Download the documents that you need.

## Specifications for HP DL360 G7 server with P410i RAID controller

For new installations of Application Enablement Services on System Platform, the new HP DL360 G7 server with a P410i RAID controller is required. The following table provides the specifications for this server.

Component	Description
Processor	One Intel Xeon E5620 quad core, 2.40 GHz
Memory	12 GB RAM
Hard Drives	Two 2.5-inch 300 GB 10 K SAS disk drives
RAID Controller	One P410i RAID-1
Drives	DVD read-only drive

## HP DL360 G7 Server physical specifications

Type	Description
Dimensions	Height: 4.32 cm (1.70 in)
	Width: 42.62 cm (16.78 in)
	Depth: 69.53 cm (27.38 in)
Weight (maximum; two processors, two power supplies, eight hard disk drives)	15.97 kg (35.20 lb)
Weight (minimum; one processor, one power supply, no hard drives)	14.51 kg (32.00 lb)
Weight (no drives installed)	14.06 kg (31.00 lb)

## HP DL360 G7 Server power specifications

Specification	Value
BTU	1794
Voltage	120 VAC
Plug Type	NEMA 5–15P
Circuit Breaker	15 amp

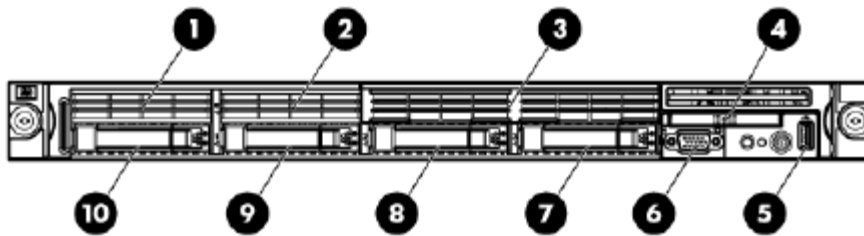
*Table continues...*

Specification	Value
Pole	1
AMP Draw	5.5

## HP DL360 G7 Server environmental specifications

Specification	Value
<b>Temperature range</b>	<p><b>* Note:</b></p> <p>All temperature ratings shown are for sea level. An altitude derating of 1°C per 300 m (1.8° per 1,000 ft.) to 3048 m (10,000 ft.) is applicable. No direct sunlight allowed.</p>
Operating	10°C to 35°C (50°F to 95°F)
Shipping	-40°C to 70°C (-40°F to 158°F)
Maximum wet bulb temperature	28°C (82.4°F)
<b>Relative humidity (noncondensing)</b>	<p><b>* Note:</b></p> <p>Storage maximum humidity of 95% is based on a maximum temperature of 45° C (113°F). Altitude maximum for storage corresponds to a pressure minimum of 70 kPa.</p>
Operating	10% to 90%
Non-operating	5% to 95%

## Front view of HP DL360 G7 Server

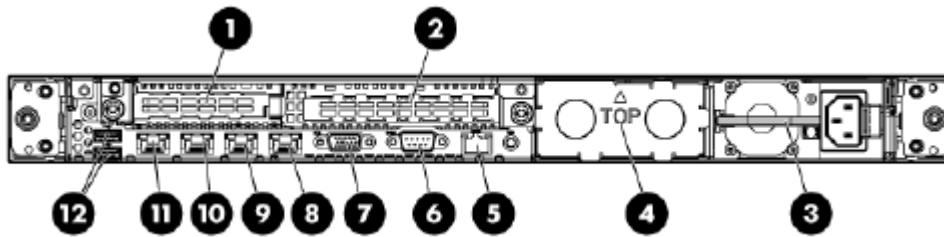


**\* Note:**

Servers ship with 2–4 hard disk drives, depending upon product requirements.

No.	Description
1	Not present
2	Not present
3	DVD-RW
4	HP Systems Insight Display
5	Front USB connector
6	Video connector
7	Hard drive bay 4
8	Hard drive bay 3
9	Hard drive bay 2
10	Hard drive bay 1

## Back view of HP DL360 G7 Server



No.	Description
1	Slot 1 PCIe2 x8 (8, 4, 2, 1) * <b>Note:</b> Servers might ship with a PCI card installed, depending upon product requirements.
2	Slot 2 PCIe2 x16 (16, 8, 4, 2, 1), 75W +EXT 75W* * <b>Note:</b> Servers might ship with a PCI card installed, depending upon product requirements.
3	Power supply bay 1 (populated)
4	Power supply bay 2
5	iLO 3 connector
6	Serial connector
7	Video connector
8	NIC 4 connector

*Table continues...*

No.	Description
9	NIC 3 connector
10	NIC 2 connector
11	NIC 1 connector
12	USB connectors (2)

\*This expansion slot provides 75 W of power to an adapter, with an additional 75 W of power supplied by external power.

## Installing the server in the rack


This installation checklist contains the principle steps that are necessary to install the server in the rack. Each task refers to an existing HP document and the topic title(s) that contains the step-by-step procedures. Where applicable, additional information and clarifications appear in the *Avaya recommendation* column. Perform each task in the order specified.

### \* Note:

Although not used frequently, Avaya customers are required to have a monitor, keyboard, and mouse available for use by servicing technicians.

No.	Task	Reference	Avaya recommendation	✓
1	Observe safety warnings	ISI UG: <i>Rack warnings</i>		
2	Examine contents of shipping container (Avaya provided equipment)	UG: <i>Contents of the server shipping carton</i>	Ensure that the 6-digit material code on the order matches the 6-digit material code on the shipping container.	
3	Verify that the rack is installed according to the manufacturer's instructions and in accordance with all local codes and laws			
4	Examine installation environment (customer provided equipment)	UG: <i>Optimum environment</i>		
5	Verify that the rack is grounded in accordance with local electrical code.	UG: <i>Electrical grounding requirements</i>		
6	Remove the cabinet doors, if necessary.			

Table continues...

No.	Task	Reference	Avaya recommendation	✓
7	Determine and plan the vertical spacing of the servers in the frame.		Note that air flows into the front of the server and out the air vents located on the top surface of the server chassis. A 1U spacing is sufficient.	
8	Attach the rails to the rack.		<p>The rails included with the server will accommodate most square-hole racks. If these rails do not fit the rack, the customer must provide rails or a shelf for rack installation. Also, the rails included with the server <b>might not</b> work with round-hole racks, in which case the customer can obtain rails and/or a shelf from any distributor, for example <a href="http://www.racksolutions.com/">http://www.racksolutions.com/</a>. The customer-provided rails and rack must be on site prior to the first day of installation.</p> <p> <b>Note:</b> The customer is responsible for any rack screws.</p>	
9	Attach the server to the rack.	UG: <i>Installing the server into the rack</i>		
10	(Optional) Install the cable management arm.			
11	Connect to the network.			
12	Connect the power cord(s).	SP: <i>Connecting the power cord to the power supply</i> UG: <i>Powering up and configuring the server</i>		
13	Power up the server.	UG: <i>Powering up and configuring the server</i>		

---

# Installing a 10 Gb network-interface card

## Before you begin

- Take an inventory of the network-interface cards on site.
- Ensure connectivity.
- Always follow safe electrostatic discharge (ESD) practices.

## About this task

Use this procedure to install a 10 Gb network-interface card in an HP DL360 G7 server.

### Note:

- Install network-interface cards before mounting and cabling.
- You must install the 10 Gb network-interface card in PCIe slot #2 of the server.

## Procedure

1. Power down the server.
  - a. Back up the AE Services database.
  - b. Shut down the operating system as directed by the operating system documentation.
  - c. If the server is installed in a rack, press the UID LED button on the front panel.

Blue LEDs illuminate on the front and rear panels of the server.
  - d. Press the Power On/Standby button to place the server in standby mode.

When the server activates standby power mode, the system power LED changes to amber.
  - e. If the server is installed in a rack, locate the server by identifying the illuminated rear UID LED button.
  - f. Disconnect the power cords.
2. Remove the server from the rack.
  - a. Disconnect all peripheral cables and power cords.
  - b. Loosen the front panel thumbscrews.
  - c. Extend the server on the rack rails until the server rail-release latches engage.

### Warning:

To reduce the risk of personal injury or equipment damage, be sure that the rack is adequately stabilized before extending a component from the rack.

### Warning:

To reduce the risk of personal injury or equipment damage, be careful when pressing the server rail-release latches and sliding the server into the rack. The sliding rails could pinch your fingers.

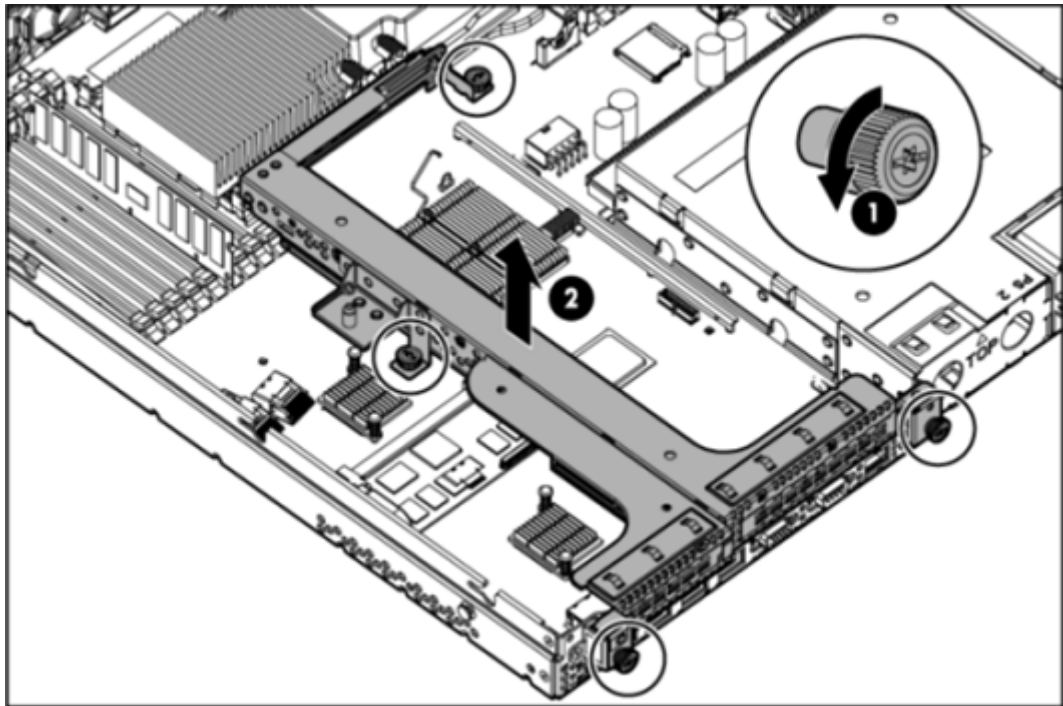
- d. Remove the server from the rack.

- e. Place the server on a sturdy, level surface.

**⚠ Warning:**


To prevent damaging the system, follow safe electrostatic discharge (ESD) practices.

3. Remove the access panel.
  - a. Open the hood latch. If the hood latch is locked, use a T-15 Torx screwdriver to unlock the latch.
  - b. Slide the access panel to the rear of the chassis.
  - c. Remove the access panel from the server.
4. Remove the PCIe riser board assembly.
  - a. Disconnect external cables connected to any existing expansion cards.
  - b. Loosen the four PCI riser board assembly thumbscrews. (See **1** in the following figure.) Use a T-15 Torx screwdriver, if needed.



- c. Lift the assembly out of the server. (See **2** in the previous figure.)
5. Remove the the PCIe slot filler panel from slot #2 (the full-height slot), if installed.
  - a. Remove the Torx screw, and set the screw aside.
  - b. Push the filler panel out of the slot.
6. Install the 10 Gb network-interface card in slot #2 (the full-height slot).
  - a. Slide the faceplate of the 10 Gb network-interface card in the slot of the PCIe riser to ensure the PCIe slot is aligned correctly.



- b. Push the 10 Gb network-interface card into the PCI socket.
  - c. Secure the faceplate of the 10 Gb network-interface card with the Torx screw that you removed from the filler panel in Step 5.
7. Install the PCIe riser board assembly back into the server.
  - a. Align the PCIe riser board assembly using the sockets on the motherboard and the screw holes, and then push the PCIe riser board assembly down to seat it securely on the motherboard.
-  **Note:**

Be sure not to pinch the BBWC battery pack cable.
- b. Tighten the four PCIe riser board assembly thumbscrews. Use a T-15 Torx screwdriver, if needed.
  - c. Reconnect the external cables for any existing expansion cards.
8. Install the access panel.
  - a. Place the access panel on top of the server with the hood latch open. Allow the access panel to extend past the rear of the server approximately 1.25 cm (0.5 in).
  - b. Push down on the hood latch. The access panel slides to a closed position.
  - c. Use a T-15 Torx screwdriver to tighten the security screw on the hood latch.
9. Install the server back into the rack.
  - a. Install the server into the rails.
  - b. Slide the server fully into the rack.
  - c. Tighten the front panel thumbscrews.
  - d. Connect all peripheral cables and power cords.
10. Connect the CAT6A crossover cable to the port on the 10 Gb network-interface card you just installed.
11. Power up the server.
  - a. Connect the power cords.
  - b. Press the Power On/Standby button.

# Chapter 7: Installing the Dell R610 server

The Dell R610 server supports several Avaya software solutions. See the following documents to install and configure the Dell R610 server.

- *Installing the Dell™ PowerEdge™ R610*, document number 03-603793
- *Dell™ PowerEdge™ R610 Systems, Rack Installation*
- *Dell™ PowerEdge™ R610 Systems, Hardware Owner's Manual*
- *Dell™ PowerEdge™ R610 Systems, Cable Management Arm Installation*
- *Dell™ PowerEdge™ R610 Systems, Getting Started with Your System*

These documents are available on the Avaya support web site.

## Accessing the Avaya support web site

To access the Dell R610 server documents on the Avaya support web site, do the following:

1. In the address bar of your browser, type `support.avaya.com`
2. From the menu on the left side of the Welcome to Avaya Support page, select **Documentation > Installation, Migrations, Upgrades & Configurations**.
3. Click the letter **C** in the alphabet listing.
4. Select **Common Servers**.

## Related links

[Specifications for Dell R610 server with H700 RAID controller](#) on page 58

[Installing a 10 Gb network-interface card](#) on page 59

---

## Specifications for Dell R610 server with H700 RAID controller

For new installations of Application Enablement Services on System Platform, the new Dell R610 server with an H700 RAID controller is required. The following table provides the specifications for this server.

Component	Description
Processor	One Intel Xeon E5620 quad core, 2.40 GHz

*Table continues...*

Memory	6 GB RAM (Three 2 GB DIMMs)
Hard Drives	Two 2.5-inch 300 GB 10 K SAS disk drives
RAID Controller	One H700 RAID-1
Drives	DVD read-only drive
Network Interface	Four 100/1000 Ethernet network interface ports Optional: two 10 Gigabit Ethernet network interface ports
Power Supply	One 520W Energy Smart power supply
Dimensions	Height: 43 mm (1.7 inches, 1U ) Depth: 772 mm (30.4 inches) Width: 482 mm (19 inches)
Weight	17.7 kg (39 lb.)

**Related links**

[Installing the Dell R610 server](#) on page 58

---

## Installing a 10 Gb network-interface card

**Before you begin**

- Take an inventory of the network-interface cards on site.
- Ensure connectivity.

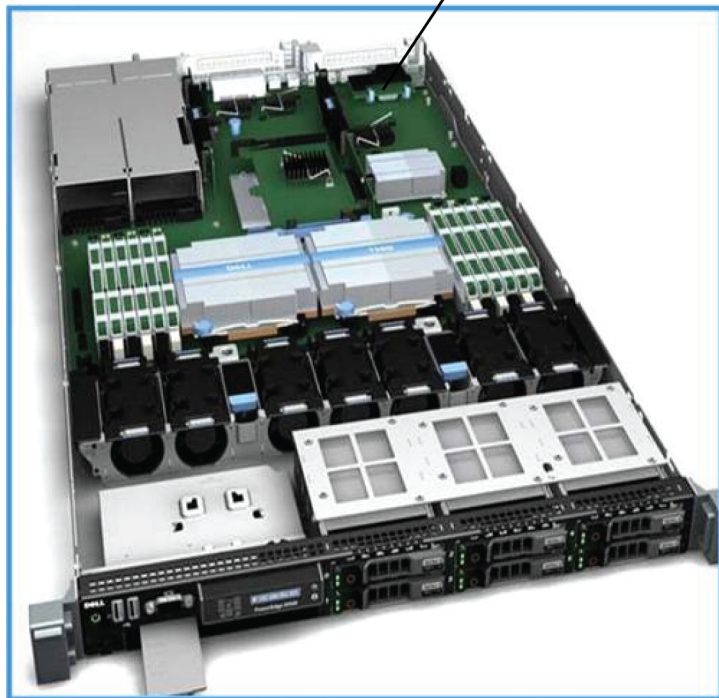
**About this task**

Use this procedure to install a 10 Gb network-interface card in a Dell R610 server.

**\* Note:**

- Install network-interface cards before mounting and cabling.
- You must install the 10 Gb network-interface card in slot 1 of the server. The following figure shows the location of slot 1.

Slot 1

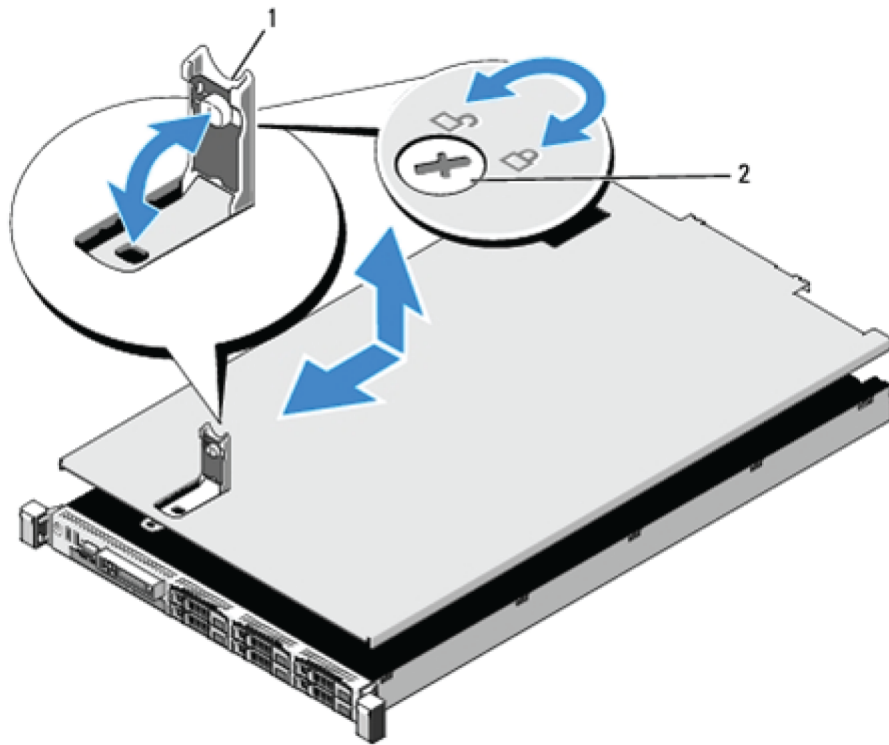


### Procedure

1. Turn off the server, including any attached peripherals, and disconnect the server from the electrical outlet.

2. Open the server:

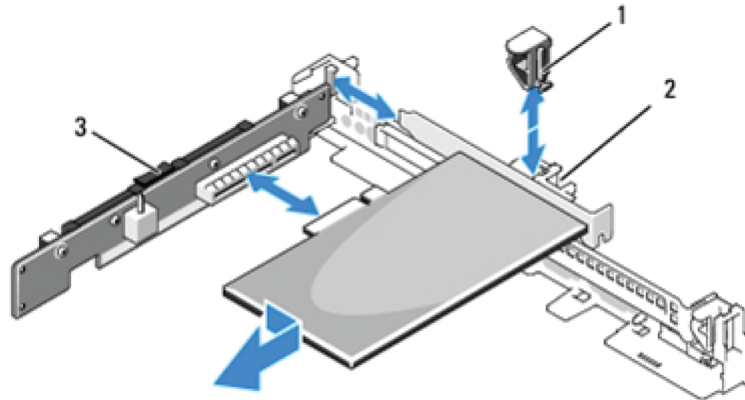
- a. Rotate the latch release lock counter clockwise to the unlocked position. See the following figure.



1 - latch  
2 - latch release lock

- b. Lift up on the latch on top of the server, and carefully lift the cover away from the server.
- c. Grasp the cover on both sides and carefully lift the cover away from the server.

3. Open the expansion-card latch, and remove the filler bracket. See the following figure.



- 1 - expansion-card latch
- 2 - expansion card
- 3 - expansion card riser

4. Install the network interface card into slot 1:
  - a. Holding the card by its edges, position the card so that the card-edge connector aligns with the expansion-card connector on the expansion-card riser.
  - b. Insert the card-edge connector firmly into the expansion-card connector until the card is fully seated.
  - c. Close the expansion-card latch.
5. Close the server:
  - a. Lift up the latch on the cover.
  - b. Place the cover onto the chassis, and offset it slightly towards the back of the server so that the two hooks on the back edge of the cover fit over the corresponding tabs on the back edge of the chassis.
  - c. Slide the cover towards the front of the chassis, and close the latch.
  - d. Rotate the latch release lock in a clockwise direction to secure the cover.
6. Connect the CAT6A crossover cable to the port on the network-interface card you just installed. (If you are looking at the back of the server, this port is located on the left-hand side.)

**\* Note:**

You *must* use the same port on both servers.

7. Connect the server to the electrical outlet.
8. Turn on the server and any attached peripherals.

**Related links**

[Installing the Dell R610 server](#) on page 58

# Chapter 8: Installing System Platform

---

## Installation methods

Use one of the following methods to install System Platform:

- Laptop connected to the services port on the server.
- Video monitor, keyboard, and mouse connected to the appropriate ports on the server.

**\* Note:**

You can complete the installation by using only a keyboard and monitor. If you do not have a mouse, use the Tab key to navigate between fields.

If you use a laptop to install the software, you must have an SSH and Telnet client application such as PuTTY installed on the laptop and Telnet must be enabled to install System Platform. Make sure that you change the network settings on the laptop before connecting to the server. See [Configuring the laptop for direct connection to the server](#) on page 68.

---

## Server requirements

Server hardware platforms must meet all requirements of the Avaya Aura<sup>®</sup> System Platform software, any feature-based configuration options (for example, High Availability), and any more requirements of a specific Avaya Aura<sup>®</sup> solution template.

**\* Note:**

Because each Avaya Aura<sup>®</sup> solution template has different requirements for server resources, configuration, capacity, and performance, see customer documentation specific to the Avaya Aura<sup>®</sup> solution you are deploying in your network.

Avaya requires that you install each server with an uninterruptible power supply (UPS) unit. The UPS power ratings should exceed server peak power requirements under a sustained maximum processing load. (Consult with Avaya Support at <http://support.avaya.com> to ensure a reliable installation.)




## Installation checklist for System Platform

Use this checklist to guide you through installation of System Platform 6.3 and the Services Virtual Machine (VM), and SAL Gateway registration and configuration.

If you are planning to install System Platform 6.3.4 and have already installed System Platform 6.3 on your system, install only the 6.3.4 feature pack. System Platform 6.3.4 is an RPM-based feature pack. See [Feature Pack installation](#) on page 93.

### Important:

If you are installing with High Availability protection, install the same version of System Platform on the active and standby servers.

No.	Task	Notes	✓
1	<p>If you are installing System Platform from a laptop, perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Ensure that a Telnet and Secure Shell application are installed on the laptop. Avaya supports use of the open source Telnet/SSH client application PuTTY.</li> <li>• Configure the IP settings of the laptop for direct connection to the server.</li> </ul> <p>See <a href="#">Configuring the laptop for direct connection to the server</a> on page 68.</p> <ul style="list-style-type: none"> <li>• Disable use of proxy servers in the Web browser on the laptop.</li> </ul> <p>See <a href="#">Disabling proxy servers in Microsoft Internet Explorer</a> on page 69 or <a href="#">Disabling proxy servers in Mozilla Firefox</a> on page 70 .</p>		
2	<p>If you are installing System Platform from a laptop, connect your laptop to the services port with an Ethernet crossover cable.</p>	<p>If you do not have a crossover cable, use an IP hub.</p> <p> <b>Note:</b></p> <p>Some laptop computer Network Interface Cards (NICs) provide an internal crossover option that makes it possible to use a straight-through Ethernet cable for this connection. See the documentation for your laptop computer to determine whether this option is available.</p>	

*Table continues...*

No.	Task	Notes	✓
3	If you are installing System Platform from the server console, connect a USB keyboard, USB mouse, and video monitor to the server.		
4	Turn on the server.		
5	Put the DVD in the DVD drive on the server. See <a href="#">Starting the installation from your laptop</a> on page 70 or <a href="#">Starting the installation from the server console</a> on page 71 depending on your selection of installation method.		
6	If using the server console to install System Platform, enter the <code>vspmediacheck</code> command and press <b>Enter</b> .		
7	If using your laptop to install System Platform, establish a Telnet connection to the server. See <a href="#">Starting the installation from your laptop</a> on page 70.		
8	Select the required keyboard type. See <a href="#">Selecting the type of keyboard</a> on page 72.		
9	Verify the System Platform server hardware. See <a href="#">Verifying the System Platform server hardware</a> on page 73.		
10	Verify that the image on the System Platform DVD is not corrupt. See <a href="#">Verifying the System Platform image on the DVD</a> on page 74.		
11	Configure the network settings for the System Domain (Domain-0). See <a href="#">Configuring network settings for System Domain</a> on page 74.		
12	Configure the network settings for the Console Domain. See <a href="#">Configuring network settings for Console Domain</a> on page 77.		
13	Install the Services Virtual Machine (services_vm). See <a href="#">Installing the Services virtual machine</a> on page 79.	<p><b>!</b> <b>Important:</b></p> <p>When the Services VM Network Configuration window displays at the beginning of the System Platform installation <i>for the standby server</i> in a System</p>	

Table continues...

No.	Task	Notes	✓
		Platform High Availability configuration, clear the <b>Enable Services VM</b> check box to ensure that you install the Services VM in a disabled state. If a failover occurs later during HA system operation, the failover subsystem activates the Services VM on the former standby (now active) server, propagates the current Services VM configuration to that server, and deactivates the Services VM on the former active (now standby) server.	
14	Configure the time zone for the System Platform server. See <a href="#">Configuring the time zone for the System Platform server</a> on page 81.		
15	Configure the date and time and specify an NTP server if using one. See <a href="#">Configuring the date and time for the System Platform server</a> on page 82		
16	Configure the System Platform passwords. See <a href="#">Configuring System Platform passwords</a> on page 82.		
17	Verify that System Platform installed correctly. See <a href="#">Verifying installation of</a> on page 85.		
18	Check for System Platform patches and feature packs at <a href="http://support.avaya.com">http://support.avaya.com</a> . Install any patches or feature packs that are available. See <a href="#">Installing patches</a> on page 96 and <a href="#">Feature Pack installation</a> on page 93.		
19	If your NMS uses SNMP v2c, change the SNMP version that is supported on the Services virtual machine.	By default, the Services VM supports SNMP v3.	
20	Configure the SAL gateway for remote access and alarming. See <a href="#">SAL Gateway</a> on page 123.		

Table continues...

No.	Task	Notes	✓
21	Install the AES template. See <a href="#">Installing template</a> on page 118.	<p><b>! Important:</b></p> <p>If you are running System Platform in any of its High Availability modes, do not install a solution template on the standby server. If you do, you will be unable to start High Availability operations. If you are using a bundled System Platform installation (with a solution template), disable template installation on the standby server. Starting High Availability automatically propagates the solution template from the active node to the standby node.</p>	
22	Generate and download license files for the template that is installed.		
23	Create an authentication file on the Authentication File System (AFS) and install it.		
24	If applicable, configure System Platform High Availability. See <a href="#">Configuring locally redundant High Availability</a> on page 108.		

---

## Connecting your laptop to the server

---

### Configuring the laptop for direct connection to the server

#### About this task

You must manually configure the IP address, subnet mask, and default gateway of the laptop before you connect the laptop to the server.

**\* Note:**

The following procedure is for Microsoft Windows XP, but the steps can vary slightly with other versions of Windows.

#### Procedure

1. Click **Start > Control Panel**.

2. Double-click **Network Connections > Local Area Connection**.
3. In the Local Area Connection Status dialog box, click **Properties**.
4. In the **This connection uses the following items** box, click **Internet Protocol (TCP/IP)**.
5. Click **Properties**.
6. In the Internet Protocol (TCP/IP) Properties dialog box, select **Use the following IP address** on the **General** tab.

 **Caution:**

Do not click the **Alternate Configuration** tab.

7. In the **IP address** field, enter a valid IP address.  
For example: 192.11.13.5
8. In the **Subnet mask** field, enter a valid IP subnet mask.  
For example: 255.255.255.252
9. In the **Default gateway** field, enter the IP address that is assigned to the default gateway.  
For example: 192.11.13.6
10. Click **OK**.

---

## Disabling proxy servers in Microsoft Internet Explorer

### About this task

Before connecting directly to the services port, disable the proxy servers in Microsoft Internet Explorer.

### Procedure

1. Start Microsoft Internet Explorer.
2. Select **Tools > Internet Options**.
3. Click the **Connections** tab.
4. Click **LAN Settings**.
5. Clear the **Use a proxy server for your LAN** option.

 **Tip:**

To re-enable the proxy server, select the **Use a proxy server for your LAN** option again.

6. Click **OK** to close each dialog box.

---

## Disabling proxy servers in Mozilla Firefox

Before connecting directly to the services port, disable the proxy servers in Firefox.

**\* Note:**

This procedure is for Firefox on a Windows-based computer. The steps can vary slightly if you are running Linux or another operating system on your laptop.

### Procedure

1. Start Firefox.
2. Select **Tools > Options**.
3. Select the **Advanced** option.
4. Click the **Network** tab.
5. Click **Settings**.
6. Select the **No proxy** option.

**+ Tip:**

To re-enable the proxy server, select the appropriate option again.

7. Click **OK** to close each dialog box.

---

## Starting the installation

---

### Starting the installation from your laptop

#### Before you begin

- A Telnet/SSH application, such as PuTTY, is installed on your laptop.
- IP settings of the laptop are configured for direct connection to the server.
- Use of proxy servers is disabled.

#### Procedure

1. Connect your laptop to the services port with an Ethernet crossover cable.

If you do not have a crossover cable, use an IP hub.

**\* Note:**

Some laptop computer Network Interface Cards (NICs) provide an internal crossover option that makes it possible to use a straight-through Ethernet cable for this connection.

- See the documentation for your laptop computer to determine whether this option is available.
2. Turn on the server.
  3. Insert the System Platform DVD in the server DVD drive.  
The server starts from the DVD.
  4. Verify that the laptop can ping the service port by performing the following steps:
    - a. Click **Start > Run**.
    - b. Enter `ping -t IP_Address`.  
For example: `ping -t 192.11.13.6`

 **Note:**

Wait for the `ping` command to return several continuous responses before proceeding to the next step.

5. Open a Telnet session by performing the following steps:

 **Important:**

If you use a Telnet client other than PuTTY or forget to set the proper terminal emulation for the PuTTY client, the system might display an incorrect Keyboard Type. This issue has no effect on the installation process.

- a. Open the PuTTY program.
- b. In the **Host Name** field, enter *Host\_Name*.  
For example: `192.11.13.6`
- c. Under **Connection type**, select **Telnet**.
- d. Under **Window** in the left navigation pane, select **Translation**.
- e. Under **Received data assumed to be in which character set**, select **UTF-8** from the list.
- f. Click **Open** to open a PuTTY session.

The system displays the Keyboard Type screen.

### Next steps

Select the required keyboard type. See [Selecting the type of keyboard](#) on page 72.

### Related links

[Connecting to the server through the services port](#) on page 87

---

## Starting the installation from the server console

## Before you begin

Connect a USB keyboard, USB mouse, and video monitor to the server.

### Procedure

1. Turn on the server.
2. Insert the System Platform DVD in the server DVD drive.  
The server boots up from the System Platform DVD and displays the Avaya screen.
3. Within 30 seconds of the system displaying the Avaya screen, type **vspmediacheck** at the boot prompt on the Avaya screen, and press **Enter**.

The **vspmediacheck** command verifies that the image on the System Platform DVD is not corrupt.

#### Important:

If you do not press **Enter** or type **vspmediacheck** within 30 seconds of the system displaying the Avaya screen, the system disables installation through the server console and enables installation through the services port. The system then displays the Waiting for Telnet connection screen, and then you can connect to the server through Telnet. To install through the server console at this point, reset the server to restart the installation.

The system displays the Keyboard Type screen.

### Next steps

Select the required keyboard type. See [Selecting the type of keyboard](#) on page 72.

---

## Selecting the type of keyboard

### Procedure

1. On the Keyboard Type screen, select the type of keyboard that you have.  
The supported keyboard types are sg-latin1, sk-qwerty, slovene, sv-latin1, trq, ua-utf, uk, and us.

2. Use the `Tab` key to highlight **OK** and press **Enter**.

The system displays one of the following screens:

- The system displays the CD Found screen if you are installing System Platform from a laptop, or if you are installing System Platform from the server console and entered the **vspmediacheck** command at the boot prompt on the Avaya screen.

See [Verifying the System Platform image on the DVD](#) on page 74.

- The system displays the System Domain Network Configuration screen if you are installing System Platform from the server console and did not enter the **vspmediacheck**



command at the boot prompt on the Avaya screen. See [Configuring network settings for System Domain \(Domain-0\)](#) on page 74.

### Next steps

- Verify that the System Platform image copied correctly to the DVD. See [Verifying the System Platform image on the DVD](#) on page 74.

OR

- Configure the network settings for System Domain (Domain-0). See [Configuring network settings for System Domain \(Domain-0\)](#) on page 74

---

## Verifying the System Platform server hardware

### Before you begin

- You are performing a new installation of the System Platform software.
- You have completed the task, [Selecting the type of keyboard](#) on page 72

### About this task

After [Selecting the type of keyboard](#) on page 72, the System Platform installer automatically performs a hardware check of the server platform. Since the servers supported by Avaya must meet all prerequisites for the System Platform, any platform options, and a specific solution template, the server hardware check normally passes. In this case, the System Platform installation continues transparently to the next phase, [Verifying the System Platform image on the DVD](#) on page 74. However, in the rare circumstance when the hardware check halts the System Platform installation, one or both of the following messages appear. (In the following examples, the first number represents what hardware resources the system nominally requires, and the second number represents what hardware resources the server actually has available for the system.)

The installation is going to abort due to the following reasons:

- The expected minimum size of hard disk is 80 GB, but the actual number of hard disk is 40 GB.
- The expected number of hard disk is 2, but the actual number of hard disk is 1.

Or:

The installer has detected the following problems:

- The expected number of CPU(s) is 2, but the actual number of CPU(s) is 1.

Do you still want to continue the installation?

In either case, capture the exact details of the error message and contact your Avaya technical support representative for further instructions.

### Note:

For any instance of the latter message, do not continue with the System Platform installation.

## Next steps

If the server hardware check passed, continue with [Verifying the System Platform image on the DVD](#) on page 74

---

# Verifying the System Platform image on the DVD

## About this task

Use this procedure to verify that the System Platform image copied correctly to the DVD.

The system displays the CD Found screen if you are installing System Platform from a laptop, or if you are installing System Platform from the server console and entered the `vspmediacheck` command at the boot prompt on the Avaya screen.

## Procedure

On the CD Found screen, perform one of the following actions:

- To test the DVD, use the `Tab` key to select **OK**.
- To skip the test and begin the installation immediately, select **Skip**.

If you choose to test the DVD, the system displays another screen with a progress bar and the percentage of completion. After the test is complete, the system displays whether the image passed the test.

### Note:

If the DVD you are using becomes corrupt, you must write a new DVD with the System Platform image. Before using the new DVD, ensure that you restart the server.

The system displays the System Domain Network Configuration screen.

## Next steps

Configure the network settings for System Domain (Domain-0). See [Configuring network settings for System Domain \(Domain-0\)](#) on page 74.

## Related links

[Writing the ISO image to DVD or CD](#) on page 38

---

# Configuring network settings for System Domain

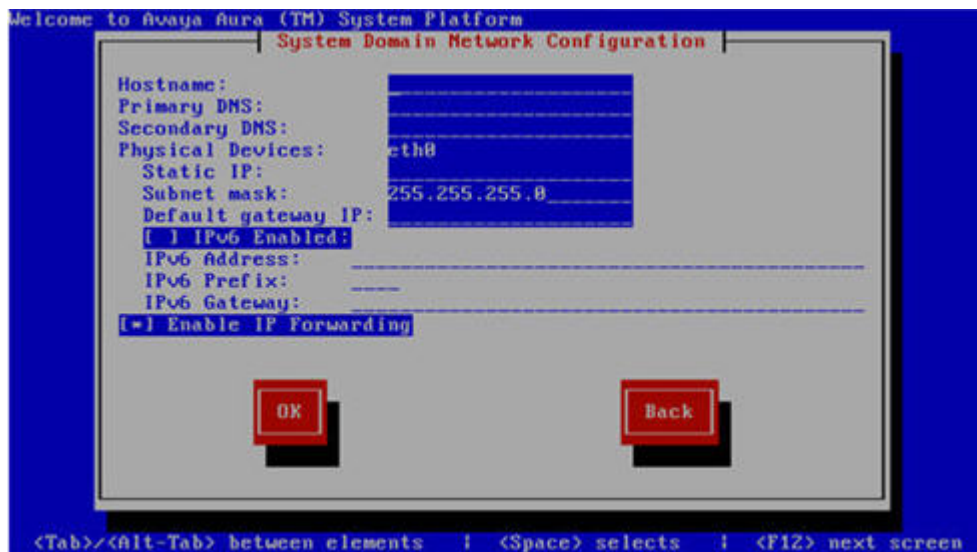
## Procedure

1. On the System Domain Network Configuration screen, complete the following fields:
  - **Hostname**

Depending on requirements of your solution template, you might need to enter the host name for System Domain as a fully qualified domain name (FQDN), for example, `SPDom0.mydomainname.com`. Otherwise, just enter the IP address for System Domain, or enter the hostname for System Domain in non-FQDN format. When using a Domain Name System (DNS) server in your network, the System Domain hostname must be FQDN format.

- **Primary DNS**
- (Optional) **Secondary DNS**

For descriptions of the fields on this page, see [System Domain Network Configuration field descriptions](#) on page 76.



2. Perform the following steps to configure the interface that is connected to the customer network:
  - a. Use the `Tab` key to highlight the **Physical Devices** field.
  - b. Complete the **Static IP** field.
  - c. Modify the subnet mask if necessary. The server displays a default value of `255.255.255.0`.
3. Complete the **Default gateway IP** field.
4. Use the `Tab` key to highlight the **IPv6 Enabled** field. Press the `Spacebar` to either enable or disable entering IP addresses in IPv6 format.
5. If you have enabled IPv6, fill in the following fields:
  - **IPv6 Address**
  - **IPv6 Prefix**
  - **IPv6 Gateway**

- Use the `Tab` key to highlight the **Enable IP Forwarding** field. Press the Space bar to either enable or disable the IP forwarding as desired.

**\* Note:**

IP forwarding is enabled by default and is denoted by an asterisk (\* character).

- Use the `Tab` key to highlight **OK** and press **Enter** to accept the configuration.
- If IP forwarding is enabled, a confirmation message displays. Use the `Tab` key to highlight **OK** and press **Enter**.

The system displays the System Platform Console Domain Network Configuration screen.

### Next steps

Configure network settings for Console Domain. See [Configuring network settings for Console Domain](#) on page 77.

## System Domain Network Configuration field descriptions

Name	Description
<b>Hostname</b>	Depending on requirements of your solution template, you might need to enter the host name for System Domain as a fully qualified domain name (FQDN), for example, <code>SPDom0.mydomainname.com</code> . Otherwise, just enter the IP address for System Domain, or enter the hostname for System Domain in non-FQDN format. When using a Domain Name System (DNS) server in your network, the System Domain hostname must be FQDN format.
<b>Primary DNS</b>	The primary Domain Name System (DNS) server address.
<b>Secondary DNS</b>	(Optional) The secondary DNS server address.
<b>Physical Devices</b>	This field displays the physical Ethernet interface (NIC) that connects to the customer network. You must configure this interface for IP.  The specific Ethernet interface number depends on the server model being used.
<b>Static IP</b>	The static IP address for the Ethernet interface that connects to the customer network.
<b>Subnet Mask</b>	The subnet mask for the Ethernet interface that connects to the customer network.
<b>Default gateway IP</b>	The default gateway IP address.

*Table continues...*

Name	Description
	This default gateway IP address will be used for all the virtual machines if you do not specify gateway IP addresses for them.
<b>IPv6 Enabled</b>	The indicator to show whether the IP addresses required by System Platform must be IPv6-compliant.
<b>IPv6 Address</b>	The IPv6-compliant IP address of System Domain.
<b>IPv6 Prefix</b>	The IPv6 prefix for <b>IPv6 Address</b> .
<b>IPv6 Gateway</b>	The IP address of the default gateway for IPv6 traffic.
<b>Enable IP Forwarding</b>	<p>The indicator to show whether IP forwarding is enabled.</p> <p>An asterisk on the left of the field denotes that IP forwarding is enabled.</p> <p>IP forwarding enables access through the services port to virtual machines on System Platform, including System Domain and Console Domain. IP forwarding must be enabled for both SSH and Web Console access.</p>

---

## Configuring network settings for Console Domain

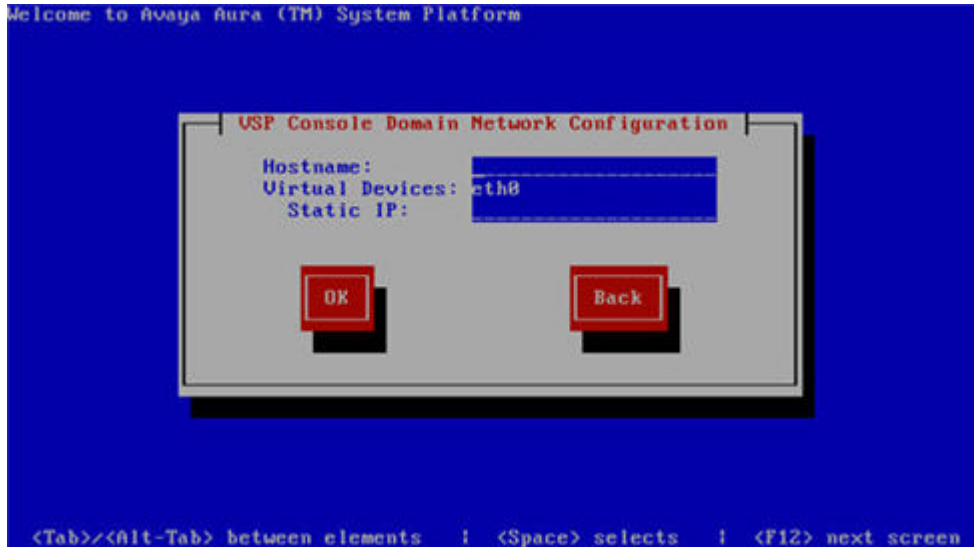
### Procedure

1. On the VSP Console Domain Network Configuration screen, complete the following fields to set up the Console Domain network:

- **Hostname.**

Depending on requirements of your solution template, you may need to enter the host name for Console Domain as a fully qualified domain name (FQDN), for example, `SPCdom.mydomainname.com`. Otherwise, just enter the IP address for Console Domain or enter the hostname for Console Domain in non-FQDN format.

- **Static IP**



2. Select **OK** and press **Enter** to accept the configuration and display the Services VM Network Configuration screen.

**Next steps**

Install and configure the Services Virtual Machine. See [Installing the Services virtual machine](#) on page 79.

## System Platform Console Domain Network Configuration field descriptions

Name	Description
Hostname	Depending on requirements of your solution template, you may need to enter the host name for Console Domain as a fully qualified domain name (FQDN), for example, <code>SPCdom.mydomainname.com</code> . Otherwise, just enter the IP address for Console Domain or enter the hostname for Console Domain in non-FQDN format.
Static IP	The IP address for the Console Domain.  <span style="color: green;">*</span> <b>Note:</b> The Console Domain does not have a physical interface. It has a virtual interface that uses the physical interface in System Domain (Domain-0). Because System Domain acts like a bridge, the IP address that you enter here must be a valid IP address. Further, the

*Table continues...*

Name	Description
	Console Domain must be on the same network as System Domain (Domain-0).
Virtual Devices	The virtual device (port) assigned to the Console Domain (Cdom) virtual machine. Default value (eth0) automatically assigned. No user input necessary.

## Installing the Services virtual machine

Beginning with System Platform release 6.2, the Secure Access Link Gateway (SAL Gateway) no longer runs on the System Platform Console Domain (cdom) virtual machine. Instead, SAL Gateway runs on an independent Services virtual machine (services\_vm domain) on your Avaya Aura<sup>®</sup> solution server. As with the earlier implementation of the SAL Gateway running on the cdom virtual machine, this new configuration supports secure remote access to local server resources, and forwards alarms (SNMP traps) from your local solution server to a remote Network Management System (NMS).

Releases of the Services virtual machine are independent of System Platform releases, so your system can use Services VM 2.0, or you can upgrade your system to use a later version of the Services VM. When you upgrade the Services VM, the process preserves the earlier Master Agent configuration. For information on upgrading the Services VM, see *Implementing and Administering Services-VM on Avaya Aura<sup>®</sup> System Platform*, which is available from Avaya Support at <http://support.avaya.com>. After the upgrade, you configure the Net-SNMP Master Agent in Services VM to forward either SNMPv2c or SNMPv3 traps to your NMS.

For *new System Platform installations* (not an upgrade procedure), you must install the Services virtual machine as part of the platform installation process. An exception to this requirement occurs when implementing a centralized SAL system, with the SAL Gateway running on a separate, dedicated server elsewhere in your network. In this case, you disable Services virtual machine installation during installation of System Platform.

### Important:

When the Services VM Network Configuration window displays at the beginning of the System Platform installation *for the standby server* in a System Platform High Availability configuration, clear the **Enable Services VM** check box to ensure that you install the Services VM in a disabled state. If a failover occurs later during HA system operation, the failover subsystem activates the Services VM on the former standby (now active) server, propagates the current Services VM configuration to that server, and deactivates the Services VM on the former active (now standby) server.

For platform upgrades (not a new System Platform installation), the platform upgrade process manages installation of the new Services VM and SAL Gateway transparently except where an administrator must enter configuration values.

For more information about SAL capabilities, see *Secure Access Link 2.2 SAL Gateway Implementation*, at <http://support.avaya.com>.

### Before you begin

- You have completed the task, “Configuring network settings for Console Domain.”
- If you plan to deploy a standalone SAL Gateway on a server elsewhere in your network, you must download, install, and configure the SAL 2.2 software on that server. For instructions, see the SAL Gateway installation section of *Avaya Secure Access Link 2.2 Gateway Implementation*, available at the Avaya Support website at <http://support.avaya.com>.

### About this task

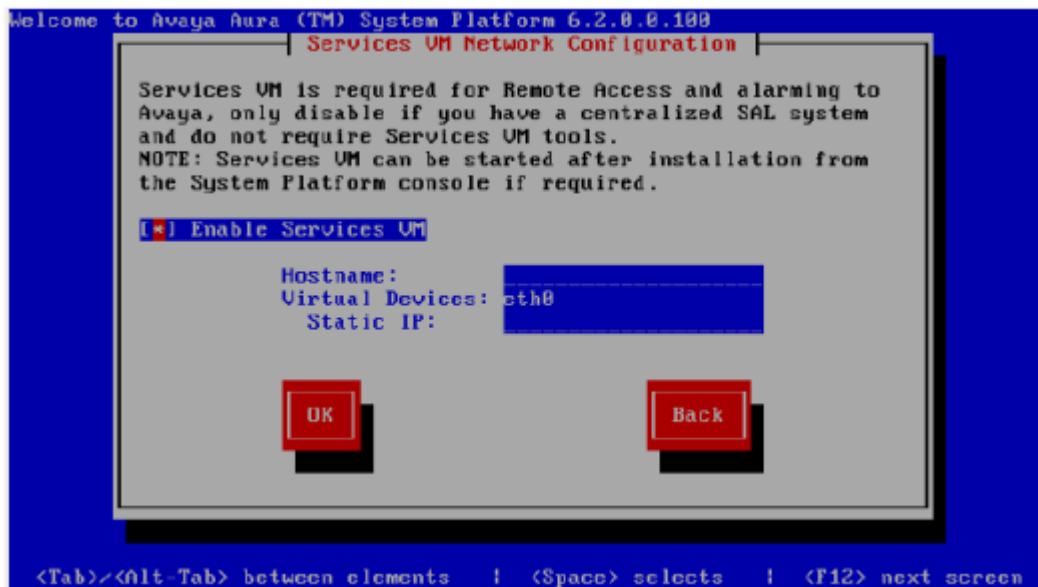
Use this procedure to install the Services VM in an enabled or disabled state, when the Services VM Network Configuration window displays during System Platform installation .

### Procedure

1. If you have a separate server dedicated for centralized SAL support, clear the **Enable Services VM** option in the Services VM Network Configuration window and click **OK**. Otherwise, leave the **Enable services VM** option enabled and begin with step [2](#) on page 80.

If you disable the **Enable Services VM** option, System Platform installation automatically continues to “Configuring System Platform time to synchronize with an NTP server.”

2. In the Services VM Network Configuration window, enter a **Hostname** for the Services virtual machine.



3. Enter a **Static IP** address for the Services virtual machine.

The IP address must be on the same subnet assigned to the Domain 0 (dom0) and Console Domain (cdom) virtual machines.

4. Click **OK**.



The Time Zone Selection screen is displayed.

### Next steps

Configure the time zone for the server.

### Related links

[Services VM Network Configuration field descriptions](#) on page 81

---

## Services VM Network Configuration field descriptions

Name	Description
<b>Enable Services VM</b>	<p>Enables or disables remote access. Also supports local or centralized alarm reporting.</p> <p>Default value: <b>Enabled</b></p> <p>Leave the <b>Enable services VM</b> option enabled (check mark) for remote access and local SAL support, or disabled (no check mark) if you have a separate server dedicated for independent/ centralized remote access and SAL support.</p> <p>In a System Platform High Availability configuration, the active node automatically propagates to the standby node, any change in the setting for this field</p>
<b>Hostname</b>	The name you assign to the Services virtual machine.
<b>Static IP address</b>	The IP address you assign to the Services virtual machine. The address must be on the same subnet assigned to the Domain 0 (dom0) and Console Domain (cdom) virtual machines.
<b>Virtual devices</b>	The virtual device (port) assigned to the Services virtual machine. Default value (eth0) automatically assigned. No user input necessary.

### Related links

[Installing the Services virtual machine](#) on page 79

---

## Configuring the time zone for the System Platform server

### Procedure

1. On the Time Zone Selection screen, select the time zone of the server location.
2. Select **OK** and press **Enter** to accept the configuration and display the Date/Time and NTP setup screen.

### Next steps

Configure date and time for the server.

---

## Configuring the date and time for the System Platform server

### About this task

For solution templates supporting the Network Time Protocol (NTP), the use of an NTP server within your network is the preferred configuration for synchronizing System Platform server time to a standards-based NTP time source. Otherwise, manually configure the System Platform server to a local time setting.

### Procedure

1. Set the current date and time on the Date/Time and NTP setup screen.

 **Note:**

Ensure that the time set here is correct on initial installation. Changing the time in a virtual machine environment causes virtual machines to restart.

2. If you are using an NTP server, perform the following steps on the Date/Time and NTP setup screen:
  - a. Select **Use NTP** if you are using one or more NTP servers.
  - b. In the **NTP server** fields, enter the DNS name or the IP address of your preferred NTP servers.
3. Select **OK** and press **Enter** to accept the configuration and display the Passwords screen.

### Next steps

Configure System Platform passwords.

---

## Configuring System Platform passwords

### Before you begin

Configure the date and time for the System Platform server.

### About this task

 **Important:**

The customer is responsible for the security of all system passwords including the password for the root account. The root password on System Domain must be kept secure. This account has

a high-level of access to the system and steps must be taken to ensure that the password is known only to authorized users. Incorrect use of the root login can result in serious system issues. The root account must be used only in accordance with Avaya documentation and when instructed by Avaya Services.

## Procedure

1. You have the option of keeping the default passwords or changing the passwords.
  - If you want to change the passwords, complete steps 2 through 6 for each of the passwords.
  - If you do not enter new passwords, the defaults are used. Skip to step 7 to accept the default passwords.

### Important:

Avaya recommends entering new passwords instead of using the default passwords. Exercising best practice for password security, make careful note of the passwords that you set for all logins. Customers are responsible for managing their passwords.

The following table shows the default password for each login.

Login	Default password	Capability
root	root01	Advanced administrator
admin	admin01	Advanced administrator
cust	cust01	Normal administrator  The cust login is for audit purposes. It has read-only access to the Web Console, except for changes to its password, and no command line access.
manager (for ldap)	root01	Administrator for the System Platform local Lightweight Directory Access Protocol (LDAP) directory.  System Platform uses a local LDAP directory to store login and password details. Use this login and password to log in to the local LDAP directory. This login does not have permissions to access the System Platform Web Console.

### Note:

The Avaya Services craft login uses Access Security Gateway (ASG) for authentication. If you are using the craft login, you must have an ASG tool to generate a response for

the challenge that is generated by the login page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

2. Click **User Administration > Change Password**.
3. Enter the old password in the **Old Password** field.
4. Type the new password.

Passwords for all users including `root` must adhere to the following rules:

- Include a minimum of 8 characters.
  - Include no more than five repeating characters.
  - Cannot include the last password as part of a new password.
  - Cannot include the user ID as part of the password.
  - Cannot be changed more than once a day.
5. Confirm the new password.
  6. Click **Change Password**.
  7. Select **OK** and press **Enter** to accept the passwords and continue the installation.

### Result

The installation takes approximately 5 minutes. During this time, you can see the Image Installation page with progress bars, followed by the Running page, as the system completes the postinstall scripts. After the installation is completed, the system ejects the DVD and restarts the server. If you are installing from server console, the system displays the Linux login page for System Domain (Domain-0) after the restart.

#### **Important:**

If the DVD does not eject automatically, eject it manually. The system restarts the installation if the DVD is not ejected.

#### **Caution:**

Do not shut down or restart the server during the first boot process of Console Domain. If you shutdown or restart the server during the first boot of Console Domain, System Platform will not function correctly and will have to be reinstalled. To determine if Console Domain has booted, try to go to the Web Console. See [Accessing the Web Console](#) on page 88.

### Next steps

Verify System Platform installation. See [Verifying installation of](#) on page 85.

## Passwords field descriptions

**\* Note:**

Passwords for all users including `root` must adhere to the following rules:

- Include a minimum of 8 characters.
- Include no more than five repeating characters.
- Cannot include the last password as part of a new password.
- Cannot include the user ID as part of the password.
- Cannot be changed more than once a day.

Name	Description
<b>root Password</b>	The password for the root login.
<b>admin Password</b>	The password for the admin login.
<b>cust Password</b>	The password for the cust login.  The cust login is for audit purposes. It has read-only access to the Web Console, except for changes to its password, and no command line access.
<b>Idap Password</b>	The password for the Idap login.  System Platform uses a local LDAP directory to store login and password details. Use this login and password to log in to the local LDAP directory. This login does not have permissions to access the System Platform Web Console.

## Verifying installation of System Platform

### Before you begin

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See [Enabling IP forwarding to access through the services port](#) on page 88.

### About this task

**! Important:**

You cannot get to Console Domain until the system finishes the first boot process.

After installing System Platform, use this procedure to successfully log on to:

- The System Domain (Domain-0) command line as `root`, and run the `check_install` command.
- The Console Domain (Cdom) Web Console as `admin`.

**\* Note:**

The System Platform installation program installs the Console Domain after installing the System Domain. Availability of the login prompt for the System Domain does not necessarily mean that the Console Domain was installed successfully.

The actions in this procedure help verify successful installation of System Platform . It can also identify various issues associated with an unsuccessful installation.

**! Important:**

If you cannot log in to Console Domain as `admin` or access the System Platform Web Console, contact Avaya using any of the technical support options at <http://support.avaya.com>.

**Procedure**

1. Go to the System Domain command line.
2. Enter the command, `check_install`.

If `check_install` finds no issues, the following message displays in the command line interface:

```
Cursory checks passed.
```

If `check_install` command indicates a problem, wait a few minutes and run the command again. If the problem persists, contact Avaya using any of the technical support options at <http://support.avaya.com>.

3. Type `exit` to exit root login.
4. Type `exit` again to exit the System Domain.
5. Go to the System Platform Web Console.
6. Perform the following steps to log in to Console Domain as `admin`:
  - a. Start PuTTY from your computer.
  - b. In the **Host Name (or IP Address)** field, type the IP address of Console Domain.
  - c. In the **Connection type** field, select **SSH**, and then click **Open**.
  - d. When prompted, log in as `admin`, and type the password that you entered for the admin login during System Platform installation.
  - e. Type `exit` to exit Console Domain.

**Related links**

[Enabling IP forwarding to access System Platform through the services port](#) on page 88

---

# Accessing System Platform

---

## Connecting to the server through the services port

### Before you begin

- A Telnet/SSH application, such as PuTTY, is installed on your laptop.
- IP settings of the laptop are configured for direct connection to the server.
- Use of proxy servers is disabled.

### Procedure

1. Connect your laptop to the services port with an Ethernet crossover cable.

If you do not have a crossover cable, use an IP hub.

 **Note:**

Some laptop computer Network Interface Cards (NICs) provide an internal crossover option that makes it possible to use a straight-through Ethernet cable for this connection. See the documentation for your laptop computer to determine whether this option is available.

2. Start a PuTTY session.
3. In the **Host Name (or IP Address)** field, type `192.11.13.6`.

The system assigns the IP address 192.11.13.6 to the services port.

4. For **Connection type**, select **SSH**.
5. In the **Port** field, type `22`.
6. Click **Open**.

 **Note:**

The system displays the PuTTY Security Alert window the first time you connect to the server.

7. Click **Yes** to accept the server's host key and display the PuTTY window.
8. Log in as **admin** or another valid user.
9. When you finish the session, type `exit` and press **Enter** to close PuTTY.

### Related links

[Configuring the laptop for direct connection to the server](#) on page 68

[Disabling proxy servers in Mozilla Firefox](#) on page 70

[Disabling proxy servers in Microsoft Internet Explorer](#) on page 69

---

## Enabling IP forwarding to access System Platform through the services port

### About this task

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

### \* Note:

For security reasons, always disable IP forwarding after finishing your task.

### Procedure

1. To enable IP forwarding:
  - a. Start an SSH session.
  - b. Log in to Domain-0 as administrator.
  - c. In the command line, type `ip_forwarding enable`.
2. To disable IP forwarding:
  - a. Start an SSH session.
  - b. Log in to Domain-0 as administrator.
  - c. In the command line, enter `ip_forwarding disable`.

An alternative to the previous command is `service_port_access disable`.

---

## Browser support for System Platform Web Console

The System Platform Web Console supports the following Web browsers:

- Microsoft Internet Explorer version 8 and version 9.
- Mozilla Firefox version 18 and version 19.

---

## Accessing the System Platform Web Console

### Before you begin

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See [Enabling IP forwarding to access through the services port](#) on page 88.



## About this task

### ! Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

## Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

### \* Note:

This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

The system displays the Virtual Machine List page in the System Platform Web Console.

## Related links

[Enabling IP forwarding to access System Platform through the services port](#) on page 88

---

## Accessing the command line for System Domain

### About this task

If you have physical access to the system, you can log in to the system directly. When you connect to the services port, you are connected to System Domain. You can also use an SSH (Secure Shell) client such as PuTTY to set up a remote connection from your computer. After logging in, the system prompts you with the Linux command prompt.

### \* Note:

Administrators use the command line for System Domain to perform a small number of tasks. Access to the command line for System Domain is reserved for Avaya or Avaya Partners for troubleshooting.

## Procedure

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of System Domain.

**+ Tip:**

You can get the IP address of Domain-0 from the Virtual Machine Management page of the Web Console. In the navigation pane of the Web Console, click **Virtual Machine Management > Manage**.

3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.
5. Once logged in, type the following command to log in as the root user: `su - root`
6. Enter the password for the `root` user.

**+ Tip:**

To get to Console Domain from System Domain, type `xm list`, note the ID for `udom`, and then type `xm console udom-id`. When prompted, log in as `admin`. Then type `su - root` and enter the root password to log in as root.

To exit Console Domain and return to System Domain, press `Control+]`.

7. After performing the necessary tasks, type `exit` to exit root login.
8. Type `exit` again to exit System Domain.

---

## Accessing the command line for Console Domain

### About this task

**! Important:**

You cannot get to Console Domain until the system finishes the first boot process.

**\* Note:**

Administrators go to the command line for Console Domain to perform a small number of tasks. Access to the command line for Console Domain is normally reserved only for Avaya or Avaya Partners for troubleshooting.

### Procedure

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of Console Domain.

**+ Tip:**

The IP address of Console Domain (cdom) is the same as the IP address of the System Platform Web Console.

3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.
5. Once logged in, type the following command to log in as the root user: `su - root`
6. Enter the password for the `root` user.
7. After performing the necessary tasks, type `exit` to exit root login.
8. Type `exit` again to exit Console Domain.

# Chapter 9: Installing Feature Pack software on System Platform

---

## Feature packs

Avaya delivers feature packs in either RPM (patch) or ISO (full upgrade) format. Install or uninstall them as follows:

- RPM patch—From the Patch Management page of the System Platform Web Console.
- ISO image—From the appropriate (System Platform or Avaya Aura® product) installation wizard.

Feature packs have installation requirements that vary, so always see your solution documentation for specific prerequisites and installation instructions.

### Guidelines for RPM-based feature packs

For any RPM-based System Platform feature pack, the following installation guidelines apply:

- If your server is already running the latest version of System Platform available, install the RPM patch containing the feature pack.
- If your server is not running the latest version of System Platform available:
  1. Upgrade to the latest version of System Platform (including service packs) available.
  2. Install the RPM patch containing the feature pack.

### Guidelines for ISO-based feature packs

For any ISO-based System Platform feature pack, only the following guideline applies:

- Use the feature pack ISO image to perform a platform upgrade on the server.

### Feature Pack installation process

If you are planning to install a new feature pack on your solution template, you must first meet System Platform requirements including platform upgrades, service pack installations, and any earlier feature packs if required. For example, with Communication Manager 6.0 running on System Platform 6.0, and with System Platform and Communication Manager each having a new FP1, the solution upgrade sequence is as follows:

1. Upgrade System Platform from version 6.0 to version 6.2.1.
2. Install RPM-based Feature Pack 1 for System Platform 6.2.1. This step brings System Platform to version 6.2.2.
3. Upgrade Communication Manager from version 6.0 to version 6.2.

4. Install Service Pack 4 for Communication Manager 6.2.

### High availability configurations

If you are deploying an Avaya Aura® system in a System Platform High Availability configuration, the same installation or upgrade sequence applies to both the primary and secondary servers in the configuration.

---

## Feature Pack installation

Use the installation method that is appropriate for the feature pack: RPM-based feature packs or ISO-based feature packs.

### RPM-based feature packs

For RPM-based feature packs (for example, Feature Pack 3, System Platform 6.3.4), see [Patch management](#) on page 93.

### ISO-based feature packs

For ISO-based feature packs (for example, Feature Pack 2, System Platform 6.3), perform a platform upgrade.

---

## Managing patches

---

### Patch management

You can install, download, and manage the regular updates and patches for System Platform and the various templates provided by Avaya. Go to <http://support.avaya.com> and see the latest Release Notes for information about the latest patches.

You can install or download the patches from the Avaya Product Licensing and Delivery System (PLDS) website at <http://plds.avaya.com>.

---

### Patch commit and rollback

System Platform **Patch Management** features make it possible for you to install, commit, roll back (undo), or remove patches. The manual rollback feature allows you to test a patch before committing it to the system. The automatic rollback feature makes it possible for the system to autonomously recover from problems resulting from patch installation, or from an administrative lockout after installing a patch remotely over the Secure Access Link.

On the Server Management Patch Detail page, a field labeled **rollbackable** with values of **Yes** or **No** indicates whether you can roll back an installed patch. (You can also **Remove** the patch.)

You can also install, commit, or remove RPM (\*.rpm) patches on either the System Platform or an installed Avaya Aura® solution template.

**\* Note:**

If you have patches to install separately on the System Platform and on an Avaya Aura® solution template, install the System Platform patch(es) first.

### Patch commit and rollback on System Platform

Patch rollback on System Platform applies only to CentOS kernel updates. These are patches applied to the CentOS kernel for System Platform.

**! Important:**

Install kernel updates only during a planned downtime for system maintenance.

The following conditions apply to System Platform patch Commit and Rollback operations:

- If you install a CentOS kernel patch on the System Platform, the platform restarts, also logging you out of the Web Console. If you log on to the Web Console within 4 hours, the system automatically commits the kernel patch at that time. If you installed the patch with communication over the Secure Access Link (SAL), but cannot log on to the Web Console, the system automatically rolls back the kernel patch after 4 hours, so that you can get to the Web Console. After automatic rollback of a kernel patch, System Platform restarts from the kernel version that was installed before you installed the latest patch.
- If you perform one or more operations before committing or rolling back a patch, those operations are implemented and visible on the system. If you roll back a patch, any operations performed before the rollback are not implemented or visible on the system.

If you perform operations locally during a patch installation, but neither **Commit** nor **Rollback** the patch within 4 hours, then System Platform automatically rolls back and restarts using the previous most recent System Platform version.

If you perform one or more operations related to template functionality and must undo those operations after committing or rolling back the patch, use the Web Console to manually roll back the template-related changes. Rolling back a patch does not automatically roll back your template-related changes. Changes that you made before committing a patch are not implemented or visible on the system.

- If you install and commit a CentOS kernel patch on the System Platform, but the Domain-0 virtual machine fails to open because of a kernel panic or other condition of similar severity, then System Platform rolls back automatically to the patch level installed before you installed the new patch.
- If you install any other type of patch on System Platform, you can effectively roll back (undo) effects of the patch by using the Web Console to remove it from the system. (See [Removing patches](#) on page 99.)

### Patch commit and rollback on a Solution Template VM

You can only roll back a solution template patch if it has a **rollbackable** value of `Yes` on the Patch Detail page.

**!** **Important:**

Installing or rolling back a patch on the solution template VM will cause the VM to restart. Install or roll back a patch to the template VM only during planned downtime for system maintenance. Patch rollback usually requires several minutes of system downtime. *Committing* a patch does not cause the template VM to restart.

When you finish installing a rollbackable patch on the solution template Virtual Machine (VM), the Web Console displays the Server Management Patch Detail page, where you can click either **Commit** or **Rollback**, as appropriate.

Rollbackable solution template patches do not have a timer for automatic rollback. You can perform the rollback manually or remove the patch.

You can only install or remove solution template VM patches that have a rollbackable value of `No` on the Patch Detail page.

---

## Downloading patches

### Procedure

1. Click **Server Management > Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
  - **Avaya Downloads (PLDS)**
  - **HTTP**
  - **SP Server**
  - **SP CD/DVD**
  - **SP USB Disk**
  - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.  
If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

### Related links

[Search Local and Remote Patch field descriptions](#) on page 100

## Configuring a proxy

### About this task

If patches are located on a different server (for example, Avaya PLDS or HTTP), and depending on your network setup, configure a proxy address and port.

### Procedure

1. Click **Server Management > Patch Management**.
2. Click **Upload/Download**.
3. On the Search Local and Remote Patch page, click **Configure Proxy**.
4. On the System Configuration page, select **Enabled** for the **Proxy Status** field.
5. Specify the proxy address.
6. Specify the proxy port.
7. Select the appropriate keyboard layout.
8. Enable or disable statistics collection.
9. Click **Save** to save the settings and configure the proxy.

### Related links

[Search Local and Remote Patch field descriptions](#) on page 100

[Downloading patches](#) on page 95

---

## Installing patches

### Before you begin

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

### About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

#### **Note:**

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs



#### 4. Solution template feature packs

##### Procedure

1. Click **Server Management > Patch Management**.
2. Click **Manage**.

The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

##### Next steps

Commit the patch.

##### Related links

[Patch List field descriptions](#) on page 102

[Patch Detail field descriptions](#) on page 102

[Downloading patches](#) on page 95

[Installing System Platform patches on High Availability systems](#) on page 97

---

## Installing System Platform patches on High Availability systems

### About this task

Before downloading any patch, be sure to check its description in the Release Notes. When indicated by the patch description, you must install patches on both the primary and secondary servers independently. The primary server does not automatically replicate patches to the secondary/standby server.

See the separate procedures for stopping, removing, and starting System Platform High Availability as needed during this procedure.

### Procedure

1. Log in to the Web Console of the server chosen to be the preferred node.
2. Click **Server Management > High Availability**.
3. Click **Stop HA** and confirm the displayed warning.
4. If the server restarts after stopping HA, log on to the Web Console of the preferred node and **Remove HA**.
5. Apply patches in the required sequence to the preferred node.
6. Log on to the Web Console of the standby node.
7. Apply the same patches that were applied to the preferred node.

### Related links

[Starting System Platform High Availability](#) on page 113

[Stopping System Platform High Availability](#) on page 114

[Removing the High Availability configuration](#) on page 115

[Installing patches](#) on page 96

[Starting System Platform High Availability](#) on page 113

[Removing the High Availability configuration](#) on page 115

[Stopping System Platform High Availability](#) on page 114

---

## Committing patches

### Before you begin

You have completed the following tasks using the Web Console:

- [Downloading patches](#) on page 95 (finding and downloading the particular patch you must install)
- [Configuring a proxy](#) on page 96 (if the patches are located in a different server)
- [Installing patches](#) on page 96 (for the particular patch you must install)

### About this task

Use the following procedure to commit patches to the Avaya Aura<sup>®</sup> solution template Virtual Machine (VM). After you commit a patch, you cannot roll it back.

#### **Note:**

If you have patches to install separately on the System Platform and on an Avaya Aura<sup>®</sup> solution template, install the System Platform patch(es) first.

### Procedure

1. Click **Server Management > Patch Management**.
2. Click **Manage**.

The Server Management Patch List page displays.

3. Click the patch that you must commit.

The Web Console displays the Server Management Patch Detail page.

4. Click **Commit**.

The Server Management Patch Detail page displays an in-progress message, for example: Patch <patch\_id> is being committed. Please wait.... The Patch Detail page then displays a completion message, for example: Patch <patch\_id> has been successfully committed, or, Failed to commit patch.

---

## Rolling back patches

### About this task

Use this procedure to roll back patches to the solution template Virtual Machine (VM).

 **Note:**

If you have patches to install separately on both System Platform and on the solution template, install the System Platform patches first.

### Procedure

1. Click **Server Management > Patch Management**.
2. Click **Manage**.

The Server Management Patch List page displays.

3. Click the patch that you want to roll back.

The Web Console displays the Server Management Patch Detail page.

4. Click **Rollback**.

The Server Management Patch Detail page displays an in-progress message, for example: Patch <patch\_id> is being rolled back. Please wait.... The Patch Detail page then displays a completion message, for example: Patch <patch\_id> has been successfully rolled back, or, Failed to roll back patch.

---

## Removing patches

### About this task

Use this procedure to uninstall a patch from either System Platform or the template. This procedure uninstalls, but does not delete, the patch file from the system. The patch is available for reinstallation.

When you remove a patch, the system reverts to a completely unpatched state, and you must reinstall previous patches as required.

Remove any uninstalled patches using the remove button, unless you want to reinstall the patch in the future. Removing patches that are no longer required will speed the patch management page display time. A patch can be redownloaded to the system.

### Procedure

1. Click **Server Management > Patch Management** .
2. Click **Manage**.

The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch that you must remove.

- On the Patch Detail page, click **Remove** if you are removing a template patch.

**+ Tip:**

You can clean up the hard disk of your system by removing a patch installation file that is not installed.

**Related links**

[Patch List field descriptions](#) on page 102

[Patch Detail field descriptions](#) on page 102

## Search Local and Remote Patch field descriptions

Use the Search Local and Remote Patch page to search for available patches and to upload or download a patch.

Name	Description
<b>Supported Patch File Extensions</b>	The patch that you are installing must match one of the extensions in this list: *.tar.gz, *.tar.bz, *.gz, *.bz, *.zip, *.tar, *.jar, *.rpm, *.patch.
<b>Choose Media</b>	<p>Displays the available location options for searching a patch. Options are:</p> <ul style="list-style-type: none"> <li>• <b>Avaya Downloads (PLDS):</b> The template files are in the Avaya Product Licensing and Delivery System (PLDS) website. You must enter an Avaya SSO login and password. The list contains all your company's entitled templates. Each line in the list begins with the <code>sold-to</code> number to allow you to select the appropriate template for the site where you are installing. Hold the mouse pointer over the selection to view more information about the <code>sold-to</code> number.</li> <li>• <b>HTTP:</b> A different server stores the files. You must specify the Patch URL for the server.</li> <li>• <b>SP Server:</b> Files are located in the <code>vsp-template</code> file system in the System Platform server. You must specify the Patch URL for the server.</li> </ul> <p><b>+ Tip:</b></p> <p>To move files from your laptop to the System Platform Server, some errors can occur because System Domain (Domain-0) and Console Domain support only SCP, but most laptops do not come with SCP support. You can download the following two programs to</p>

*Table continues...*

Name	Description
	<p>enable SCP (Search the Internet for detailed procedures to download them):</p> <ul style="list-style-type: none"> <li>- Pscp.exe</li> <li>- WinSCP</li> </ul> <ul style="list-style-type: none"> <li>• <b>SP CD/DVD:</b> Files are located in a System Platform CD or DVD.</li> <li>• <b>SP USB Device:</b> Files are located in a USB flash drive. This option is: <ul style="list-style-type: none"> <li>- supported for RPM patch upgrades not exceeding the storage capacity of the flash drive.</li> <li>- not supported for full-platform (ISO) upgrades to System Platform 6.2 or later.</li> </ul> </li> <li>• <b>Local File System:</b> Files are located in a local computer.</li> </ul>
<b>Patch URL</b>	<p>Active only when you select <b>HTTP</b> or <b>SP Server</b> as the media location.</p> <p>URL of the server where the patch files are located.</p>

### Button descriptions

Button	Description
<b>Search</b>	Searches for the available patches in the media location you specify.
<b>Configure Proxy</b>	<p>Active only when you select <b>HTTP</b> as the media location option.</p> <p>Opens the System Configuration page and lets you configure a proxy based on your specifications.</p> <p>If the patches are located in a different server, and depending on your network setup, configure a proxy address and port.</p>
<b>Add</b>	Displays when <b>Local File System</b> is selected and adds a patch file to the local file system.
<b>Upload</b>	Displays when <b>Local File System</b> is selected and uploads a patch file from the local file system.
<b>Download</b>	Downloads a patch file.

### Related links

[Downloading patches](#) on page 95

---

## Patch List field descriptions

The Patch List page displays:

- Patches you can install or remove on the System Platform server.
- In three separate panels, the fields associated with System Platform patches, services\_vm patches, and Solution Template patches.

### Components with patches

Name	Description
System Platform	List of patches available for System Platform.
services_vm	List of patches available for the Services Virtual Machine.
Templates	List of patches available for a specific solution template.

### Fields per patch

Name	Description
Patch ID	File name of a patch. Click the name to view more details about the patch.
Description	Information about the patch, for example, if the patch is available for System Platform, the description is shown as <i>SP patch</i> .
Status	Status of a patch.  Possible values of <b>Status</b> are <b>Installed</b> , <b>Not Installed</b> , <b>Active</b> , and <b>Not Activated</b> .
Service Affecting	Shows if installing the patch causes the associated virtual machine to restart.

### Button descriptions

Button	Description
Refresh	Refreshes the patch list.

### Related links

[Removing patches](#) on page 99

[Installing patches](#) on page 96

---

## Patch Detail field descriptions

The Patch Detail page provides detailed information about a patch. Use this page to view details of a patch or to install, commit, roll back, or remove a patch.

Name	Description
<b>ID</b>	File name of the patch file.
<b>Version</b>	Version of the patch file.
<b>Product ID</b>	Name of the virtual machine.
<b>Description</b>	Virtual machine name for which the patch is applicable.
<b>Detail</b>	Virtual machine name for which the patch is applicable. For example, Console Domain (cdom patch).
<b>Dependency</b>	Shows if the patch file has any dependency on any other file.
<b>Applicable for</b>	Shows the software load for which the patch is applicable.
<b>Service affecting when</b>	Shows the action (if any) that causes the selected patch to restart the System Platform Web Console.
<b>Restart this console when</b>	Shows the conditions or circumstances when the System Platform Web Console must be restarted.
<b>Disable sanity when</b>	Shows at what stage the sanity is set to disable.
<b>Status</b>	Shows if the patch is available for installing or already installed.
<b>Patch File</b>	Shows the URL for the patch file.
<b>Publication Date</b>	Shows the publication date of the patch file.
<b>License Required</b>	This field is applicable only for products that support Service Pack Guardian. Communication Manager is the only product that supports this feature.
<b>Rollbackable</b>	Shows whether you can roll back the patch after installation.

### Button descriptions

Button	Description
<b>Refresh</b>	Refreshes the Patch Details page.
<b>Patch List</b>	Opens the Patch List page, that displays the list of patches.
<b>Install</b>	Installs the respective patch.
<b>Rollback</b>	Rolls back the installed patch if the <b>Rollbackable</b> field value is <i>Yes</i> .
<b>Remove</b>	Uninstalls the respective patch.  This button uninstalls, but does not delete, the patch file from the system. The patch is available for reinstallation.

*Table continues...*

Button	Description
	When you remove a patch, the system reverts to a completely unpatched state, and you must reinstall previous patches as required.
<b>Remove Patch File</b>	Deletes the respective patch file from the system. After the patch file is deleted, it is unavailable for reinstallation. To reinstall the patch, you must download the patch again.

**Related links**

[Removing patches](#) on page 99

[Installing patches](#) on page 96



# Chapter 10: Configuring System Platform High Availability

---

## About System Platform High Availability

System Platform High Availability is an optional feature that provides different levels of services continuity. This feature is available with some, but not all, Avaya Aura® solution templates. For example, the Communication Manager template does not currently use the System Platform High Availability feature.

For more information about System Platform High Availability, see administration topics relevant to this functionality in your Avaya Aura® solution documentation.

---

## Template administration during High Availability operation

System Platform does not support installation, upgrade, or deletion of templates while running the system in an active High Availability mode. The web console displays a warning message on template pages, and you cannot perform any actions associated with them.

To install, upgrade, or delete a template, you must first stop High Availability and remove the configuration. Templates must be installed, upgraded, or deleted only on the preferred node in a High Availability configuration.

You must perform all template operations while logged on to the preferred node. When you finish template configuration, you can restart High Availability operation in the mode that you want

### Important:

If you have a System Platform High Availability configuration, do not install a template on the standby node. If you do, you will be unable to start High Availability operation. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability operation.

---

## Prerequisites for High Availability configuration

---

### Introduction to High Availability prerequisites

For Avaya Aura® solutions that support System Platform High Availability operation, configuration prerequisites exist in two areas:

- Common prerequisites for all System Platform High Availability configurations
- Prerequisites for a specific type of System Platform High Availability (for example, locally redundant HA)

System Platform supports Locally Redundant High Availability configurations

You must satisfy all of the Common and HA-specific prerequisites before attempting to configure System Platform High Availability.

Note also that some solution templates support alternatives to System Platform High Availability. To determine specific support for either System Platform High Availability or an alternative template-driven implementation of solution High Availability, refer to feature support information in your Avaya Aura® solution documentation.

---

### Common prerequisites for all High Availability modes

If your Avaya Aura® solution template supports any mode of System Platform High Availability operation, you must satisfy all applicable prerequisites identified in this topic.

#### Servers

- Two servers with the same hardware configuration. At a minimum, the servers must have identical memory, number of processors, total disk space or free disk space as determined by template requirements.
- The servers must have a spare Gigabit network interface to be dedicated exclusively to System Platform High Availability services. The servers must be connected on the same ports on both machines.
- Verify that System Platform and the solution template both support the specific server.

#### Cabling

The System Platform High Availability physical configuration requires an Ethernet CAT5E cable with straight-through wiring for the connection from local server port eth0 to a port on the local default gateway router. This provides each server with connectivity to the public IP network. This connection also carries Ping traffic between each server and the default gateway router.

#### Software

- Verify that the same version of System Platform, including software patch updates, have been installed on the primary and secondary servers.

**\* Note:**

For Avaya Aura solutions deployed in a System Platform High Availability configuration, you must install/apply patches on both the primary and secondary servers independently. The primary server does not automatically replicate System Platform patches to the secondary server.

- Record the cdom user name and password for logon to the primary and secondary System Platform servers when necessary.
- If you have a System Platform High Availability configuration, do not install a template on the standby node. If you do, you will be unable to start High Availability operation. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability operation.

---

## Prerequisites for locally redundant High Availability

If your Avaya Aura® solution template uses System Platform FRHA, or MPHA with LMHA High Availability modes, you must satisfy all common prerequisites for all HA modes. You must also satisfy the prerequisites specifically for Locally Redundant High Availability described in this topic.

### Network Interface Cards (NICs)

- Both servers should have a spare network interface dedicated exclusively to High Availability data replication, as follows:
  - FRHA: 1 Gb/s interface
  - MPHA and LMHA: 10 Gb/s interface

### Cabling

- Both servers must be in close proximity for interconnection by a high-speed Ethernet cable with crossover signal wiring. This cable carries data replication traffic between the primary and secondary servers. It also carries heartbeat messaging between the two servers.

**\* Note:**

The Ethernet specification limit for the length of this cable between the primary and secondary servers is 100 meters. This interconnection must not include a layer-2 switch. The same Ethernet port on each server must be used to create the crossover connection, for example, eth2 to eth2, eth3 to eth3, or eth4 to eth4. The minimum acceptable cable type for this node-to-node crossover connection is Ethernet CAT5E. For installation sites with higher than normal electrical or signal noise in some areas, use Ethernet type CAT5A cabling for the crossover connection. Type CAT6A cable provides the best levels of shielding against crosstalk and external signal interference.

- For FRHA operation, use a type CAT5E Ethernet cable *with crossover wiring* for the high-speed crossover connection between a 1Gb/sec NIC port on the primary server to a 1 Gb/sec NIC port on the secondary server. You must use the same port on both servers, usually eth 2 to eth2. If eth2 is unavailable, you cannot use eth 0 or eth1 for the crossover connection, but you can use other available 1Gb/s Ethernet ports on the two servers.
- For MPHA (and implicitly LMHA operation for standard Cdom and Services virtual machines), use a type CAT6A Ethernet 10 Gb/sec cable *with crossover wiring* for the high-speed

crossover connection between a 10Gb/sec NIC port on the primary server to a 10 Gb/sec NIC port on the secondary server. You must use the same port on both servers, typically eth 2 to eth2. If eth2 is unavailable, you cannot use eth 0 or eth1 for the crossover connection, but use other available 10 Gb/s Ethernet ports on the two servers.

### **Networking for locally redundant High Availability**

- Install both servers on the same IP subnetwork.
- Document IP addresses for the following Ping targets:
  - The IP address of the default gateway router interface local to the primary (preferred) server. (The primary server requires this target to assure connectivity to the public network.)
  - The IP address of the default gateway router interface local to the standby server. (The standby server requires this target to assure connectivity to the public network.)
  - The IP address of any servers (not including System Platform servers) deployed as part of your Avaya Aura<sup>®</sup> solution. Add these servers as optional Ping targets, to help extend connectivity monitoring (using Ping) throughout the solution topology. See the requirements of your specific solution template.
- Ensure that the default gateway replies to ICMP pings from each System Platform node. Use each server's command line to check:

```
ping <default_gateway_IP_address>.
```

Verify the ping responses to each server from the default gateway, each containing a ping response time.

---

## **Configuring System Platform High Availability**

---

### **Configuring locally redundant High Availability**

#### **Before you begin**

You must have a user role of Advanced Administrator to perform this task.

You must complete:

- Common prerequisites for all System Platform High Availability configurations
- Prerequisites for a specific type of System Platform High Availability (for example, locally redundant HA)

#### **About this task**

- Perform this task only on the System Platform server chosen to be the Preferred (primary) Node in the High Availability pair.
- The primary server propagates its configuration to the secondary (standby) server when you start High Availability operation.

- This procedure synchronizes all required configuration settings from the preferred node to the standby node so that the standby node can assume the role of active node if required.
- If you have a System Platform High Availability configuration, do not install a template on the standby node. If you do, you will be unable to start High Availability operation. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability operation.
- During disk synchronization (typically while HA operations are starting up) the High Availability software automatically adjusts the default rate of disk synchronization (typically 100 MB/sec) to the speed of the crossover interface between the two nodes.
- After starting HA, you can log on to the Web Console of the active server.

## Procedure

1. Log in to the Web Console of the server chosen to be the preferred node.

Use the IP address of the server's Cdom virtual machine when logging on to the Web Console.

2. Click **Server Management > High Availability**.

The High Availability page displays the current status of the High Availability configuration.

3. Click **Configure HA**.

### **Note:**

The **Configure HA** button in the Web Console will be disabled whenever the server has no physical or logical interfaces available for High Availability configuration.

4. On the Configure HA page, enter the appropriate information to configure High Availability operation for all template virtual machines.

If your Avaya Aura<sup>®</sup> solution template supports any enhanced System Platform High Availability modes in addition to the default (Fast Reboot High Availability, or FRHA), you can change the mode of High Availability protection on template virtual machines. To verify solution support for any System Platform enhanced High Availability modes, refer to your solution documentation. The Web Console displays different HA configuration fields, according to the HA modes supported by your solution template.

5. Click **Create**.

6. After the system finishes creating the High Availability configuration, click **Start HA** and confirm the displayed warning.

The Start HA button is visible only if High Availability is fully configured but inactive.

7. Click **Server Management > High Availability**.

You can check the status of virtual machines on the High Availability page and ensure that the data replication software is synchronizing virtual machine disk volumes on the active and standby servers.


For virtual machines configured for Fast Reboot High Availability (FRHA), the HA virtual machine status on the High Availability page should display `Connected` and `Synching`

first and then `Running` when the logical disk volumes on the active and standby servers achieve synchronization.

For virtual machines supporting for Machine Preserving High Availability (MPHA), the HA virtual machine status on the High Availability page should display `Ready for Interchange` when both disk and memory on the active and standby servers achieve synchronization.

## High Availability field descriptions

This initial System Platform High Availability page contains mainly read-only fields associated with the current status of the High Availability software. It also contains its primary and secondary server nodes. The page otherwise includes a single button, **Configure HA**.

Button	Description
<b>Configure HA</b>	Invokes the Configure HA page to begin the process of configuring or modifying the configuration of System Platform High Availability   <b>Note:</b> The <b>Configure HA</b> button is disabled when the server has no physical or logical interfaces available for High Availability configuration.

## Configure HA field descriptions

The following tables describe:

- The status of individual virtual machines that are running on the primary server on a System Platform server.
- Fields for configuring System Platform local High Availability operation.
- Buttons to aid you in navigating through High Availability configuration, creating (applying) a High Availability configuration on primary and secondary servers, starting High Availability, manually interchanging High Availability server roles, stopping High Availability, and removing High Availability when needed.

### Virtual Machine Protection Mode configuration

VM Name	VM Description	Protection Mode
cdom	System Platform Console Domain	The mode of System Platform High Availability (SPHA) protection configured on the cdom virtual machine: Fast Reboot (FRHA)

*Table continues...*

VM Name	VM Description	Protection Mode
		If Machine Preserving High Availability (MPHA) is selected for the solution template, the protection mode for all other virtual machines automatically changes to Live Migration.
services_vm	System Platform Services Domain	The mode of System Platform High Availability (SPHA) protection configured on the services_vm virtual machine: Fast Reboot (FRHA)  If Machine Preserving High Availability (MPHA) is selected for the solution template, the protection mode for all other virtual machines automatically changes to Live Migration.
<solution_template_vm>	Avaya Aura <sup>®</sup> solution template	The mode of System Platform High Availability (SPHA) protection configured on a solution template virtual machine. If the VM supports multiple SPHA protection modes, a drop-down menu is available for selecting alternate modes: <ul style="list-style-type: none"> <li>• Fast Reboot (FRHA)</li> <li>• Machine Preserving (MPHA)</li> </ul> If Machine Preserving High Availability (MPHA) is selected for the solution template, the protection mode for all other virtual machines automatically changes to Live Migration.

### Local and remote server Cdom and Dom0 network interface configuration

Name	Description
Local Server (Dom-0) IP Name	Host name of the Domain-0 VM on the preferred active server.
Local Server (Dom-0) IP Address	IP address of the Domain-0 VM on the preferred active server.
Remote cdom IP address	IP Address of the Console Domain VM on the standby node.
Remote cdom user name	User name for accessing the Console Domain VM on the standby node.

*Table continues...*

Name	Description
<b>Remote cdom password</b>	Password for accessing the Console Domain VM on the standby node.
<b>Crossover network interface</b>	Network interface connected to the standby server. Required for internode communication supporting node arbitration, High Availability failover, and High Availability switchover events.

### Ping targets configuration

Name	Description
<b>Ping Target (IP Address/HostName)</b>	IP address or host name of the gateway to the network. You can add multiple ping targets to verify if the System Platform server is connected to network.
<b>Interval (sec)</b>	Interval after which the local System Platform server sends ICMP pings to listed ping targets.
<b>Timeout (sec)</b>	Timeout interval after which no ICMP reply indicates a network failure.

### Buttons

Name	Description
<b>Create</b>	Applies to the primary and secondary nodes in the High Availability configuration entered on the Configure HA page. When the system completes this operation, you can click <b>Start HA</b> .
<b>Start HA</b>	Starts the System Platform High Availability configuration applied to the primary and secondary nodes when you clicked <b>Create</b> . Also restarts a previously running High Availability configuration after you clicked <b>Stop HA</b> to perform certain HA-related administrative tasks.
<b>Stop HA</b>	Stops System Platform High Availability on the primary and secondary nodes. Does not remove the High Availability configuration.
<b>Remove HA</b>	Removes the System Platform High Availability configuration from the primary or secondary nodes.
<b>Add Ping Target</b>	Adds a new ping target.
<b>Edit</b>	Allows you to edit any existing ping target you select in the adjacent check box.
<b>Delete</b>	Allows you to delete any existing ping target you select in the adjacent check box.
<b>Manual Interchange</b>	Manually triggers a graceful switch-over of the current active and standby nodes in the System Platform High Availability configuration.



---

## High Availability start/stop

### High Availability start

You can **Start HA** (start High Availability) operation after committing the feature to the active node configuration. The active node will propagate this configuration to the standby node at commit time. When you start High Availability operation, the console domain and template virtual machines restart on the active and standby nodes.

#### Important:

If you have a System Platform High Availability configuration, do not install a template on the standby node. If you do, you will be unable to start High Availability operation. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability operation.

### High Availability stop

Stopping High Availability operation (using the **Stop HA** button) returns System Platform to standard operation without High Availability protection. (This action does not remove the High Availability configuration from either node.)

#### Important:

Stopping High Availability operations during disk synchronization might corrupt the file system of the standby console domain. Check the status of virtual machine disk synchronization on the High Availability page of the web console.

When High Availability operations halt:

- the two nodes function independently in simplex mode.
- the system no longer propagates VM disk changes (FRHA, LMHA) or VM CPU memory changes (MPHA) from the active node to the standby node.
- you can get to the Web Console on the standby server by using its IP address (provided during configuration of the High Availability feature).

### Related links

[Starting System Platform High Availability](#) on page 113

[Stopping System Platform High Availability](#) on page 114

---

## Starting System Platform High Availability

This procedure synchronizes all required configuration settings from the preferred node to the standby node so that the standby node can assume the role of active node if required.

### About this task

Whether you have completed a new System Platform installation or a System Platform upgrade, your Avaya Aura solution documentation should indicate which of the two High Availability servers will be the preferred node. You must **Start HA** from that node.

**!** **Important:**

If you are performing a platform upgrade, do not start High Availability operation until after you commit the platform upgrade on both the primary and secondary servers.

**\*** **Note:**

- If you are restarting Fast Reboot High Availability (FRHA) operation after performing **Stop HA**, you can restart anytime after FRHA halts.
- If you are restarting Machine Preserving (and implicitly, Live Migration) High Availability (MPHA/LMHA) after performing **Stop HA**, you can restart anytime after MPHA/LMHA halts.

**\*** **Note:**

When starting HA, System Platform removes all bonded interfaces defined earlier on the standby node, but then automatically propagates (duplicates) all bonded interfaces defined on the active node to the standby node. This operation assures that both nodes have the same bonded interface configuration after HA startup.

### Procedure

1. Click **Server Management > High Availability**.
2. Click **Start HA** and confirm the displayed warning.
3. Click **Server Management > High Availability**.

Verify the progress of virtual machine replication on the High Availability page.

### Related links

[High Availability start/stop](#) on page 113

[Upgrading System Platform on both servers](#) on page 177

[Installing System Platform patches on High Availability systems](#) on page 97

[Removing the High Availability configuration](#) on page 115

[Stopping System Platform High Availability](#) on page 114

---

## Stopping System Platform High Availability

### Before you begin

**!** **Important:**

Stopping High Availability operations during disk synchronization could corrupt the file system of the standby console domain. Check the status of virtual machine replication on the High Availability page of the Web Console.

### About this task

This procedure stops High Availability operation and returns System Platform to standard operation without High Availability protection. This procedure does not remove the High Availability configuration from either server.

## Procedure

1. Click **Server Management > High Availability**.
2. Click **Stop HA** and confirm the displayed warning.  
Verify the status of virtual machine replication on the High Availability page.

## Related links

[High Availability start/stop](#) on page 113

[Upgrading System Platform on both servers](#) on page 177

[Installing System Platform patches on High Availability systems](#) on page 97

[Starting System Platform High Availability](#) on page 113

[Removing the High Availability configuration](#) on page 115

---

# Manually switching High Availability server roles

## Before you begin

- All virtual machine disks on the active and standby nodes must be in a synchronized state (contain the same data). Check the **Disk Status** area of the High Availability page.
- MPHA-protected virtual machine memory on the active and standby nodes must be in a synchronized state (contain the same data). Check the **Disk Status** and **Memory Status** areas of the High Availability page.

## About this task

Use this procedure for many administrative, maintenance, or troubleshooting tasks affecting only one server. For example, use this procedure before replacing a hardware module on the active node in an Avaya Aura® system with High Availability protection.

## Procedure

1. From the **Server Management** menu, click **High Availability**.
2. Click **Manual Interchange** the High Availability page.
3. Click **OK** to confirm the warning message.

---

# Removing the High Availability configuration

Use this procedure to permanently remove the High Availability configuration.

## Before you begin

- You have stopped System Platform High Availability.

## About this task

Use this procedure, for example:

- to remove the HA configuration from Avaya Aura® solution servers before a System Platform upgrade. Removing the HA configuration from the primary/active HA server also removes the HA configuration from the standby server automatically.
- to restore Avaya Aura® solution servers in an HA configuration to simplex operation

## Procedure

1. Log on to the Web Console for the primary/active HA server.
2. Click **Server Management > High Availability**.
3. Click **Remove HA** and confirm the displayed warning.

## Related links

[Upgrading System Platform on both servers](#) on page 177

[Installing System Platform patches on High Availability systems](#) on page 97

[Starting System Platform High Availability](#) on page 113

[Stopping System Platform High Availability](#) on page 114

# Chapter 11: Installing Application Enablement Services

---

## Prerequisites for installing the AES template

- Stop High Availability Failover if it is running. You cannot install the AES template if High Availability Failover is running.
- Verify the IP addresses for the *avprivate* bridge do not conflict with any other IP addresses in your network.

Go to the Network Configuration page on the System Platform Web Console (**Server Management > Network Configuration**) to view the addresses that are allocated to *avprivate*. The range of IP addresses starts with the Domain-0 interface on *avprivate*. Console Domain automatically receives the consecutive IP address. Resolve any conflicts by assigning an IP address for Domain-0 on a subnet that you know is not used in your network. Also keep in mind that some templates require additional addresses on the private bridge.

The *avprivate* bridge is an internal, private bridge that allows virtual machines to communicate with each other. This private bridge has no connection to your LAN. During installation, System Platform runs an algorithm to find a set of IP addresses that do not conflict with the addresses configured on the System Domain Network Configuration page. However, it is still possible that the addresses selected conflict with other addresses in your network. Since this private bridge is isolated from your LAN, this address conflict could result in the failure of System Platform or an installed template to route packets correctly.

---

## Configuring a proxy

### About this task

If the template files are located on a different server (for example, Avaya PLDS or HTTP), configure a proxy server address and port.

### Procedure

1. On the Search Local and Remote Template Patch page, click **Configure Proxy**.
2. On the System Configuration page, select **Enabled** for the **Proxy Status** field.
3. Specify the proxy address.
4. Specify the proxy port.

5. Click **Save** to save the settings and configure the proxy.

---

## Installing Application Enablement Services template

### Procedure

1. On a Web browser, type the following URL: `https://ipaddress/webconsole`, where `ipaddress` is the IP address of the Console Domain that you configured during installation of System Platform.

 **Note:**

This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

2. In the User ID box, enter `admin`.
3. Click **Continue**.
4. Enter the password for this account.
5. Click **Log On**.
6. Click **Virtual Machine Management > Templates**.
7. On the Search Local and Remote Template page, select a location from the list in the Install Template From box.

 **Note:**

If the template installation files are located on a different server (for example, Avaya PLDS or HTTP), you may be required to configure a proxy depending on your network.

8. Click **Search** to display a list of template descriptor files (each available template has one template descriptor file).
9. On the Select Template page, click the **AES** template, and then click **Select**.
10. On the Select EPW File page, do one of the following:
  - If you have completed the AE Services Electronic Pre-installation Worksheet (EPW), do the following:
    - a. Click **Browse EPW File**.
    - b. From the Choose File to Upload dialog box, select the EPW file, and click **Open**.
    - c. Click **Upload EPW file**.

The system displays the Template Details page with information on the AES template and its Virtual Appliances.

- If you have not completed the AE Services Electronic Pre-installation Worksheet (EPW), click **Continue without EPW file**.

The system displays the Template Details page with information on the AES template and its Virtual Appliances.

11. Click **Install**.

The Template Installation page shows the status of the installation.

**\* Note:**

Make sure the web browser is set to temporarily allow pop-ups. Once pop-ups are allowed, the Network Settings page appears.

12. On the Network Settings page, enter the following network settings
  - ETH0 IP address of the AES
  - ETH1 IP address of the AES (optional)
  - ETH1 network mask (optional)
  - AES hostname
13. Click **Next Step**.
14. On the Customer Login page, enter the password for the root login in the Password box (optional). *If you do not enter the password, the default password will be used.*
15. Re-enter the root login password in the Re-type password box.
16. Enter the password for the cust login in the Password box (optional). *If you do not enter the password, the default password will be used.*
17. Re-enter the cust login password in the Re-type password box.
18. Click **Next Step**.
19. On the Alarming page, enter the AES Alarm ID and click **Next Step**.
20. On the Summary page, verify the information displayed. If you need to make any changes, click **Previous Step**. When you are finished, click **Next Step**.
21. On the Confirm Installation page, click **Accept**.
22. Click **Install**.

The Template Installation page shows the status of the installation. When the installation is complete, the message "Template Installation Completed Successfully" appears. You can log out.

#### Related links

[Search Local and Remote Template field descriptions](#) on page 119

---

## Search Local and Remote Template field descriptions

Use the Search Local and Remote Template page to select the template to install on System Platform, to upgrade an installed template, or to delete an installed template.

Name	Description
<b>Install Template From</b>	<p>Locations from which you can select a template and install it on System Platform. Available options are as follows:</p> <p><b>Avaya Downloads (PLDS)</b></p> <p>The template files are located in the Avaya Product Licensing and Delivery System (PLDS) website. You must enter an Avaya SSO login and password. The list contains your company's templates. Each line in the list begins with the "sold-to" number to allow you to select the appropriate template for the site where you are installing. Hold the mouse pointer over the selection to view more information about the "sold-to" number.</p> <p><b>HTTP</b></p> <p>The template files are located on an HTTP server. You must enter the template URL information.</p> <p><b>SP Server</b></p> <p>The template files are located in the <code>/vsp-template</code> file system in the Console Domain of the System Platform server.</p> <p><b>SP CD/DVD</b></p> <p>The template files are located on a CD or DVD in the CD/DVD drive on the server.</p> <p><b>SP USB Disk</b></p> <p>The template files are located on a USB flash drive connected to the server.</p>
<b>SSO Login</b>	<p>Active only when you select the <b>Avaya Downloads (PLDS)</b> option to search for a template.</p> <p>Login id for logging on to Single Sign On.</p>
<b>SSO Password</b>	<p>Active only when you select the <b>Avaya Downloads (PLDS)</b> option to search for a template.</p> <p>Password for Single Sign On.</p>

### Search Local and Remote Template button descriptions

Name	Description
<b>Install</b>	Installs the solution template. This button only displays if there is not an installed System Platform template.

*Table continues...*



Name	Description
<b>Configure Proxy</b>	Active only when you select the HTTP option to search for a solution template. Lets you configure a proxy for the HTTP address. Configures a proxy for Secure Access Link(SAL) and alarming functions to gain access to the Internet.
<b>Upgrade</b>	Upgrades the installed solution template from the selected template location option. This button only displays if there is an installed System Platform template.
<b>Delete</b>	Deletes the installed and active template. This button only displays if there is an installed System Platform template.

**Related links**

[Installing Application Enablement Services template](#) on page 118

---

## Reinstalling or replacing the Avaya Access Security Gateway default authentication file

**Before you begin**

The Avaya Access Security Gateway (ASG) default authentication file has been installed.

**About this task**

Use this procedure to reinstall or replace the Avaya Access Security Gateway (ASG) default authentication file. ASG is a challenge and response authentication mechanism. When the ASG is configured, the craft and sroot accounts will receive a challenge when logging into the AE Services server using ssh and the AE Services Management Console.

During the installation process, the ASG default authentication file is installed automatically for the following AE Services 6.3.3 or later offers:

- AE Services Software-Only offer
- AE Services on System Platform offer
- AE Services on VMware offer

**\* Note:**

For the AE Services 6.3.3 or later Bundled offer, the ASG default authentication file is installed after the first successful login to the AE Services Management Console.

**\* Note:**

AE Services on System Platform uses the System Platform Authentication File. Load the Authentication File in both, the Cdom and the AE Services shell.

**\* Note:**

Performing this procedure will remove the current authentication file. If you want to maintain a copy of the current authentication file on the server, you must make a copy of this authentication file before performing this procedure.

**Procedure**

1. Open an ssh session to the AE Services server, and log in as the system administrator.
2. From the command line as the root user, type `loadauth -f -l authFileName` where `authFileName` is the path and file name of the authentication file you want to use. The path and file name for the default authentication file is `/opt/mvap/asg/AESvcs-default-asg-auth.xml`.

3. Press **Enter**.

The system displays `Loading file <name of the authentication file>`.

**\* Note:**

The `loadauth` command removed the account password for the root user. If you want to maintain access via a password for `root`, perform the following command from the command line: `passwd root`.

4. On another machine or in another window, log into the AE Services server as `craft`.

The system will present a challenge.

5. Enter the appropriate ASG response.

You are logged into the system.

6. At the command line, type `su - sroot` and press **Enter** to promote the `craft` account to the `sroot` account.

The system will present a challenge.

7. Enter the appropriate ASG response.

You are logged into the system.

8. Log out of `sroot`.

# Chapter 12: Configuring SAL Gateway on System Platform

---

## SAL Gateway

Secure Access Link (SAL) Gateway provides Avaya support engineers and Avaya Partners with alarming and remote access to the applications on System Platform. System Platform includes an embedded SAL Gateway. SAL Gateway software is also available separately for standalone deployments. The SAL Gateway program on System Platform receives alarms from applications in the solution template and forwards them to Secure Access Core Concentrator Servers at Avaya and applicable Avaya Partners. SAL Gateway can also forward alarms to the customer's Network Management System (NMS) if configured to. The SAL gateway program also polls designated service providers for connection requests.

### Remote Serviceability

System Platform utilizes SAL as Avaya's exclusive method for remote delivery of services. System Platform can be serviced remotely, possibly eliminating a service technician visit to the customer site. System Platform uses the customer's Internet connectivity to help remote support. All communication is outbound from the customer's environment using encapsulated Hypertext Transfer Protocol Secure (HTTPS). SAL requires upload bandwidth (customer to Avaya or Avaya Partner) of at least 90 KB/s with latency no greater than 150 ms (round trip). Business Partners without a SAL Core Concentrator Server must provide their own IP-based connectivity (for example, B2B VPN connection) to deliver remote services.

#### Note:

Avaya Partners and customers must register SAL at least three weeks before activation during System Platform installation. Avaya support will be delayed or not possible if SAL is improperly implemented or not operational. System Platform and SAL do not support modem connections.

### Standalone SAL Gateway

You can choose to use a standalone SAL Gateway instead of the SAL Gateway that is embedded in System Platform. You might prefer a standalone gateway if you have a large network with many Avaya devices. The standalone gateway makes it possible to consolidate alarms from many Avaya devices and send those alarms from one SAL Gateway instead of multiple SAL Gateways sending alarms. See **Secure Access Link** on <http://support.avaya.com> for more information about standalone SAL Gateway.

If you use a standalone SAL Gateway, you must add it as an SNMP trap receiver for System Platform. See [Adding an SNMP trap receiver](#) on page 139. You can also disable the SAL Gateway

that is embedded in System Platform so that it does not send duplicate heart beat messages to Avaya. See [Disabling SAL Gateway](#) on page 139.

## SAL Gateway configuration

The SAL Gateway includes a Web-based user interface that provides status information, logging information, and configuration interfaces. You must configure the SAL Gateway and other devices for alarming and remote access. The devices include System Platform's System Domain (dom 0), Console Domain (cdom), and other products that are in the installed solution template. For example, virtual machines might include Communication Manager, Communication Manager Messaging, Session Manager, and other applications in the template.

To configure SAL, perform these high-level steps:

1. Register the system.

You must submit the Universal Install/SAL Registration Request form to obtain from Avaya the information that you must enter in SAL Gateway.

Avaya assigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway and managed device that is registered. In System Platform, managed devices are the components of System Platform and of the applications in the solution template. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely. The Product ID is in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

2. Configure the SAL Gateway.

The SAL Gateway provides remote access to those devices that are configured for remote access within it. It controls connections to managed elements, new or updated models, and verifies certificates for authentication.

### Note:

On systems using High Availability operation, configure the SAL Gateway only on the primary server. When you enable High Availability operations, SAL Gateway will propagate to the standby server.

### Related links

[Configuration prerequisites](#) on page 124

[Registering the system](#) on page 34

---

## Configuration prerequisites

Before configuring the SAL Gateway, you must start the registration process and receive product registration information from Avaya.

To register a product, download and complete the *SAL Universal Install Form Help Document* form and submit the form to Avaya. The form includes complete instructions.

The SAL registration form is available at <http://support.avaya.com>. In the Help & Policies section, click **More Resources**. The system displays the More Resources page. Click **Avaya Equipment Registration**, and search for *SAL Universal Install Form Help Document*.

**\* Note:**

Submit the registration form three weeks before the planned installation date.

#### Related links

[Registering the system](#) on page 34

[SAL Gateway](#) on page 123

[Registering the system](#) on page 34

---

## Changing the Product ID for System Platform

### Before you begin

You must have registered the system and obtained a Product ID for System Platform from Avaya. The Product ID is in alarms that System Platform sends to alarm receivers. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

### About this task

When you install System Platform, a default Product ID of 1001119999 is set. You must change this default ID to the unique Product ID that Avaya provides.

### Procedure

1. In the navigation pane of the System Platform Web Console, click **Server Management > SNMP Trap Receiver Configuration**.
2. On the SNMP Trap Receiver Configuration page, delete the ID in the **Product ID** field and enter the unique Product ID for System Platform Console Domain.

**\* Note:**

VSPU is the model name for Console Domain.

3. Click **Save**.

---

## System and browser requirements

Browser requirements for accessing the SAL Gateway user interface:

- Microsoft Internet Explorer 7, 8, or 9
- Firefox 3.6 through 19

System requirements:

- A computer with access to the System Platform network.

---

## Starting the SAL Gateway user interface

### Procedure

1. Log in to the System Platform Web Console.
2. In the navigation pane of the System Platform Web Console , click **Server Management > SAL Gateway Management**.
3. On the **Server Management: SAL Gateway Management** page, click **Enable SAL Gateway**.
4. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.
5. When the SAL Gateway displays the Log on page, enter the same user ID and password that you used for the System Platform Web Console.

To configure SAL Gateway, you must log in as `admin` or another user that has an advanced administrator role. Users that have an administrator role can only view configuration of the SAL Gateway.

After you log in, the Managed Element page of the SAL Gateway user interface displays. If the SAL Gateway is running, the system displays two messages at the top of the page:

- `SAL Agent is running`
- `Remote Access Agent is running`

---

## Configuring the SAL Gateway

### About this task

Use this procedure to configure the identity of the SAL Gateway. This information is required for the SAL Gateway to communicate with the Secure Access Concentrator Core Server (SACCS) and Secure Access Concentrator Remote Server (SACRS) at Avaya.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Gateway Configuration**.
2. On the Gateway Configuration page, click **Edit**.
3. On the **Gateway Configuration** (edit) page, complete the following fields:
  - **IP Address**
  - **Solution Element ID**

- **Alarm ID**
- **Alarm Enabled**

For field descriptions, see [Gateway Configuration field descriptions](#) on page 127.

4. (Optional) Complete the following fields if the template supports inventory collection:

- **Inventory Collection**
- **Inventory collection schedule**

5. Click **Apply**.

 **Note:**

The configuration changes do not take effect immediately. The changes take effect after you apply configuration changes on the Apply Configuration Changes page.

6. To cancel your changes, click **Undo Edit**.

The system restores the configuration before you clicked the **Edit** button.

See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at <http://support.avaya.com>.

### Next steps


After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

### Related links

[Gateway Configuration field descriptions](#) on page 127

[Applying configuration changes](#) on page 135

## Gateway Configuration field descriptions

Name	Description
<b>Hostname</b>	<p>A host name for the SAL Gateway.</p> <p> <b>Warning:</b></p> <p>Do not edit this field as the SAL Gateway inherits the same hostname as the CentOS operating system that hosts both the System Platform Web Console and the SAL Gateway.</p>
<b>IP Address</b>	The IP address of the SAL Gateway.

*Table continues...*

Name	Description
	This IP address must be different from the unique IP addresses assigned to either the Cdom or Dom0 virtual machines.
<b>Solution Element ID</b>	<p>The Solution Element ID that uniquely identifies the SAL Gateway. Format is (000) 123-4567.</p> <p>If you have not obtained Solution Element IDs for the system, start the registration process.</p> <p>The system uses the SAL Gateway Solution Element ID to authenticate the SAL Gateway and its devices with the Secure Access Concentrator Remote Server.</p>
<b>Alarm ID</b>	<p>The Product ID (also called Alarm ID) for the SAL Gateway. This ID should start with a 5 and include ten digits.</p> <p>The system uses the value in the this field to uniquely identify the source of Gateway alarms in the Secure Access Concentrator Core Server.</p>
<b>Alarm Enabled</b>	Enables the alarming component of the SAL Gateway. This check box must be selected for the SAL Gateway to send alarms.
<b>Inventory Collection</b>	<p>Enables inventory collection for the SAL Gateway.</p> <p>When this check box is selected, SAL Gateway collects inventory information about the supported managed devices and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel working on tickets and must review the configuration of managed devices. For more information on this feature, see the <i>Secure Access Link Gateway 1.8 Implementation Guide</i>. This document is available at <a href="http://support.avaya.com">http://support.avaya.com</a></p>
<b>Inventory collection schedule</b>	Interval in hours at which the SAL Gateway collects inventory data.

**Related links**

[Configuring the SAL Gateway](#) on page 126

[Registering the system](#) on page 34



## Configuring a proxy server

### About this task

Use the Proxy Server page to configure proxy settings if required for SAL Gateway to communicate with the Secure Access Concentrator Remote Server and the Secure Access Concentrator Core Server.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Proxy**.
2. On the Proxy Server page, complete the following fields:
  - **Use Proxy**
  - **Proxy Type**
  - **Host**
  - **Port**
3. Click **Apply**.
4. (Optional) When you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the proxy server.

See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at <http://support.avaya.com>.

### Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

### Related links

[Proxy Server field descriptions](#) on page 129

[Applying configuration changes](#) on page 135



## Proxy Server field descriptions

The Proxy Server page of the SALGateway user interface provides you the options to view and update the proxy server configuration for SAL Gateway. SAL Gateway uses the proxy configured on this page to establish external connections.

The page displays the following fields:

Name	Description
Use Proxy	Check box to enable the use of a proxy server.

*Table continues...*

Name	Description
<b>Proxy Type</b>	The type of proxy server that is used. Options are: <ul style="list-style-type: none"> <li>• <b>SOCKS 5</b></li> <li>• <b>HTTP</b></li> </ul>
<b>Host</b>	The IP address or the host name of the proxy server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
<b>Port</b>	The port number of the Proxy server.
<b>Login</b>	Login if authentication is required for the HTTP proxy server.   <b>Important:</b> SAL Gateway in System Platform does not support authenticating proxy servers.
<b>Password</b>	Password for login if authentication is required for the HTTP proxy server.   <b>Important:</b> SAL Gateway in System Platform does not support authenticating proxy servers.
<b>Test URL</b>	The HTTP URL used to test the SAL Gateway connectivity through the proxy server. The Gateway uses the proxy server to connect to the URL you provide.

The page displays the following buttons:

Name	Description
<b>Test</b>	Initiates a test of the SAL Gateway connectivity through the proxy server to the URL specified in the <b>Test URL</b> field. You can initiate a test before or after applying the configuration changes.
<b>Edit</b>	Makes the fields on the Proxy Server page available for editing.
<b>Apply</b>	Saves the configuration changes.

**Related links**

[Configuring a proxy server](#) on page 129

# Configuring SAL Gateway communication with a Concentrator Core Server

## About this task

Use the Core Server page of the SAL Gateway user interface to review settings for communication between SAL Gateway and a Secure Access Concentrator Core Server (SACCS) at Avaya Data Center. The SACCS handles alarming and inventory. Do not change the defaults unless you are explicitly instructed to.

## Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Core Server**.

The Core Server page displays.

2. Do not change the defaults on this page.

See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at <http://support.avaya.com>.

3. (Optional) When you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the defined Secure Access Concentrator Core Servers.

See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at <http://support.avaya.com>.

## Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

The system does not connect to the new Secure Access Concentrator Core Server until you restart the SAL Gateway.

## Related links

[Core Server field descriptions](#) on page 131

[Applying configuration changes](#) on page 135

## Core Server field descriptions

Name	Description
Passphrase	Default passphrase is <code>Enterprise-production</code> . Do not change the default unless you are explicitly instructed to do so. This passphrase is used to establish a channel for communication between the

*Table continues...*

Name	Description
	SAL Gateway and the Secure Access Concentrator Core Server.
<b>Primary Core Server</b>	IP Address or the host name of the primary Secure Access Concentrator Core Server.  The default value is <code>secure.alarming.avaya.com</code> .
<b>Port</b>	Port number of the primary Secure Access Concentrator Core Server.  The default value is 443.
<b>Secondary Core Server</b>	This value must match the value in the <b>Primary Core Server</b> field.
<b>Port</b>	This value must match the value in the <b>Port</b> field for the primary server.

**Related links**

[Configuring SAL Gateway communication with a Concentrator Core Server](#) on page 131

---

## Configuring SAL Gateway communication with a Concentrator Remote Server

**About this task**

Use the Remote Server page of the SAL Gateway user interface to review settings for communication between SAL Gateway and a Secure Access Concentrator Remote Server (SACRS) at Avaya Data Center. The SACRS handles remote access, and updates models and configuration. Do not change the defaults unless you are explicitly instructed to.

**Procedure**

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Remote Server**.

The Remote Server page displays.

2. Do not change the defaults on this page unless you are explicitly instructed to.
3. (Optional) When you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the defined Secure Access Concentrator Remote Servers.

See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at <http://support.avaya.com>.

**Next steps**

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and

restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

The system does not connect to the new Secure Access Concentrator Remote Servers until you restart the SAL Gateway.

When you restart the SAL Gateway, the system closes all active connections.

### Related links

[Remote Server field descriptions](#) on page 133

[Applying configuration changes](#) on page 135

---

## Remote Server field descriptions

Name	Description
<b>Primary Remote Server</b>	The IP address or host name of the primary Secure Access Concentrator Remote Server. The default value is <code>s11.sal.avaya.com</code> .
<b>Port</b>	The port number of the primary Secure Access Concentrator Remote Server. The default value is 443.
<b>Secondary Remote Server</b>	This value must match the value in the <b>Primary Remote Server</b> field.
<b>Port</b>	This value must match the value in the <b>Port</b> field for the primary server.

### Related links

[Configuring SAL Gateway communication with a Concentrator Remote Server](#) on page 132

---

## Configuring NMS

### About this task

Use this procedure to specify SNMP trap destinations. When you configure Network Management Systems (NMSs), the SAL Gateway copies traps and alarms (encapsulated in traps) to each NMS that you configure.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > NMS**.
2. On the Network Management Systems page, complete the following fields:
  - **NMS Host Name/ IP Address**
  - **Trap port**

- **Community**

3. Click **Apply**.
4. (Optional) Use the **Add** button to add multiple NMSs.

See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at <http://support.avaya.com>.

### Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

### Related links

[Network Management Systems field descriptions](#) on page 134

[Applying configuration changes](#) on page 135

---

## Network Management Systems field descriptions

Name	Description
<b>NMS Host Name/ IP Address</b>	The IP address or host name of the NMS server.
<b>Trap port</b>	The port number of the NMS server.
<b>Community</b>	The community string of the NMS server. Use <code>public</code> as the <b>Community</b> , as SAL agents support only public as community at present.

### Related links

[Configuring NMS](#) on page 133

---

## Managing service control and status

### About this task

Use this procedure to view the status of a service, stop a service, or test a service that the SAL Gateway manages.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Service Control & Status**.

The system displays the Gateway Service Control page. The page displays several Gateway Services such as:

- **SAL Agent**
- **Alarming**
- **Inventory**
- **Health Monitor**
- **Remote Access**
- **SAL Watchdog**
- **SAL SNMP Sub-agent**
- **Package Distribution**

The Gateway Service Control page also displays the status of each service as:

- **Stopped**
- **Running**

2. Click one of the following buttons:

- **Stop** to stop a service.
- **Start** to start a service that is stopped.
- **Test** to send a test alarm to the Secure Access Concentrator Core Server.

**!** **Important:**

Use caution if you stop the Remote Access service. Stopping the Remote Access service blocks you from accessing SAL Gateway remotely.

---

## Applying configuration changes

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Apply Configuration Changes**.

The system displays the Apply Configuration Changes page.

2. Click the **Apply** next to **Configuration Changes**.

See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at <http://support.avaya.com>.

When you click **Apply**, the system restarts the SAL Gateway and updates the Gateway with the new values you configured.

The SAL Gateway misses any alarms that are sent while it restarts.

## Managed element worksheet for SAL Gateway

Use this worksheet to record the information required by an administrator to add managed devices to the SAL Gateway.

System Domain (Domain-0) does not have alarming enabled; however, the System Domain has its own Product ID (Alarm ID).

Console Domain (cdom or udom) has alarming enabled. System Domain sends all syslog (system logs) to Console Domain, which then triggers alarms for System Domain.

**! Important:**

For High Availability Failover configurations, you must have two different solution element IDs (SEIDs) for System Domain (Domain-0): one for the active System Domain and one for the standby System Domain. You must administer both SEIDs in the SAL Gateway user interface.

Managed device (virtual machine)	IP Address	SE ID	Product ID	Model	Notes
System Domain (Domain-0)				VSP_2.0.0.0	
Console Domain (cdom or udom)				VSPU_2.1.1.2	

**Related links**

[Adding a managed element](#) on page 136

## Adding a managed element

**Before you begin**

Complete the Managed Element Worksheet for SAL Gateway.

**About this task**

Perform this procedure for each Solution Element ID (SE ID) in the registration information from Avaya.

**Procedure**

1. In the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Managed Element**.



2. On the Managed Element page, click **Add new**.
3. Complete the fields on the page as appropriate.
4. Click **Add**.
5. Click **Apply** to apply the changes.

### Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

### Related links

[Managed Element field descriptions](#) on page 137

[Applying configuration changes](#) on page 135

[Managed element worksheet for SAL Gateway](#) on page 136

---

## Managed Element field descriptions

Name	Description
<b>Host Name</b>	Host name for the managed device. This must match the host name on the Network Configuration page of the System Platform Web Console ( <b>Server Management &gt; Network Configuration</b> in the navigation pane).
<b>IP Address</b>	IP address of the managed device.
<b>NIU</b>	Not applicable for applications that are installed on System Platform. Leave this field clear (not selected).
<b>Model</b>	The model that is applicable for the managed device.
<b>Solution Element ID</b>	The Solution Element ID (SE ID) of the device. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely.
<b>Product ID</b>	The Product ID (also called Alarm ID). The Product ID is in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm.
<b>Provide Remote Access to this device</b>	Check box to allow remote connectivity to the managed device.

*Table continues...*

Name	Description
<b>Transport alarms from this device</b>	(Optional) Check box to enable alarms from this device to be sent to the Secure Access Concentrator Core Server.
<b>Collect Inventory for this device</b>	<p>Check box to enable inventory collection for the managed device.</p> <p>When this check box is selected, SAL Gateway collects inventory information about the managed device and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel working on tickets and must review the configuration of managed devices. For more information on this feature, see the <i>Secure Access Link Gateway 1.8 Implementation Guide</i>. This document is available at <a href="http://support.avaya.com">http://support.avaya.com</a>.</p>
<b>Inventory collection schedule</b>	Interval in hours at which the SAL Gateway collects inventory information about the managed device.
<b>Monitor health for this device</b>	Check box to enable health monitoring of the managed device by SAL Gateway. SAL Gateway uses heartbeats to monitor health. Heartbeats must be configured on the device.
<b>Generate Health Status missed alarm every</b>	<p>Interval in minutes at which SAL Gateway generates an alarm if it does not receive a heartbeat from the managed device.</p> <p>You must restart the SAL Gateway for the configuration changes to take effect. SAL Gateway starts monitoring heartbeats from the device after the restart and generates alarms if it does not receive a heartbeat within the configured interval.</p>
<b>Suspend health monitoring for this device</b>	Check box to suspend health monitoring for the managed device.
<b>Suspend for</b>	Number of minutes to suspend health monitoring for the managed device. SAL Gateway resumes monitoring the device after the configured time elapses.

**Related links**

[Adding a managed element](#) on page 136

---

## Using a stand-alone SAL Gateway

---

### Adding an SNMP trap receiver

#### About this task

Use this procedure to add an SNMP trap receiver for System Platform. If you are using a standalone SAL Gateway, you must add it as an SNMP trap receiver.

#### Procedure

1. In the navigation pane of the System Platform Web Console, click **Server Management > SNMP Trap Receiver Configuration**.
2. On the SNMP Trap Receiver Configuration page, complete the following fields:
  - **IP Address**
  - **Port**
  - **Community**
3. Click **Add SNMP Trap Receiver**.

---

### Disabling SAL Gateway

The locally embedded SAL must be in a disabled state if your Avaya Aura® solution requires a stand-alone SAL Gateway server.

Disable the local SAL if your Avaya Aura® solution requires a higher-capacity, stand-alone SAL Gateway server. This configuration is more appropriate for handling SNMP trap/alarm forwarding and Avaya remote services for a larger Enterprise solution.

Disable the SAL Gateway running on the Services Virtual Machine if you determine, for example, that after expanding your existing Avaya Aura® solution, this SAL Gateway no longer has enough capacity to handle the increased requirements for trap/alarm forwarding and remote services. In this case, install and configure the SAL Gateway on an independent server elsewhere in your network.

#### About this task

Use this procedure to disable the SAL Gateway running on the System Platform Services Virtual Machine.

#### Note:

- If you installed System Platform version 6.2 or later, and deselected the **Enable Services VM** default setting during that process, then neither the embedded SAL nor the local Services Virtual Machine will be active. (With System Platform version 6.2 or later, SAL no longer runs on the Cdom virtual machine, but instead runs on a Services Virtual Machine or services\_vm.) In this scenario, you take no action to disable the embedded SAL Gateway before installing and launching the SAL Gateway on a stand-alone server.

- With System Platform version 6.2 or later, disabling the Services Virtual Machine also disables the local SAL gateway running on that virtual machine.

### **Procedure**

1. In the navigation pane of the System Platform Web Console , click **Server Management > SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Disable SAL Gateway**.

# Chapter 13: Upgrading System Platform

---

## Introduction

This chapter describes how to upgrade System Platform.

**\* Note:**

If you are using the WebLM server co-resident in System Platform to provide licensing services to the AE Services VM, your licenses could be removed when upgrading to System Platform 6.3.4 from an earlier 6.x release. Before upgrading System Platform, see [Determining whether the WebLM license will be removed during an upgrade](#) on page 141.

### Related links

[Determining whether the WebLM license will be removed during an upgrade](#) on page 141

[Upgrades to System Platform 6.3.4](#) on page 143

[Service continuity](#) on page 143

[System Platform upgrades on High Availability systems](#) on page 144

[SAL deployment on the Services Virtual Machine](#) on page 144

---

## Determining whether the WebLM license will be removed during an upgrade

If you are using the WebLM server co-resident in System Platform to provide licensing services to the AE Services VM, your licenses could be removed when upgrading to System Platform 6.3.4 from an earlier release 6.x release. In previous System Platform 6.x releases, the WebLM server was able to support multiple Host IDs. In System Platform 6.3.4, the WebLM server can support only the Primary Host ID.

Depending on your AE Services release, perform the appropriate procedure to determine whether your WebLM license will be affected.

### Systems running AE Services 6.1.x or 6.2.x

If your system is running AE Services 6.1.x or 6.2.x, perform the following steps:

1. Open an ssh session to the System Platform Dom0 VM, and log in as the system administrator.
2. Promote your account to the root user.

3. From the command line, enter `ifconfig | grep eth0` and press **Enter** to obtain the Host ID (HWaddr) of Dom0.

The system displays the Host ID (HWaddr) of Dom0. The following is an example of the output displayed for the command you entered:

```
eth0 Link encap: Ethernet HWaddr 00:12:3A:BC:DE:FG
```

In this example, HWaddr 00:12:3A:BC:DE:FG is the Host ID (HWaddr) of Dom0.

4. Open an ssh session to the System Platform C-Dom VM, and log in as the system administrator.
5. Promote your account to the root user.
6. From the command line, enter `cd /opt/avaya/vsp/tomcat/webapps/WebLM/licenses/` and press **Enter**.
7. From the command line, enter `grep APPL_ENAB *` and press **Enter**.

The system displays information about the AE Services license. The following is an example of the output displayed for the AE Services license:

```
wlm12345678license.xml:<LAR platformType="APPL_ENAB" sid="123456" version="1.0">
```

**\* Note:**

If no information is displayed, an AE Services license is not installed in the SP WebLM. If a license is not installed in the SP WebLM, do not perform the remaining steps in this procedure.

8. From the command line, enter `grep <Dom0-Host-ID> <AESvcs-License-File-Name>`

where

- `<Dom0-Host-ID>` is the Host ID of Dom0 (without any colons) that you obtained in Step 3 (for example, 00123ABCDEF).
- `<AESvcs-License-File-Name>` is the AE Services license file name you obtained in Step 7 (for example, wlm12345678license.xml).

Using the examples from Steps 3 and 7, you would enter the command `grep 00123ABCDEF 00123ABCDEF wlm12345678license.xml`.

9. Press **Enter**.
10. Verify that the Primary Host ID from Step 3 is displayed.
11. Perform one of the following steps:
  - If the Primary Host ID is not displayed, contact Avaya Services to obtain a new license based on the Primary Host ID.
  - If the Primary Host ID is displayed, proceed with the System Platform upgrade process.

### Systems running AE Services 6.3.0

If your system is running AE Services 6.3.3, perform the following steps:

1. Log into the System Platform Management Console.

2. Select **Server Management > License Management**.
3. Click **Launch WebLM License Manager**.
4. Log into the WebLM Management Console.
5. From the WebLM menu, select **Server Properties**.
6. Note the Host ID specified as Primary Host ID.
7. From the WebLM menu, select **Licensed products > APPL\_ENAB > Application\_Enablement**.
8. In the displayed AE Services license, locate the label License File Host IDs.
9. Verify that the Primary Host ID from Step 6 is specified in the license file.
10. Perform one of the following steps:
  - If the Primary Host ID is not specified in the license file, contact Avaya Services to obtain a new license based on the Primary Host ID.
  - If the Primary Host ID is specified in the license file, proceed with the System Platform upgrade process.

#### Related links

[Introduction](#) on page 141

---

## Upgrades to System Platform 6.3.4

System Platform 6.3.4 is an RPM-based feature pack and installed on System Platform 6.3, which is an ISO image.

If the system is currently running a version of System Platform that is earlier than 6.3, you must first upgrade to 6.3. Once the system is running System Platform 6.3, you can install the 6.3.4 patch.

#### Related links

[Introduction](#) on page 141

---

## Service continuity

### **Caution:**

To minimize service disruptions during platform upgrades, complete all preupgrade tasks and the entire upgrade process during a planned maintenance interval.

If System Platform is being upgraded from a version earlier than 6.2 and uses the embedded SAL Gateway, before you attempt the platform upgrade, you must assign a new IP address to the Console Domain and assign the former Console Domain IP address to the SAL Gateway. If you fail to complete this requirement, your System Platform server will lose communication with Avaya during a critical phase of the platform upgrade. The process itself includes a reboot of the entire system, and this too will disrupt the continuity of Avaya services during the maintenance interval.

## Related links

[Introduction](#) on page 141

---

# System Platform upgrades on High Availability systems

## \* Note:

Avaya Aura System Platform High Availability does not support:

- IPv6 and cannot be configured with IPv6 addresses.
- Customer provided servers.

When both the primary and secondary servers in a High Availability (HA) configuration require a System Platform upgrade, perform the platform upgrade on each server independently. In addition, the following are key requirements of the platform upgrade process for High Availability deployments with System Platform:

- Regardless of your existing or planned System Platform High Availability deployment scenario, complete all preupgrade tasks on both the primary and secondary servers before proceeding with the two independent platform upgrades.
- If the primary and secondary servers are part of an existing System Platform 6.0 High Availability configuration, you must **Stop HA** and **Remove HA** on the primary server before you perform the preupgrade tasks and the platform upgrade procedure on either server. System Platform does not support platform upgrades while High Availability is running. If you attempt an upgrade with High Availability running, a warning message appears and the system prevents you from performing the upgrade on either server.
- When the Services VM Network Configuration window appears at the beginning of the System Platform upgrade *for the standby server*, clear the **Enable Services VM** check box to ensure that you install the Services VM in a disabled state. If a failover occurs later during HA system operation, the failover subsystem activates the Services VM on the former standby (now active) server, propagates the current Services VM configuration to that server, and deactivates the Services VM on the former active (now standby) server.
- After completing the platform upgrade on both servers, you must reenter your High Availability configuration and then **Start HA** on the primary server.

## Related links

[Introduction](#) on page 141

[Upgrading System Platform on both servers](#) on page 177

---

# SAL deployment on the Services Virtual Machine

Beginning with System Platform release 6.2, the Secure Access Link Gateway (SAL Gateway) no longer runs on the System Platform Console Domain (cdom) virtual machine. Instead, SAL Gateway runs on an independent Services virtual machine (services\_vm domain) on your Avaya Aura<sup>®</sup> solution server. As with the earlier implementation of the SAL Gateway running on the cdom virtual



machine, this new configuration supports secure remote access to local server resources, and forwards alarms (SNMP traps) from your local solution server to a remote Network Management System (NMS).

As of System Platform release 6.2, releases of the Services virtual machine are independent of System Platform releases. Services VM version 2.0 is included with System Platform 6.3. After upgrading to System Platform 6.3.1, you must upgrade the Services VM to version 3.0.

- If you are upgrading from System Platform 6.2.x or later, the Master Agent configuration is preserved when you upgrade Services VM.
- If you are upgrading from System Platform 6.0.3, Services VM version 2.0 is included in your upgrade to System Platform 6.3. After the platform upgrade, you must configure the Net-SNMP Master Agent in the Services VM to forward either SNMPv2c or SNMPv3 traps to your NMS.

For more information on the Services VM, see *Implementing and Administering Services-VM*, available at <http://support.avaya.com>.

For more information about SAL capabilities, see *Secure Access Link 2.2 SAL Gateway Implementation*, at <http://support.avaya.com>.

### Related links

[Introduction](#) on page 141

[Configuring SNMP version support on the Services VM](#) on page 180

[Upgrading Services-VM on System Platform](#) on page 182

[Platform upgrade process in different System Platform deployments](#) on page 166

---

## Checklists for upgrading System Platform

### Checklist for upgrading System Platform

Use this checklist to upgrade to System Platform 6.3 from an earlier version.

If you are planning to install System Platform 6.3.4 and System Platform 6.3 is already installed on your system, install just the 6.3.4 feature pack. System Platform 6.3.4 is an RPM-based feature pack. Start with Step 6 in the following checklist.

**\* Note:**

If you are upgrading a High Availability system, see “Checklist for upgrading System Platform on a High Availability system.”

#	Task	Notes	✓
1	Complete all System Platform preupgrade tasks. See <a href="#">Preupgrade checklist</a> on page 155.		

*Table continues...*

#	Task	Notes	✓
	See also the latest Release Notes for System Platform and for your solution template.		
2	Upgrade System Platform to version 6.3 by first understanding the <a href="#">Platform upgrade process in different System Platform deployments</a> on page 166, and then by following the steps for <a href="#">Upgrading a System Platform server</a> on page 167 .		
3	Verify a successful System Platform upgrade. See <a href="#">Verifying an upgrade</a> on page 170 .		
4	Commit the platform upgrade. See <a href="#">Committing an upgrade</a> on page 173.		
5	If you are upgrading from System Platform 6.0.3 and your NMS uses SNMP v2c, change the SNMP version that is supported on the Services virtual machine. See <a href="#">Configuring SNMP version support on the Services VM</a> on page 180.	This task is required only if you are upgrading from System Platform 6.0.3 and if your NMS uses SNMP v2c. By default the Services VM supports SNMP v3. If you are upgrading from System Platform 6.2 or later, omit this task.	
6	Check for System Platform patches and features packs at <a href="http://support.avaya.com">http://support.avaya.com</a> . Install any patches or features packs that are available.  System Platform 6.3.4 is installed as a patch.  See <a href="#">Feature Pack installation</a> on page 93 and <a href="#">Installing patches</a> on page 96.		
7	Download and upgrade the Services virtual machine to version 3.0. See <a href="#">Upgrade of Services VM</a> on page 182.		
8	If a license was generated using a host ID other than the primary host ID, generate and install a new license file with the primary host ID. See <a href="#">Licensing change in System Platform 634</a> on page 181.		
9	Inform users to change their passwords if you want SHA2 hashing to take effect. See <a href="#">Password hashing</a> on page 182.		
10	Download required patches or upgrades for the solution template.		
11	Upgrade the solution template.		

**Related links**

[Introduction](#) on page 141

**Checklist for upgrading System Platform on High Availability systems**

Use this checklist to upgrade an existing pair of System Platform servers that is running in a High Availability Fast Reboot configuration to System Platform version 6.3.

If you are planning to install System Platform 6.3.4 and System Platform 6.3 is already installed on your system, install just 6.3.4 feature pack. System Platform 6.3.4 is an RPM-based feature pack. Start with Step 6 in the following checklist.

#	Task	Notes	✓
1	Understand and complete all preupgrade tasks for Locally Redundant System Platform High Availability configurations. See <a href="#">Preupgrade checklist for System Platform on High Availability systems</a> on page 157.  See also the latest Release Notes for System Platform and for your Avaya Aura® solution template.	<b>! Important:</b> <ul style="list-style-type: none"> <li>Requirement to Stop HA and Remove HA on the primary server before you attempt to upgrade either System Platform server.</li> </ul>	
2	Upgrade System Platform on both servers in a Locally Redundant High Availability configuration, as described in <a href="#">Upgrading System Platform on both servers</a> on page 177 and in <a href="#">Upgrading a System Platform server</a> on page 167.	<b>! Important:</b> <p>The Services virtual machine must be disabled on the standby server during the upgrade procedure.</p>	
3	Verify the System Platform upgrade on each HA server individually. See <a href="#">Verifying an upgrade</a> on page 170.		
4	Commit the platform upgrade on each server individually. See <a href="#">Committing an upgrade</a> on page 173.		
5	If you are upgrading from System Platform 6.0.3 and your NMS uses SNMP v2c, change the SNMP version that is supported on the Services virtual machine. See <a href="#">Configuring SNMP version support on the Services VM</a> on page 180.	This task is required only if you are upgrading from System Platform 6.0.3 and if your NMS uses SNMP v2c. By default the Services VM supports SNMP v3. If you are upgrading from System Platform 6.2 or later, omit this task.	
6	Check for System Platform patches and features packs at <a href="http://support.avaya.com">http://support.avaya.com</a> . Install any patches or features packs that are available.		

*Table continues...*

#	Task	Notes	✓
	System Platform 6.3.4 is installed as a patch. See <a href="#">Installing System Platform patches on High Availability systems</a> on page 97 and <a href="#">Installing patches</a> on page 96.		
7	Download and upgrade the Services virtual machine to version 3.0. See <a href="#">Upgrade of Services VM</a> on page 182.	Perform this upgrade only on the primary server.	
8	If a license was generated using a host ID other than the primary host ID, generate and install a new license file with the primary host ID. See <a href="#">Licensing change in System Platform 634</a> on page 181.		
9	Inform users to change their passwords if you want SHA2 hashing to take effect. See <a href="#">Password hashing</a> on page 182.		
10	Download required patches or upgrades for the solution template.		
11	Upgrade the solution template. Perform this upgrade only on the primary server.		

**Related links**

[Introduction](#) on page 141

## System Platform upgrade paths, service packs, and patches

### About System Platform upgrade files

Avaya distributes System Platform upgrade files and patches in various formats and from various sources.

#### System Platform upgrade files

Avaya distributes System Platform software in the standardized *ISO file format* commonly written to optical disk (CD or DVD). For System Platform, the ISO file typically contains all the files necessary to perform either a new System Platform installation or an upgrade.

**\* Note:**

With Avaya Aura solutions that run on System Platform, your solution documentation can require you to download additional files individually.

You can obtain the ISO file or the platform upgrade (\*.ova) description file from any of the following sources:

- **PLDS** – Avaya Product Licensing and Delivery System. Contains all files necessary for System Platform new installations and upgrades.
- **HTTP** – ISO and/or \*.ova upgrade description file stored in advance on a designated remote HTTP server in the customer's network.
- **SP server** – ISO and/or \*.ova upgrade description file stored in advance on a designated System Platform server in the customer's network.

System Platform knows where to look for ISO and \*.ova files because you configured the URLs for each of the above servers during earlier System Platform installation.

**\* Note:**

Regardless of what is the source of upgrade files (PLDS, HTTP web server, or System Platform server), that source must contain all of the files required for your upgrade, especially if you must download some non-ISO files individually, according to upgrade instructions in your Avaya Aura solution documentation.

If you download an ISO file to the server you must upgrade, you can:

- Use File Manager in the Web Console to copy the contents of a physical CD/DVD (inserted in the server's CD/DVD drive) into the System Platform file system. During the upgrade, you can then use the **SP CD/DVD** option as your source for any files you require to upgrade System Platform.
- Use WinZip release 12 (or later) to extract from the ISO file a FAT32 file system to a folder you specify, and then copy the contents of that folder to a USB storage device. You can then use the **SP USB Disk** option in the Web console to identify the USB disk as the source for files for upgrading System Platform.

**\* Note:**

System Platform 6.2 and later versions do not fit on CD media. The ISO file could contain enough data to fill one or more DVDs.

If your source of upgrade files is PLDS, you can typically download the \*.ova description file to the server you must upgrade, activate the upgrade process through the Web Console, and System Platform automatically downloads only the files referenced in the \*.ova description file.

## System Platform patches

Avaya distributes \*.rpm patches for you to apply to your existing version of System Platform. Before you attempt a System Platform upgrade, you must apply these patches in the required sequence. See “Upgrade paths to System Platform 6.3.4” and “System Platform release history and upgrade information.”

**!** **Important:**

For information about Patches issued after the release date of this publication, see the latest System Platform Release Notes, available from <http://support.avaya.com>

**\*** **Note:**

Before downloading any patch, be sure to check its description in the Release Notes. When indicated by the patch description, you must install patches on both the primary and secondary servers independently. The primary server does not automatically replicate patches to the secondary/standby server.

**!** **Important:**

Before installing any patches on either server, **Stop HA** and **Remove HA** on the primary server.

**Related links**

[Upgrade paths to System Platform 6.3.4](#) on page 150

[System Platform release history and upgrade information](#) on page 151

---

## Upgrade paths to System Platform 6.3.4

System Platform 6.3.4 is an RPM-based feature pack and installed on System Platform 6.3, which is an ISO image.

If the system is currently running a version of System Platform that is earlier than 6.3, you must first upgrade to 6.3. Once the system is running System Platform 6.3, you can install the 6.3.4 patch.

Direct upgrade to System Platform 6.3 is possible from the following software versions:

- 6.0.3.0.3 plus patch 6.0.3.4.3 or later
- 6.2.0.0.27 or 6.2.0.2.27
- 6.2.1.0.9
- 6.2.2

### Upgrade path from System Platform 1.1

If you are upgrading to System Platform 6.3.4 from System Platform 1.1, you must:

1. Perform a platform upgrade to 1.1.1.0.2.
2. Apply cumulative patch 1.1.1.98.2.
3. Perform a platform upgrade to System Platform version 6.0.3.0.3.
4. Apply cumulative patch 6.0.3.10.3.
5. Perform a platform upgrade to 6.3.
6. Install 6.3.4, an RPM-based feature pack, as a patch.

### Upgrade path from System Platform 6.0

If you are upgrading to System Platform 6.3.4 from System Platform 6.0, you must:

1. Perform a platform upgrade to System Platform version 6.0.3.0.3.

2. Apply cumulative patch 6.0.3.10.3.
3. Perform a platform upgrade to 6.3.
4. Install 6.3.4, an RPM-based feature pack, as a patch.

### Upgrade path from System Platform 6.2.1.0.9

If you are upgrading to System Platform 6.3.4 from System Platform 6.2.1.0.9, perform a platform upgrade directly to 6.3, and then install 6.3.4 as a patch.


## System Platform release history and upgrade information

The following table summarizes ISO (initial release) versions, as well as service pack and feature pack (RPM) patch versions available for System Platform upgrades. The table also describes:

- the upgrade paths from version to version of each initial and patch release of System Platform.
- whether you can install each platform upgrade or patch on systems running System Platform High Availability.

All patches for a release are cumulative and include fixes from earlier patches for the same release

See the *Avaya Aura® System Platform 6.3.1 Release Notes* for more details about ISO (initial release) and RPM patch (service pack or feature pack) versions available for System Platform.


Initial release	Subsequent patches (service packs or feature packs)	Install patch on	Can install patch on systems running System Platform High Availability?	Can upgrade to the next major/minor release?
1.0.0.0.25 (ISO)	First release of 1.0.	Not applicable.	Not applicable.	Yes, to System Platform 1.1.0.
1.1.0.0.10 (ISO)	First release of 1.1.	Not applicable.	Not applicable.	No.
	1.1.0.3.10	1.1.0.0.10	<p>No. If you are running System Platform High Availability, you must stop it before installing this patch, and then install the patch on both the active and standby nodes.</p> <p> <b>Note:</b> If you install the patch before stopping System Platform High</p>	No.

*Table continues...*

Initial release	Subsequent patches (service packs or feature packs)	Install patch on	Can install patch on systems running System Platform High Availability?	Can upgrade to the next major/minor release?
			Availability, you must remove the patch, stop High Availability, and then reinstall the patch. Otherwise, you will not be able to install the patch on the standby node. The standby node will inaccurately report that the patch is already installed and prevent you from installing it.	
	1.1.0.6.10	1.1.0.3.10	No.	Yes, to 1.1.1.0.2.
1.1.1.0.2 (ISO)	First release of 1.1.1.	Not applicable.	Not applicable.	No.
	1.1.1.98.2	1.1.1.0.2	Yes.	Yes, to 6.0.0.0.11 or 6.0.3.0.3.
6.0.0.0.11 (ISO)	First release of 6.0.0.	Not applicable.	Not applicable.	Yes, to 6.0.1.0.5, 6.0.2.0.5, or 6.0.3.0.3.
6.0.1.0.5 (ISO)	First release of 6.0.1.	Not applicable.	Not applicable.	No.
	6.0.1.3.5	6.0.1.0.5	Yes. Stop HA and Remove HA before applying patch. Configure HA and Start HA after applying patch.	Yes, to 6.0.2.0.5 or 6.0.3.0.3.
6.0.2.0.5 (ISO)	First release of 6.0.2.	Not applicable.	Not applicable.	No.
	6.0.2.6.5 (cumulative patch that includes fixes from 6.0.2.1.5, 6.0.2.3.5, 6.0.2.5.5, and 6.0.2.6.5)	6.0.2.0.5	Yes. Stop HA and Remove HA before applying patch. Configure HA and Start HA after applying patch.	Yes.

*Table continues...*



Initial release (ISO)	Subsequent patches (service packs or feature packs)	Install patch on	Can install patch on systems running System Platform High Availability?	Can upgrade to the next major/minor release?
6.0.3.0.3 (ISO)	First release of 6.0.3.	Not applicable.	Not applicable.	No.
	6.0.3.1.3	6.0.3.0.3	Not applicable.	No.
	6.0.3.3.3	6.0.3.1.3	Yes. Stop HA and Remove HA before applying patch. Configure HA and Start HA after applying patch.	No.
	6.0.3.4.3  <b>Note:</b> The minimum patch level from which you can upgrade to System Platform 6.2.0.0.27 is 6.0.3.4.3.	6.0.3.3.3	Yes. Stop HA and Remove HA before applying patch. Configure HA and Start HA after applying patch.	Yes, to 6.2.0.0.27 or 6.2.1.0.9 or 6.3.
	6.0.3.6.3	6.0.3.4.3	Yes. Stop HA and Remove HA before applying patch. Configure HA and Start HA after applying patch.	Yes, to 6.2.0.0.27 or 6.2.1.0.9 or 6.3.
	6.0.3.7.3	6.0.3.4.3 or 6.0.3.6.3	Yes. Stop HA and Remove HA before applying patch. Configure HA and Start HA after applying patch.	Yes, to 6.2.0.0.27 or 6.2.1.0.9 or 6.3.
	6.0.3.9.3	6.0.3.4.3, 6.0.3.6.3, or 6.0.3.7.3	Yes. Stop HA and Remove HA before applying patch. Configure HA and Start HA after applying patch.	Yes, to 6.2.0.0.27 or 6.2.1.0.9 or 6.3.
	6.0.3.10.3	6.0.3.4.3, 6.0.3.6.3, 6.0.3.7.3, or 6.0.3.9.3	Yes. Stop HA and Remove HA before applying patch. Configure HA and Start HA after applying patch.	Yes, to 6.2.0.0.27 or 6.2.1.0.9 or 6.3.
6.2.0.0.27 (ISO)	First release of System Platform 6.2.	Not applicable.	Not applicable.	Yes.

*Table continues...*

Initial release	Subsequent patches (service packs or feature packs)	Install patch on	Can install patch on systems running System Platform High Availability?	Can upgrade to the next major/minor release?
	6.2.0.2.27	6.2.0.0.27	Yes. Stop HA and Remove HA before applying patch. Configure HA and Start HA after applying patch.	Yes, to 6.2.1.0.9 or 6.3.
6.2.1.0.9 (ISO)	First release of System Platform 6.2.1.	Not applicable.	Not applicable.	Yes, to System Platform 6.2.2 or 6.3.
6.2.2.06002.0 (Feature Pack 1 RPM patch for System Platform 6.2.1)	6.2.2.06002.0 is the FP1 RPM patch for 6.2.1.0.9.	6.2.1.0.9	Yes. Stop HA and Remove HA before applying the FP1 patch. Configure HA and Start HA after applying the FP1 patch.	Yes, to 6.3.
	6.2.2.08001.0	6.2.2.06002.0		Yes, to 6.3.
	6.2.2.09001.0	6.2.2.x		Yes, to 6.3.
6.3 (Feature Pack 2 ISO for System Platform 6.2)	First release of 6.3.	Not applicable. First release of 6.3.	Yes. Stop HA and Remove HA before installing 6.3. Configure HA and Start HA after installing 6.3.	
6.3.1 (Feature Pack 3 RPM patch for System Platform 6.3)	6.3.1 is the Feature Pack 3 RPM patch for 6.3.	6.3	Yes. Stop HA and Remove HA before applying the feature pack patch. Configure HA and Start HA after installing the feature pack patch.	
6.3.4 (Feature Pack 4 RPM patch for System Platform 6.3)	6.3.4 is the Feature Pack 4 RPM patch for 6.3.	6.3	Yes. Stop HA and Remove HA before applying the feature pack patch. Configure HA and Start HA after installing the feature pack patch.	

---

## System Platform releases

Go to Avaya Support at <http://support.avaya.com> and download the *Avaya Aura® System Platform 6.3.4 Release Notes*. See in particular the section “Software Release Versions,” which provides the names, dates of issue, and exact filenames for every full release (ISO platform upgrade or ISO feature pack upgrade) and patch release (RPM service pack or RPM feature pack upgrade) you can download from the Avaya Product Licensing and Download System (PLDS) at <https://plds.avaya.com>. The Release Notes also provide information about any known issues, as well as issues fixed, in the current release.

---

## Solution template patches

Check with your Avaya representative or the latest release notes for your solution template to determine compatibility with the latest System Platform version. Apply recommended patches to your solution template where required to ensure compatibility with the version of System Platform qualified with your solution template.)

You can download, install, and manage the regular updates and patches for solution templates at <http://support.avaya.com>. You can also download or install solution template patches from the Avaya Product Licensing and Delivery System (PLDS) at <http://plds.avaya.com>.

---

## Preupgrade tasks

---

### Preupgrade checklist

#	Task	Notes	✓
1	Download and install any patches for your current version of System Platform. See “Installing patches.”		
2	If you have not already done so, download all necessary System Platform upgrade files from DVD media, a USB storage device, or an HTTP server, or use File Manager to copy it to the target System Platform server's local <code>/vsp-template</code> directory.		

*Table continues...*

#	Task	Notes	✓
3	Check with your Avaya representative or the latest release notes for your solution template to confirm that it is compatible with the latest version of System Platform. If required, install recommended patches to your solution template to ensure compatibility with the version of System Platform that is qualified with your solution template.	You can download, install, and manage the regular updates and patches for solution templates at <a href="http://support.avaya.com">http://support.avaya.com</a> . You can also download or install solution template patches from the Avaya Product Licensing and Delivery System (PLDS) at <a href="http://plds.avaya.com">http://plds.avaya.com</a> .	
4	Capture all current configuration settings from the <b>Server Management &gt; System Configuration</b> page of the Web Console.	You will need this information later to verify that all configuration settings carried forward during the upgrade process are correct and complete.	
5	Note the method of the date and time configuration that is set. Are the date and time manually set or configured to synchronize with an NTP server at a specific IP address?		
6	Back up System Platform and the solution template. See <a href="#">System Platform backup</a> on page 159.		
7	<p>If you are upgrading from System Platform 6.0, assign a new IP address to the Console Domain virtual machine and assign the former Console Domain IP address to the SAL Gateway. The customer must provide to the installer one new IP address for Console Domain. See <a href="#">Cdom and SAL Gateway IP address assignments</a> on page 160.</p> <p><b>* Note:</b></p> <p>Perform this task only if the current version System Platform is using the embedded SAL Gateway. This task is not applicable if System Platform is currently using a stand-alone SAL Gateway.</p>	Perform this task only if you are upgrading from a System Platform version earlier than 6.2. If upgrading from System Platform 6.2 or later, this task is not required.	

## Preupgrade checklist for System Platform on High Availability systems

#	Task	Notes	✓
1	Download and install any patches for your current version of System Platform. See "Installing patches."		
2	If you have not already done so, download all necessary System Platform upgrade files from DVD media, a USB storage device, or an HTTP server, or use File Manager to copy it to the target System Platform server's local <code>/vsp-template</code> directory.		
3	Check with your Avaya representative or the latest release notes for your solution template to confirm that it is compatible with the latest version of System Platform. If required, install recommended patches to your solution template to ensure compatibility with the version of System Platform that is qualified with your solution template.	You can download, install, and manage the regular updates and patches for solution templates at <a href="http://support.avaya.com">http://support.avaya.com</a> . You can also download or install solution template patches from the Avaya Product Licensing and Delivery System (PLDS) at <a href="http://plds.avaya.com">http://plds.avaya.com</a> .	
4	Record all High Availability settings.		
5	Capture all current configuration settings from the <b>Server Management &gt; System Configuration</b> page of the Web Console.	You will need this information later to verify that all configuration settings carried forward during the upgrade process are correct and complete.	
6	Note the method of the date and time configuration that is set. Are the date and time manually set or configured to synchronize with an NTP server at a specific IP address?		
7	Stop and remove High Availability on the primary server. See <a href="#">Stopping System Platform High Availability</a> on page 114 and <a href="#">Removing the High Availability configuration</a> on page 115.		
8	Back up System Platform and the solution template. See <a href="#">System Platform backup</a> on page 159.		

*Table continues...*

#	Task	Notes	✓
9	<p>If you are upgrading from System Platform 6.0, assign a new IP address to the Console Domain virtual machine and assign the former Console Domain IP address to the SAL Gateway. The customer must provide to the installer one new IP address for Console Domain. See <a href="#">Cdom and SAL Gateway IP address assignments</a> on page 160.</p> <p><b>* Note:</b></p> <p>Perform this task only if the current version System Platform is using the embedded SAL Gateway. This task is not applicable if System Platform is currently using a stand-alone SAL Gateway.</p>	<p>Perform this task only if you are upgrading from a System Platform version earlier than 6.2. If upgrading from System Platform 6.2 or later, this task is not required.</p>	

## Stopping System Platform High Availability

### Before you begin

#### Important:

Stopping High Availability operations during disk synchronization could corrupt the file system of the standby console domain. Check the status of virtual machine replication on the High Availability page of the Web Console.

### About this task

This procedure stops High Availability operation and returns System Platform to standard operation without High Availability protection. This procedure does not remove the High Availability configuration from either server.

### Procedure

1. Click **Server Management > High Availability**.
2. Click **Stop HA** and confirm the displayed warning.

Verify the status of virtual machine replication on the High Availability page.

### Related links

[High Availability start/stop](#) on page 113

[Upgrading System Platform on both servers](#) on page 177

[Installing System Platform patches on High Availability systems](#) on page 97

[Starting System Platform High Availability](#) on page 113

[Removing the High Availability configuration](#) on page 115

---

## System Platform backup

With some exceptions, you can back up configuration information for System Platform and the solution template (all template virtual machines).

**\* Note:**

The System Platform backup feature does not back up the following types of configuration data:

- System parameters (examples: SNMP Discovery, Template product ID)
- Networking parameters (examples: Template IP and host name, Console Domain IP and host name, static IP route configuration)
- Ethernet parameters (examples: Auto-negotiation, speed and port information)
- Security configuration (examples: SSH keys, Enable Advance password, Host access list)

In scenarios where, for example, an administrator performs a system backup prior to a template or platform upgrade or platform replacement, and the system generates new unique SSH keys internally as part of the upgrade or replacement action. The SSH keys generated prior to the backup operation are of no use to the system updated or replaced.

System Platform backs up sets of data and combines them into a larger backup archive. Backup sets are related data items available for backup. When you perform a back up, the system executes the operation for all backup sets. All backup sets must succeed to produce a backup archive. If any of the backup set fails, then the system removes the backup archive. The amount of data backed up depends on the specific solution template.

The system stores the backup data in the `/vspdata/backup` directory in Console Domain. This is a default location. During an upgrade, the system does not upgrade the `/vspdata` folder, facilitating a data restore operation if required. You can change this location and back up the System Platform backup archives to a different directory in System Platform or in an external server. Optionally, send the backup data to an external e-mail address if the file size is smaller than 10 MB.

If a backup fails, the system automatically redirects to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup succeeds.

**! Important:**

If you backup an instance of System Platform with not template installed, the server to which you restore the backup must also have no template installed. If any template is installed, the restore will fail.

### Backups and restores across different versions of System Platform

You cannot restore an older version of System Platform from a backup created on a newer version of System Platform. For example, you cannot restore a System Platform 6.3 backup to System Platform 6.0. However, you can (for example), restore a System Platform 6.0 backup to System Platform 6.3, although not all templates support this ability. Confirm in your solution documentation

whether or not the solution template supports restoring an older version of System Platform backup to the current version.

### **Backups and System Platform High Availability**

The System Platform backup feature does not provide a mechanism to reenab a failed System Platform High Availability node. For more information, see one of the following topics appropriate for your troubleshooting scenario:

- Re-enabling a failed preferred node to High Availability
- Re-enabling a failed standby node to High Availability

---

## **Cdom and SAL Gateway address assignments**

### **Overview**

If you are upgrading to System Platform 6.3 from a version earlier than 6.2, you must complete one of the following procedures. Choose the appropriate procedure depending on whether you are performing the upgrade from a remote location or on-site where the server is located:

- [Reassigning Cdom and SAL Gateway IP addresses remotely](#) on page 161
- [Reassigning Cdom and SAL Gateway IP addresses onsite](#) on page 163

#### **! Important:**

Perform this task only if you are upgrading from a System Platform version earlier than 6.2. If upgrading from System Platform 6.2 or later, this task is not required.

#### **\* Note:**

This prerequisite does not apply to Avaya Aura solutions that have deployed a remote stand-alone SAL Gateway server. In this case, IP addresses assigned to your system must remain unchanged, because you will not enable the Services Virtual Machine during the platform upgrade process. During an upgrade, the System Platform installation software verifies if your system already uses the local SAL Gateway. If the system is not using the local SAL Gateway, the System Platform installation program automatically installs the Services Virtual Machine in a disabled state, which also disables its embedded SAL Gateway.

On both procedures, you must assign a new IP address to the Cdom virtual machine, and then assign the former Cdom IP address to the SAL Gateway. The Avaya customer must provide any site-specific IP address assignments.

With System Platform versions 6.2 and later, a new Services Virtual Machine hosts the SAL Gateway unless you have already deployed a remote SAL Gateway server. You do not need to redefine alarm destinations for template applications running on the same server if you assigned both:

- The previous Cdom IP address to the embedded SAL Gateway and
- A new IP address to the Cdom virtual machine.



. You do not have to redefine alarm destinations because the IP address of the SAL Gateway remains unchanged throughout the upgrade process. Completing this process ensures that the SAL Gateway remains in communication with Avaya (or an Avaya Partner) during the upgrade event.

The following tables provide an example of Dom0, Cdom, and embedded SAL Gateway address assignments before and after completing the System Platform upgrade prerequisite:

**Table 1: Example Dom0, Cdom, and SAL Gateway address allocations before upgrading to System Platform 6.3**

Virtual Machine or Application	IP Address 1	IP Address 2
Domain 0 (dom0)	192.168.10.100	
Console Domain (cdom)		192.168.10.101 (shared)
Integrated SAL Gateway (version 1.8)		

**Table 2: Example Dom0, Cdom, and SAL Gateway address allocations after upgrading to System Platform 6.3**

Virtual Machine or Application	IP Address 1	IP Address 2	IP Address 3
Domain 0 (dom0)	192.168.10.100		
Console Domain (cdom)		(Reallocated to Services Virtual Machine.)	192.168.10.102 (New address assignment)
Integrated SAL Gateway (version 2.2) on Services Virtual Machine (services_vm)		192.168.10.101 (Reassigned from former cdom virtual machine)	

## Reassigning Cdom and SAL Gateway IP addresses remotely

Perform this task when a System Platform upgrade must be performed from a location remote from the customer site. A Support Engineer at Avaya or an Avaya Partner site must complete this task entirely by communication established between an Avaya Remote Server and the server you must upgrade.

### Before you begin

- If you are a customer of Avaya or an Avaya Partner and must upgrade to System Platform version 6.3 from a version earlier than 6.2, go to <http://support.avaya.com> and click on **Support Contact Options > Maintenance Support**.
- Complete the blank fields in the following table. The following steps reference either address “A” or “B”, as appropriate.

**Table 3: Cdom IP address assignments (remote procedure)**

<b>Current Cdom (avpublic) IP Address:</b>	A.
<b>New customer-provided IP address for Cdom:</b>	B.

*Table continues...*

(The new address for the cdom virtual machine must be on the same IP subnet used by the System Platform Domain 0 virtual machine. Verify using Linux <code>ipcalc</code> or similar tool.)	
--	--

- Support Engineers must have their Token (SecureID) USB device available for additional authentication.

## About this task

### Important:

If you are upgrading a System Platform High Availability configuration that uses the embedded SAL Gateway, complete Cdom and SAL Gateway IP address reassignments on the primary server only, and only after stopping High Availability. If you later have a High Availability failover event (triggered manually or automatically), the High Availability subsystem enables the Services VM on the standby server. The HA data replication software also automatically propagates the new Cdom and SAL Gateway IP addresses to the standby server.

Use of the term *target server* in this procedure refers to the System Platform server you must upgrade.

## Procedure

1. Log on to the SAL Remote Server at <https://tech1.sal.avaya.com>
2. Using the SE ID of VSPU (cdom), open a remote HTTPS SAL session with the Cdom virtual machine on the target server.
3. Log on to the System Platform Web Console, and log in as **admin**.
4. Click **Server Management > Network Configuration**.
5. From the **Domain Network Interface** panel, under the **Console Domain**, note the **avpublic** IP address from [Table 3: Cdom IP address assignments \(remote procedure\)](#) on page 161, field "A".
6. Enter the new, customer-provided cdom IP address (from [Table 3: Cdom IP address assignments \(remote procedure\)](#) on page 161, field "B") into the Console Domain **avpublic IP** field.
7. Click **Save**.  
Saving the change you made to the Cdom IP address configuration temporarily severs your secure connection to the target server. However, the server continues to have connectivity and communication with the remote Avaya servers. (Your SAL Gateway 1.8 gracefully manages changes to the server's IP address configuration.)
8. From the SAL Remote Server at <https://tech1.sal.avaya.com>, request an HTTPS session with the SAL Gateway on the target server.
9. Log on to the SAL Gateway user interface using the VSALGW SE ID: (`https://<localhost>:7443`)
10. Update the Cdom managed element (VSPU) to match the value in [Table 3: Cdom IP address assignments \(remote procedure\)](#) on page 161, field "B".

11. Click **Apply** and submit your changes to restart SAL Gateway services.
12. Disconnect from the SAL Gateway on the target server.
13. From the SAL Remote Server at <https://tech1.sal.avaya.com>, again request an HTTPS session with the Cdom virtual machine on the target server.  
This tunnel session now ends at the new address assigned to the Cdom virtual machine on the target server.
14. Using the SE ID of VSPU (Cdom), open a remote HTTPS SAL session with the Cdom virtual machine on the target server.
15. Log on to the Web Console of the target server.
16. Restart AES DBService and aesvs:
  - a. Start an SSH session.
  - b. Log in to AES as administrator
  - c. Type `su -sroot`.
  - d. Enter the password for the sroot user.
  - e. Type `/sbin/service DBService restart`.
  - f. Type `/sbin/service aesvcs restart`.

## Reassigning Cdom and SAL Gateway IP addresses onsite

Perform this task when a System Platform upgrade can be performed at the customer site. In this case, Avaya or Avaya Partner Support Engineering personnel are available onsite to assist with local (customer network) login to the Web Console for the server that you must upgrade.

### Before you begin

- If you are a customer of Avaya or an Avaya Partner and must upgrade to System Platform version 6.3 from a version earlier than 6.2, go to <http://support.avaya.com> and click on **Support Contact Options > Maintenance Support**.
- Complete the blank fields in the following table. The following steps reference either address "A" or "B", as appropriate.

**Table 4: Cdom IP address assignments (local procedure)**

<b>Current Cdom (avpublic) IP Address:</b>	A.
<b>New customer-provided IP address for Cdom:</b> (The new address for the cdom virtual machine must be on the same IP subnet used by the System Platform Domain 0 virtual machine. Verify using Linux <code>ipcalc</code> or similar tool.)	B.

- Support Engineers must have their Token (SecureID) USB device available for additional authentication.

## About this task

### Important:

If you are upgrading a System Platform High Availability configuration that uses the embedded SAL Gateway, complete Cdom and SAL Gateway IP address reassignments on the primary server only, and only after stopping High Availability. If you later have a High Availability failover event (triggered manually or automatically), the High Availability subsystem enables the Services VM on the standby server. The HA data replication software also automatically propagates the new Cdom and SAL Gateway IP addresses to the standby server.

## Procedure

1. Log on to the System Platform Web Console as `admin`.
2. Select **Server Management > Network Configuration**.
3. From the **Domain Network Interface** panel, under the **Console Domain**, note the **avpublic** IP address in preceding table, field "A".
4. Enter the new, customer-provided Cdom IP address (from the preceding table, field "B") into the Console Domain **avpublic IP** field.
5. Click **Save**.

Saving the change you made to the Cdom IP address configuration temporarily severs your secure connection to Cdom on the target server. However, the server continues to have connectivity and communication with the remote Avaya servers. (Your SAL Gateway 1.8 gracefully manages changes to the server's IP address configuration.)

6. Log on to the SAL Gateway user interface using the new Cdom IP address (`https://<new_Cdom_IP>:7443`) and update the Cdom managed element (VSPU) to match the value in the preceding table, field "B".
7. Log on to the System Platform Web Console as `admin` and check for errors.
8. Select **Server Management > Network Configuration**.
9. Verify that the Web Console displays the new Cdom IP address in the Console Domain **avpublic IP** field.
10. Restart AES DBService and aesvs:
  - a. Start an SSH session.
  - b. Log in to AES as administrator
  - c. Type `su -sroot`.
  - d. Enter the password for the sroot user.
  - e. Type `/sbin/service DBService restart`.
  - f. Type `/sbin/service aesvcs restart`.

---

# Upgrading System Platform

---

## Feature packs

Avaya delivers feature packs in either RPM (patch) or ISO (full upgrade) format. Install or uninstall them as follows:

- RPM patch—From the Patch Management page of the System Platform Web Console.
- ISO image—From the appropriate (System Platform or Avaya Aura® product) installation wizard.

Feature packs have installation requirements that vary, so always see your solution documentation for specific prerequisites and installation instructions.

### Guidelines for RPM-based feature packs

For any RPM-based System Platform feature pack, the following installation guidelines apply:

- If your server is already running the latest version of System Platform available, install the RPM patch containing the feature pack.
- If your server is not running the latest version of System Platform available:
  1. Upgrade to the latest version of System Platform (including service packs) available.
  2. Install the RPM patch containing the feature pack.

### Guidelines for ISO-based feature packs

For any ISO-based System Platform feature pack, only the following guideline applies:

- Use the feature pack ISO image to perform a platform upgrade on the server.

## Feature Pack installation process

If you are planning to install a new feature pack on your solution template, you must first meet System Platform requirements including platform upgrades, service pack installations, and any earlier feature packs if required. For example, with Communication Manager 6.0 running on System Platform 6.0, and with System Platform and Communication Manager each having a new FP1, the solution upgrade sequence is as follows:

1. Upgrade System Platform from version 6.0 to version 6.2.1.
2. Install RPM-based Feature Pack 1 for System Platform 6.2.1. This step brings System Platform to version 6.2.2.
3. Upgrade Communication Manager from version 6.0 to version 6.2.
4. Install Service Pack 4 for Communication Manager 6.2.

## High availability configurations

If you are deploying an Avaya Aura® system in a System Platform High Availability configuration, the same installation or upgrade sequence applies to both the primary and secondary servers in the configuration.

## Feature Pack installation

Use the installation method that is appropriate for the feature pack: RPM-based feature packs or ISO-based feature packs.

### RPM-based feature packs

For RPM-based feature packs (for example, Feature Pack 3, System Platform 6.3.4), see [Patch management](#) on page 93.

### ISO-based feature packs

For ISO-based feature packs (for example, Feature Pack 2, System Platform 6.3), perform a platform upgrade.

## Platform upgrade process in different System Platform deployments

This topic provides a summary of different System Platform deployments and, for each deployment, the platform upgrade process.

Deployment scenarios for the System Platform upgrade process are as follows:

- Simplex (single-server) deployment
- SAL Gateway configuration prior to System Platform upgrade:
  - Embedded SAL Gateway
  - Standalone SAL Gateway
- Primary server upgrade for System Platform HA
- Secondary (standby) server upgrade for System Platform HA
- Services Virtual Machine installed state after dual-server upgrade for System Platform HA

The following table summarizes deployment options and the outcomes to expect during and after a System Platform upgrade:

**Table 5: System Platform deployments and upgrade outcomes**

Server upgrade type	SAL Gateway type	Cdom and SAL Gateway address reassignment	Services Virtual Machine installed state after upgrade
Simplex (single-server)	Embedded gateway	Yes	Enabled, to support embedded SAL Gateway operation.

*Table continues...*

Server upgrade type	SAL Gateway type	Cdom and SAL Gateway address reassignment	Services Virtual Machine installed state after upgrade
Simplex (single-server)	Standalone gateway	No, but an IP address must be reserved for the location of the standalone gateway.	Disabled, since no requirement exists for operation of the SAL Gateway on the Services Virtual Machine.
Duplex (dual-server) for System Platform High Availability: <i>Primary server</i>	Embedded gateway	Yes	Enabled to support embedded SAL Gateway operation after platform upgrade.
Duplex (dual-server) upgrade for System Platform High Availability: <i>Primary server</i>	Standalone gateway	No, but an IP address must be reserved for the location of the standalone gateway.	Disabled, since no requirement exists for operation of the SAL Gateway on the Services Virtual Machine.
Duplex (dual-server) upgrade for System Platform High Availability support: <i>Secondary (standby) server</i>	Embedded gateway, but no System Platform HA configuration required on the secondary/standby server.	No. System Platform HA software activates the Services VM on the standby server and propagates the HA configuration (including use of the embedded SAL Gateway) to that server on automatic or manual failover.	Disabled until automatic or manual failover, when the Services Virtual Machine must support operation of the embedded SAL Gateway on the Services Virtual Machine.
Duplex (dual-server) upgrade for System Platform High Availability support: <i>Secondary (standby) server</i>	Standalone gateway, but no System Platform HA configuration required on the secondary/standby server.	No. System Platform HA data replication software automatically propagates the HA configuration (including use of the standalone SAL Gateway configuration) to the standby server on automatic or manual failover.	Remains disabled after automatic or manual failover, since no requirement exists for operation of the embedded SAL Gateway on the Services Virtual Machine.

### Related links

[SAL deployment on the Services Virtual Machine](#) on page 144

## Upgrading a System Platform server

This is a procedure for performing a full platform upgrade on your System Platform server, from an earlier version to a later version of the System Platform software. You can also use this procedure to install new feature pack software offered only in ISO format, since this scenario also follows the full

platform upgrade process. Use standard patch management procedures to install any feature pack software offered only in RPM (patch) format.

### Before you begin

- Perform all preupgrade tasks that are listed in [Preupgrade checklist](#) on page 155.
- If you are upgrading two servers supporting a System Platform High Availability configuration, **Stop HA** and then **Remove HA** on the Primary server. System Platform does not support platform upgrades while High Availability is running. If you attempt an upgrade while High Availability is running, a warning message appears and the system prevents you from performing the upgrade.

### Procedure

1. Log in to the Web Console for the primary (if HA) or standalone (if non-HA) System Platform server.
2. Click **Server Management > Platform Upgrade** in the navigation pane.  
The Server Management Platform Upgrade page appears.
3. In the **Upgrade Platform From** field, select the location of the software to be installed.

 **Note:**

If the software is located on a different server (for example, Avaya PLDS or HTTP), and depending on your specific network environment, configure a proxy if necessary to access the software. See [Configuring a proxy](#) on page 117.

4. If you selected **HTTP** or **SP Server** in the **Upgrade Platform From** field, enter the complete URL or path of the platform upgrade files.
5. Click **Search**.  
The system searches the location that you specified for an upgrade description file that has an .ovf extension.
6. Select the VSP description file for the platform upgrade, and then click **Select**.  
The system displays the version and additional information for the current and the new platform on the Platform Upgrade Details page.
7. On the Platform Upgrade Details page, click **Upgrade**.

 **Important:**

As part of the upgrade process, the System Domain (Domain-0) and Console Domain virtual machines will reboot.

8. Click **OK** when prompted to confirm that the template has been qualified for the platform version to which you are upgrading, and that both the System Platform Web Console and Console Domain will reboot upon completion of the upgrade .
9. Click **OK** when prompted to confirm the upgrade.

At this stage, the upgrade process starts and the system displays the Platform Upgrade workflow status page.



**\* Note:**

The System Domain (Domain-0) and Console Domain reboot at this stage. For this reason, the Platform Upgrade workflow status page does not show any updates until it reboots in the new Console Domain. After the Web Console is up, the system automatically redirects you to the login page. This routine can take approximately 20 minutes.

10. Log in to the System Platform Web Console.

**\* Note:**

You are allowed a 4-hour period to log in to the System Platform Web Console. If you do not login during this period, the system will reboot using the previous release of System Platform. If a user logs in to System Platform Web Console within the 4-hour period, it is assumed that System Platform is reachable and the timer is cancelled.

11. Before electing to commit or roll back the platform upgrade, complete the procedure for verifying an upgrade.
12. On the Commit or Rollback platform upgrade page, perform the procedure to either commit the upgrade or rollback the upgrade.
13. If you elected to commit the upgrade and the system finishes rebooting automatically, log on to the upgraded server's Web Console.
14. Select **SAL Gateway Management**.

**\* Note:**

If your network includes a standalone SAL gateway, the platform upgrade leaves the embedded SAL Gateway disabled on the local Services Virtual Machine. You must administratively configure the details of the standalone server and then enable the SAL gateway to run on that server.

15. Click **Enable SAL Gateway**.
16. Click **Launch SAL Gateway Management Portal**.  
The Avaya SAL Gateway user interface appears.
17. Log on to the SAL Gateway user interface.  
The default username is `admin`; the default password is `admin01`.
18. Click **Administration > Service Control & Status**.  
The Gateway Service Control window opens.
19. Click **Check Health for the Gateway** on the Gateway Service Control page.

This action displays results of a final check for proper SAL Gateway operation and communication with Avaya remote servers.

This completes the System Platform upgrade procedure.

## Related links

[System Platform upgrades on High Availability systems](#) on page 144

[Verifying an upgrade](#) on page 170

[Commit and Rollback](#) on page 172

[Upgrading System Platform on both servers](#) on page 177

---

## Verifying an upgrade

### Before you begin

You have performed all of the platform upgrade steps leading up to, but not including, the commit or rollback step. Before returning to commit or rollback and then finishing the procedure for [Upgrading a System Platform server](#) on page 167, you must first complete all of the checks in the following procedure successfully.

### About this task

This procedure helps to verify certain key indications of a successful platform upgrade, for example:

- the new System Platform version running on the server
- the presence and versions of virtual machines required for your Avaya Aura® solution
- networking and user configuration capabilities
- Network Time Protocol (NTP) configuration

### Procedure

1. Log on to the Web Console as **admin**.

You should see the **Commit/Rollback** page, which verifies:

- The server successfully booted up to the new platform version.
- No image or kernel faults occurred during the upgrade. Otherwise, System Platform automatically rolls back into its prior version and the **Rollback Acknowledge** page appears.
- No problems occurred in LDAP storage.

2. Go to **Server Management > System Configuration** in the Web Console and verify that all the system configuration information is accurate before committing the upgrade.

This action performs a quick check for accuracy of system configuration information carried forward during the platform upgrade.

3. On the **Virtual Machine Management** page, verify that the Domain-0 and Console Domain (cdom) versions are identical to the version of your System Platform upgrade (6.3 or later).
4. Use SSH to log on to Dom-0 and Cdom as an advanced administrator (**admin**) and run the `swversion` command.

The command output should verify the new System Platform version (6.3 or later).

5. If an administrator installed a solution template before performing the System Platform upgrade, use the Web Console to verify that all virtual machines for the installed template are visible and accessible. (Click on the virtual machine links and verify their version labels.)
6. Go to **Server Management > Date/Time Configuration** in the Web Console and verify that the Date and time are correct as configured prior to the upgrade (manual date/time setting or configured to synchronize with an NTP server at a specific IP address).

This action performs a quick sanity check on the NTP protocol, date, and time configuration.

7. Go to **Server Management > Backup/Restore > Restore** in the Web Console and note the latest backup information.

A successful backup during platform upgrade should result in a file visible at this location. As such, this action performs a quick sanity check on System Platform backup/restore functionality.

8. Go to **Server Management > Network Configuration** in the Web Console and verify that all network configuration values are correct as configured.

This action performs a quick validation of the System Platform networking setup.

9. If possible at this time, go to **User Administration > Local Management** in the Web Console, and then click **Create User** to create a test user.

10. **Delete** the test user.

The last two steps together perform a quick check for user administration functionality.

11. Go to **Server Management > SAL Gateway Management** in the Web Console.

If you chose **Enable Services VM** during the platform upgrade procedure, the SAL Gateway should be running. Otherwise (if you deploy the SAL Gateway on a separate stand alone server), the embedded SAL Gateway should be stopped. This action verifies availability of the SAL Gateway running on the Services Virtual Machine.

12. Go to **Server Management > SNMP Trap Receiver Configuration** in the Web Console and verify that all the SNMP trap receivers configured before the platform upgrade have been carried forward into the new version of System Platform.

The upgrade process automatically adds a trap receiver of 127.0.0.1 if the Services Virtual Machine is, by default, still enabled. Otherwise, you must add trap receiver destinations corresponding to Network Management Systems in your own network, including one for an external SAL Gateway.

13. Trigger a test alarm from the Cdom Command Line Interface (CLI) and verify that all configured SNMP trap receivers did receive the alarm.

The last two steps together perform a quick check for SNMP trap receiver functionality.

14. Go to **Server Management > License Management** in the Web Console and launch the **WebLM License Manager**.

15. Log in to WebLM portal to verify that all template virtual machine license files are still valid.

The last two steps together perform a quick check on WebLM functionality in the new version of System Platform.

16. Return to step [12](#) on page 169 of [Upgrading a System Platform server](#) on page 167

### Related links

[Upgrading a System Platform server](#) on page 167

---

## Commit and Rollback

System Platform upgrades must be committed before performing other operations, including installation of patches. During an upgrade, after the system boots in the new platform release, the user is required to commit or rollback the upgrade. While the system is waiting for the user to either commit or rollback, Avaya advises not to perform any of the following operations:

- Delete a template
- Install a template
- Upgrade a template
- Reboot the System Platform Web Console

**\* Note:**

Rebooting System Platform Web Console before committing will roll back the system to the previous release.

- Install or remove a patch
- Start High Availability operation

### Commit

You can commit an upgrade when you are satisfied that the new System Platform software is working without any issues. After committing an upgrade, you cannot go back to the older version of the System Platform software. If you do not log in to System Platform Web Console within 4 hours after the upgrade, the system performs an automatic rollback.

The system performs the following when you commit an upgrade:

- Performs a clean up operation (such as, removing state files and so on).
- Commits boot loader (grub) to boot up into the new platform from now on.
- Marks the Workflow as complete and indicates that on the Platform Upgrade Status page.

### Rollback

You can perform a rollback operation if you find any errors or issues with the new System Platform software and must go back to the older version of software. Rollback reboots the server.

The system performs the following when you roll back an upgrade:

- Performs a clean up operation (such as, removing state files and so on).
- Prepares the system to notify the user of the reason for rollback after rebooting into the old platform.

- Reboots the platform to boot up into the old platform and restores access to System Platform Web Console.

### Related links

[Upgrading a System Platform server](#) on page 167

---

## Committing an upgrade

### Procedure

On the Commit or Rollback platform upgrade page, click **Commit** to continue the platform upgrade process.

---

## Rolling back an upgrade

### Procedure

On the Commit or Rollback platform upgrade page, click **Rollback** to cancel the upgrade process and go back to the previous version of the software.

#### **Note:**

After a rollback, when you log on to the System Platform Web Console, the system displays the Rollback Acknowledge page that specifies the reason for rollback (either user initiated rollback or deadmans switch) based Auto rollback; or if the upgrade failed and the system rebooted to an older version of System Platform as part of fail-safe fallback mechanism.

---


## Platform Upgrade field descriptions

Name	Description
Upgrade Platform From	<p>Lets you specify the location from where to download or upload the template image files for the platform upgrade.</p> <p>Options are:</p> <ul style="list-style-type: none"> <li>• <b>Avaya Downloads (PLDS)</b> The files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password.</li> <li>• <b>HTTP</b> The files are located on an HTTP server. You must specify the URL of the platform upgrade if you select this option.</li> </ul>


*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• <b>SP Server</b> The platform upgrade files are located in the / <code>vsp-template</code> directory in the System Platform Console Domain. You must copy the platform upgrade files in this directory using a file transfer program and change their permissions as follows: <code>chmod 644 &lt;files-copied&gt;</code></li> <li>• <b>SP CD/DVD</b> The files are located in a CD or DVD.</li> <li>• <b>SP USB Device</b> The files are located on a USB flash drive. This option is:                             <ul style="list-style-type: none"> <li>- supported for RPM patch upgrades not exceeding the storage capacity of the flash drive.</li> <li>- not supported for full-platform (ISO) upgrades to System Platform 6.2 or later.</li> </ul> </li> </ul>
<b>SSO Login</b>	Single Sign-On username required when the <b>Upgrade Platform From</b> source is <b>Avaya Downloads (PLDS)</b> .
<b>SSO Password</b>	Single Sign-On password required when the <b>Upgrade Platform From</b> source is <b>Avaya Downloads (PLDS)</b> .
<b>Platform Upgrade URL</b>	URL required when the <b>Upgrade Platform From</b> source is either <b>HTTP</b> or <b>SP Server</b> .

**Button descriptions**

Button	Description
<b>Search</b>	<p>Searches for a template description file that has an .ovf (Open Virtualization Format) extension at the location that you specify.</p> <p>Opens the Platform Upgrade Details page with the search results.</p> <p> <b>Note:</b> Open virtualization format (OVF) is an open standard for packaging and distributing software that runs on virtual machines.</p>
<b>Configure Proxy</b>	Redirects to the System Configuration page after clicking <b>Search</b> , enabling you to configure a proxy server (if needed) to reach the <b>Avaya Downloads (PLDS)</b> server, an <b>HTTP</b> server, or a System

*Table continues...*

Button	Description
	Platform server ( <b>SP Server</b> ) chosen as the source for platform upgrade file downloads.
<b>Select</b>	Selects the template description file you require to upgrade your system. (You identified the file after searching your upgrade file source: (PLDS, HTTP, or SP Server).
<b>Upgrade</b>	Upgrades the system with the template description file you selected after searching your upgrade file source (PLDS, HTTP, or SP Server).
<b>Commit</b>	Commits an upgrade operation and upgrades the System Platform software to the latest version.   <b>Note:</b> After executing a commit operation, you cannot go back to the older version of the System Platform software. If you do not execute a commit operation within 4 hours after the upgrade, the system performs an automatic rollback.
<b>Rollback</b>	Cancels an upgrade operation, and the system goes back to the previous version of System Platform software.
<b>Acknowledge</b>	Lets you confirm the reason for the rollback operation.

---

## Upgrading System Platform on High Availability Systems

---

### High Availability during platform upgrades

System Platform does not support platform upgrades while High Availability is running. You must first go to the primary server Web Console > High Availability page and **Stop HA**. If you attempt an upgrade while High Availability is running, a warning message appears and the system prevents you from performing the upgrade.

 **Important:**

To proceed with the upgrade, you must additionally **Remove HA** from the primary server.

---

## Installing System Platform patches on High Availability systems

### About this task

Before downloading any patch, be sure to check its description in the Release Notes. When indicated by the patch description, you must install patches on both the primary and secondary servers independently. The primary server does not automatically replicate patches to the secondary/standby server.

See the separate procedures for stopping, removing, and starting System Platform High Availability as needed during this procedure.

### Procedure

1. Log in to the Web Console of the server chosen to be the preferred node.
2. Click **Server Management > High Availability**.
3. Click **Stop HA** and confirm the displayed warning.
4. If the server restarts after stopping HA, log on to the Web Console of the preferred node and **Remove HA**.
5. Apply patches in the required sequence to the preferred node.
6. Log on to the Web Console of the standby node.
7. Apply the same patches that were applied to the preferred node.

### Related links

- [Starting System Platform High Availability](#) on page 113
- [Stopping System Platform High Availability](#) on page 114
- [Removing the High Availability configuration](#) on page 115
- [Installing patches](#) on page 96
- [Starting System Platform High Availability](#) on page 113
- [Removing the High Availability configuration](#) on page 115
- [Stopping System Platform High Availability](#) on page 114

---

## Removing the High Availability configuration

Use this procedure to permanently remove the High Availability configuration.

### Before you begin

- You have stopped System Platform High Availability.



## About this task

Use this procedure, for example:

- to remove the HA configuration from Avaya Aura® solution servers before a System Platform upgrade. Removing the HA configuration from the primary/active HA server also removes the HA configuration from the standby server automatically.
- to restore Avaya Aura® solution servers in an HA configuration to simplex operation

## Procedure

1. Log on to the Web Console for the primary/active HA server.
2. Click **Server Management > High Availability**.
3. Click **Remove HA** and confirm the displayed warning.

## Related links

[Upgrading System Platform on both servers](#) on page 177

[Installing System Platform patches on High Availability systems](#) on page 97

[Starting System Platform High Availability](#) on page 113

[Stopping System Platform High Availability](#) on page 114

---

# Upgrading System Platform on both servers

## Before you begin

- Have a record of settings for your current High Availability configuration.
- Stop High Availability on the primary node.
- Remove High Availability on the primary node.
- Complete all System Platform preupgrade tasks. See [Preupgrade checklist for System Platform on High Availability systems](#) on page 157.

## About this task

This is a high-level procedure for sequential upgrade of two System Platform servers deployed in a Locally Redundant High Availability configuration. As such, use this procedure with its companion topics, [Upgrading a System Platform server](#) on page 167 and [Verifying an upgrade](#) on page 170, where indicated.

## Procedure

1. Log on to the System Platform Web Console for the primary node.
2. Go to the Platform Upgrade page and start the upgrade procedure for the primary node.  
See [Upgrading a System Platform server](#) on page 167.
3. Upon completion of the platform upgrade procedure, go to the **Server Management > Patch Management** page and apply to the primary node any post-upgrade System Platform patches specified in your solution upgrade documentation.
4. Log on to the Web Console on the standby node.

5. Go to the Platform Upgrade page and start the upgrade procedure for the standby node.
6. When the Services VM Network Configuration window appears at the beginning of the System Platform upgrade *for the standby server*, clear the **Enable Services VM** check box to ensure that you install the Services VM in a disabled state.

If a failover occurs later when the High Availability system is running, High Availability activates the Services VM on the former standby (now active) server, propagates the current Services VM configuration to that server, and deactivates the Services VM on the former active (now standby) server.

7. Upon completion of the platform upgrade procedure, go to the **Server Management > Patch Management** page and apply to the standby node any post-upgrade System Platform patches specified in your solution upgrade documentation.
8. Log on to the Web Console of the primary node.
9. Navigate to the High Availability page.
10. Reenter your System Platform High Availability configuration.
11. **Save** the HA configuration
12. **Restart HA** from the High Availability page of the Web Console for the primary node.

**\* Note:**

Platform upgrade must be performed on each server separately. A difference of version between the servers (including patches) will prevent System Platform High Availability from starting after you finish upgrading both servers.

**\* Note:**

After finishing a System Platform upgrade, you have 4 hours to log into the Web Console again. Otherwise, the platform upgrade automatically rolls back to the prior platform version. This is a scenario more common with High Availability configurations.

### Related links

[System Platform upgrades on High Availability systems](#) on page 144

[Starting System Platform High Availability](#) on page 113

[Stopping System Platform High Availability](#) on page 114

[Upgrading a System Platform server](#) on page 167

[Removing the High Availability configuration](#) on page 115

---

## Starting System Platform High Availability

This procedure synchronizes all required configuration settings from the preferred node to the standby node so that the standby node can assume the role of active node if required.

## About this task

Whether you have completed a new System Platform installation or a System Platform upgrade, your Avaya Aura solution documentation should indicate which of the two High Availability servers will be the preferred node. You must **Start HA** from that node.

### ! Important:

If you are performing a platform upgrade, do not start High Availability operation until after you commit the platform upgrade on both the primary and secondary servers.

### \* Note:

- If you are restarting Fast Reboot High Availability (FRHA) operation after performing **Stop HA**, you can restart anytime after FRHA halts.
- If you are restarting Machine Preserving (and implicitly, Live Migration) High Availability (MPHA/LMHA) after performing **Stop HA**, you can restart anytime after MPHA/LMHA halts.

### \* Note:

When starting HA, System Platform removes all bonded interfaces defined earlier on the standby node, but then automatically propagates (duplicates) all bonded interfaces defined on the active node to the standby node. This operation assures that both nodes have the same bonded interface configuration after HA startup.

## Procedure

1. Click **Server Management > High Availability**.
2. Click **Start HA** and confirm the displayed warning.
3. Click **Server Management > High Availability**.

Verify the progress of virtual machine replication on the High Availability page.

## Related links

[High Availability start/stop](#) on page 113

[Upgrading System Platform on both servers](#) on page 177

[Installing System Platform patches on High Availability systems](#) on page 97

[Removing the High Availability configuration](#) on page 115

[Stopping System Platform High Availability](#) on page 114

---

# Postupgrade tasks

---

## SNMP configuration overview

Services-VM can support either SNMP v2c or SNMP v3 for SAL Gateway. Services-VM is configured for SNMP v3 by default. You can change the configuration to support the required SNMP version.

The system preserves the SNMP configuration, either v2c or v3, from the earlier version of Services-VM during the upgrade of Services-VM.

Services-VM contains two files, `snmpv2c.conf` and `snmpv3.conf`, for SNMP v2c configuration and SNMP v3 configuration respectively. Based on the SNMP version you want to support, you must use one of the two files for SNMP configuration. The files contain the following default values that you must replace with actual values after consulting with your network administrator.

File	Parameter	Default value
<code>snmpv2c.conf</code>	Community string	avaya123
<code>snmpv3.conf</code>	User name	initial
	Authentication protocol	MD5
	Authentication password	avaya123
	Privacy protocol	Data Encryption Standard (DES)
	Privacy password	avaya123

## Configuring SNMP version support on the Services VM

### Before you begin

You must have:

- Root level access to the Linux command line on the Services virtual machine
- The default community string for SNMPv2c: avaya123
- The default user string for SNMPv3: initial
- The SNMPv3 password: avaya123

After successfully configuring SNMP version support on the System Platform server, use the SNMP community, user, and password strings to perform services-specific operations (for example, SNMP querying) on the Services VM.

### About this task

Use the following steps to change the Net-SNMP Master Agent configuration on the Services virtual machine. You change the Master Agent configuration to match the version of SNMP (v2c or v3) required by your NMS.

For upgrades to System Platform 6.3, this task is required only if you are upgrading from System Platform 6.0.3. If you are upgrading from System Platform 6.2 or later, the existing Net-SNMP Master Agent configuration is preserved.

### Procedure

1. Open an SSH session to log on to the Services VM as `root`.
2. Change the current directory to `/etc/snmp`.
3. Find the `snmpd.conf` file.
4. Check the version of `snmp<v2c | v3>.conf` linked to the file `snmpd.conf`.

For example:

```
# ls -l
lrwxrwxrwx 1 root root 11 Jul 19 20:35 snmpd.conf -> snmpv3.conf
-rw-r--r-- 1 root root 77 Jun 28 11:54 snmpv2c.conf
-rw-r--r-- 1 root root 72 Jun 28 11:54 snmpv3.conf
```

5. If the `snmpd` service is active, run the following command to stop the service:

```
/sbin/service snmpd stop
```

6. Run the following command to back up the file `snmpd.conf` :

```
cp snmpd.conf snmpd.conf.bak
```

7. Run the following command to remove `snmpd.conf`:

```
rm -f snmpd.conf
```

8. Run one of the following commands to create a soft link to the SNMP version you want to support:

To configure the Master Agent for SNMP v3:

```
ln -s snmpv3.conf snmpd.conf
```

To configure the Master Agent for SNMP v2c:

```
ln -s snmpv2c.conf snmpd.conf
```

9. Run the following command to start the `snmpd` service:

```
/sbin/service snmpd start
```

---

## Licensing change in System Platform 6.3.4

In System Platform 6.3.4, WebLM 6.3.4 supports only license files that are generated using the primary host ID. The primary host ID is the MAC address of System Domain (Domain 0) and physical port eth0 of the server. Other host IDs on the system are no longer displayed on the Server Properties page and are not supported for license installation. If an administrator has generated a license using any ID other than primary host ID, then after upgrade to WebLM 6.3.4 in System Platform 6.3.4, the license will continue to work but should be regenerated using the primary host ID. Any licenses that were generated using the Console Domain MAC address should be regenerated using the Domain 0 MAC address (the primary host ID).

For information on how to generate a license for System Platform, see *Installing and Configuring Avaya Aura® System Platform*.

## Password hashing

Beginning in System Platform 6.3.1, SHA2 is used for hashing of user passwords instead of MD5. When the upgrade to System Platform 6.3 is complete, users must change their existing passwords for SHA2 hashing to take effect. MD5 hashes are retained until users change their passwords. If the 6.3 patch is removed, previous users and passwords are restored, and any new users that were created in 6.3 are removed.

---

## Upgrading the Services virtual machine

---

### Upgrade of the Services virtual machine

After upgrading to System Platform 6.3.1 or higher, you must upgrade the Services VM to version 3.0. System Platform 6.3 includes Services VM version 2.0.

Perform this upgrade during a maintenance window.

Upgrading the Services virtual machine includes the following tasks:

1. [Upgrading Services-VM on System Platform](#) on page 182
  2. [Verifying Services-VM installation and upgrade](#) on page 186
  3. [Committing the template upgrade](#) on page 188
- 

## Upgrading Services-VM on System Platform

Services-VM 3.0 supports direct upgrade from versions 1.0.x and 2.0.

After System Platform installs Services-VM for the first time, you must maintain Services-VM in the same way as a solution template. Services-VM follows the same methods for announcements, distribution, and installation of a solution template. You must apply the Services-VM upgrades only through the System Platform Web Console, in the same way as for all other solution templates.

### **Caution:**

Never directly upgrade Avaya Diagnostic Server and the components that are running on Services-VM. You must upgrade Avaya Diagnostic Server and the components on Services-VM only through the Services-VM upgrade process.

### **Important:**

You must perform backup and restore operations of the Avaya Diagnostic Server components, such as SAL Gateway, on Services-VM through the integrated Backup and Restore features on the System Platform Web Console. The Services-VM upgrade process does not save the

backup archives that you create locally on Services-VM by using the backup features of Avaya Diagnostic Server components.

### About this task

The Services-VM upgrade procedure is similar to the upgrade procedure of other solution templates on System Platform. This section mainly describes the steps that you must do differently for Services-VM from a template upgrade. For more information about upgrading a solution template, see *Upgrading Avaya Aura® System Platform*.

### Procedure

1. Log on to the System Platform Web Console as an administrator.
2. If you have an ISO image for the Services\_VM upgrade, write the ISO image to a DVD, and insert the DVD in the System Platform server CD-ROM or DVD drive.

**!** **Important:**

The preferred method for upgrading Services-VM is to write the ISO image to a DVD and then choosing the **CD/DVD** option to install the template.

3. If you have an ISO image but do not have physical access to the server, perform the following steps.

**!** **Important:**

You must perform the following steps as the root user. Perform all operations carefully. The incorrect use of the root account might affect the performance of the system.

- a. Transfer the Services-VM image file to the cdom virtual machine as the admin user.

You can use the `scp` command to copy the file from a Linux system to the remote virtual machine. To copy the file from a Windows system, you can use WinSCP or a similar file transfer tool.

- b. Establish an SSH session to cdom as the root user.
- c. Create the mount directory for the image file of Services-VM.

For example:

```
mkdir /mnt/Services_VM
```

- d. Change the directory to the location where you copied the image file.
- e. Mount the image file on the mount directory that you created earlier.

For example:

```
mount -o loop Services_VM-3.0.0.0.X.iso /mnt/Services_VM
```

- f. Copy the folder where you mounted the ISO image to the `/vsp-template` folder.

For example:

```
cp -r /mnt/Services_VM /vsp-template/
```

- g. List the files in the `/vsp-template/Services_VM` folder to check that the copy operation is successful.

The following is a sample output of the `ls` command for the `/vsp-template/Services_VM/` folder:

```
ls -l /vsp-template/Services_VM/
```

```
total 839000
-r----- 1 tomcat tomcat      5811 Aug 27 18:20 backup_sdom.sh
-r----- 1 tomcat tomcat      2507 Aug 27 18:20 index.html
-r----- 1 tomcat tomcat     12090 Aug 27 18:20 patch_sdom.sh
-r----- 1 tomcat tomcat      4084 Aug 27 18:20 resizeVM.sh
-r----- 1 tomcat tomcat 858218207 Aug 27 18:21 services_vm.gz
-r----- 1 tomcat tomcat     12316 Aug 27 18:21 Services_VM_Medium.ovf
-r----- 1 tomcat tomcat        522 Aug 27 18:21 Services_VM.mf
-r----- 1 tomcat tomcat     12270 Aug 27 18:21 Services_VM_Small.ovf
-r----- 1 tomcat tomcat     4448 Aug 27 18:21 srvcs-vm-srvc-control.sh
-r----- 1 tomcat tomcat      2673 Aug 27 18:21 versioninfo_sdom.sh
```

- h. Unmount the image file.

For example:

```
umount /mnt/Services_VM
```

- i. Remove the folder that you created for mounting the ISO image.

For example:

```
rm -rf /mnt/Services_VM
```

4. In the left navigation pane of the System Platform Web Console, click **Virtual Machine Management > Templates**.

The Search Local and Remote Template page displays the Services-VM version and the solutions templates installed on System Platform.

5. Click **Upgrade** next to the Services-VM version installed.
6. In the **Install Template From** field, select the location from where the system must install the Services-VM upgrade. Follow the same steps as you do to search and select a template for upgrade in System Platform.

If you copied the ISO image file for Services-VM to the server, select **SP Server**.

If you wrote the ISO image to a DVD and inserted the DVD to the server CD or DVD drive, select **SP CD/DVD**.

7. Select the appropriate Open Virtualization Format (OVF) file for Services-VM according to your common release server.

The following table lists the OVF file that you must select depending on the common server release.

Common server release	OVF file
R1	Services_VM_Small.ovf
R2	Services_VM_Medium.ovf



The Template Details page displays the version and additional information about the current and the new template for Services-VM.

8. Select the check box next to the **Normal** configuration, and click **Install**.

The Template Network Configuration page displays the general network settings for Services-VM.

9. Click **Save**.

The Template Details page displays the default values for Services-VM.

10. If required, change the default values.

11. Click **Install**.

The upgrade process starts and the Template Installation page displays the progress of the upgrade process.

 **Note:**

As part of the upgrade process, the system stops Services-VM at this stage, which results in termination of the SAL Gateway services running on Services-VM. The temporary termination of the services causes termination of all established connections to SAL Gateway and might result in product alarms being missed. If you have connected to the System Platform Web Console remotely through the SAL Gateway that is on board, the system logs you off from the Web Console at this stage. The Services-VM upgrade process continues in the background until all tasks in the upgrade process are complete.

 **Note:**

The first task in the process, downloading the disk image for Services-VM, might take varied amount of time to complete. The completion time depends on the location of the server from which you download the template and the network quality, such as bandwidth and traffic. The other tasks take approximately 20 minutes to complete.

12. Log on to the System Platform Web Console to check the progress of the upgrade process.

After the completion of the upgrade tasks, the Template Installation page displays two buttons, **Commit Installation** and **Rollback Installation**.

13. Verify the upgrade, and perform one of the following actions:

- Click **Commit Installation** to apply the newly upgraded Services-VM.
- Click **Rollback Installation** to cancel the upgrade process and return to the previous version of Services-VM.

 **Important:**

You must log on to the Web Console within *4 hours* of the completion of the upgrade tasks and commit the upgrade process. Otherwise, the system cancels the upgrade process and automatically rolls back to the previous version of Services-VM.

## Related links

[Starting System Platform High Availability](#) on page 113

[Stopping System Platform High Availability](#) on page 114

---

# Verifying the Services-VM installation and upgrade

## About this task

After installing or upgrading Services-VM, you must perform the following steps to verify whether the system is functional.

## Procedure

1. On the System Platform Web Console, click **Virtual Machine Management > Manage**.
2. On the Virtual Machine List page, verify the following:
  - Verify that `services_vm` is present in the list of virtual machines.
  - Verify that the state for `services_vm` is **Running**.
  - If SAL Gateway is enabled on Services-VM, verify that the application state for `services_vm` is **Running**.
3. If SAL Gateway is disabled, enable SAL Gateway from the System Platform Web Console.

 **Note:**

If SAL Gateway was disabled on Services-VM before the upgrade, SAL Gateway remains disabled after the upgrade. You cannot open the SAL Gateway user interface unless you enable SAL Gateway on Services-VM.

4. Perform the following steps to verify that all SAL Gateway services are running:
  - a. Log in to the SAL Gateway UI.
  - b. Click **Administration > Service Control & Status**.
  - c. On the Gateway Service Control page, click **Check Health for the Gateway**.
  - d. When the system completes the check, verify that all services listed under **Gateway Services** are running as indicated by a green check mark.

 **Note:**

For more information, see *Checking the status of SAL Gateway* and *Troubleshooting for SAL Gateway diagnostics* in *Administering Avaya Diagnostic Server for SAL Gateway 2.2*.

5. Perform the following actions to verify that all SLA Mon™ services are running:
  - a. Log in to Services-VM as an administrator user, and change the user to root.
  - b. Change the directory to `/opt/services_vm`.
  - c. If SLA Mon™ is enabled on Services-VM, run the following command to verify that the application state for SLA Mon™ is **Running**:

```
./application_control.sh slamon -status
```

### Next steps

Enable SLA Mon™ on Services-VM. After the Services-VM upgrade, the SLA Mon™ services are in the Stopped state by default. You cannot start SLA Mon™ Server unless you enable the SLA Mon™ technology on Services-VM.

#### Caution:

You must create a new backup point for Services-VM from the System Platform Web Console after a successful upgrade to Services-VM 3.0. The system might not restore some configurations when you use the earlier backups taken with Services-VM 1.0 or 2.0.

---

## Enabling SAL Gateway

### About this task

Using the System Platform Web Console, you can enable the SAL Gateway hosted on Services-VM.

When System Platform installs Services-VM for the first time, the SAL Gateway residing in Services-VM is not enabled by default. To avail the SAL alarming and remote access services through the SAL Gateway on Services-VM, you must enable SAL Gateway.

#### Important:

To enable the SAL Gateway services, ensure that Services-VM is already enabled on System Platform. See [Enabling Services-VM](#) on page 188.

### Procedure

1. Log on to the System Platform Web Console as an administrator.
2. Select **Server Management > SAL Gateway Management** in the navigation pane.



Figure 1: SAL Gateway Management page

3. On the SAL Gateway Management page, click **Enable SAL Gateway** if it is displayed. If **Disable SAL Gateway** is displayed, SAL Gateway is already enabled.

 **Note:**

If you have already enabled SAL Gateway, the SAL Gateway Management page displays the **Disable SAL Gateway** button.

---

## Committing the template upgrade

### Procedure

When the upgrade is complete, click **Commit Installation** on the Template Installation page. Or, to cancel the upgrade and revert to the previously installed software version, click **Rollback Installation**.

---

## Enabling Services-VM

### About this task

To avail the Avaya Diagnostic Server features, including the SAL alarming and remote access services, through the SAL Gateway residing in Services-VM, you must enable Services-VM. If you did not enable Services-VM during a platform upgrade or a fresh installation of System Platform, you can enable Services-VM using the System Platform Web Console.

 **Caution:**

Do not change any network settings on the Network Configuration page while enabling or disabling Services-VM. If you need to make any network configuration change, first save the enabling or disabling action and then navigate back to the Network Configuration page to make further changes.

### Procedure

1. Log on to the System Platform Web Console as an administrator.
2. In the navigation pane, click **Server Management > Network Configuration**.
3. On the Network Configuration page, navigate to the **Solution Template - ServicesVM** section, which displays the configuration parameters for Services-VM.
4. In the **Solution Template - ServicesVM** section, select the **Enable Services VM** check box.
5. Click **Save**.

## Upgrading the standby and active servers when Geographical Redundancy High Availability feature is enabled

### About this task

You can use this procedure to upgrade the standby and active servers, when the AE Services server is upgraded and Geographical Redundancy High Availability (GRHA) is enabled.

### Procedure

1. Perform a backup of the AE Services server data for the active server.
2. Using the AE Services Management Console, stop High Availability on the active server.
3. Upgrade the standby AE Services server.
4. Upgrade the active AE Services server.
5. Restore the data for the active AE Services server.
6. Using the AE Services Management Console, start High Availability on the active server.

# Chapter 14: Upgrading Application Enablement Services

---

## Upgrading Application Enablement Services template

### About this task

Use this procedure to upgrade from an earlier version of AE Services.

**\* Note:**

If you are upgrading from AE Services 6.1.x, 6.2, 6.3, or 6.3.1 and you already have a license, you do not need another license file. The 6.1.x, 6.2, 6.3, or 6.3.1 license file is still valid. A new license file is required if you are upgrading from an earlier major release of AE Services (for example, AE Services 5.2.x).

**\* Note:**

If you have AE Services 6.3.0 or 6.3.1 installed and you want to upgrade to AE Services 6.3.3, you can install the AE Services 6.3.3 feature pack zip file instead of performing a template upgrade. You can install the AE Services 6.3.3 feature pack from either the System Platform Web Console or the AE Services shell console. You can install the AE Services 6.3.3 feature pack from either the System Platform Web Console or the AE Services shell console. To install the AE Services 6.3.3 feature pack from the System Platform Web Console, see [Using RPM Only installer for installing the Application Enablement Services 6.3.3 feature pack from the System Platform Web Console](#) on page 192. To install the AE Services 6.3.3 feature pack from the AE Services shell console, see [Using RPM Only installer for installing AE Services 6.3.3 feature pack from the AE Services shell console](#) on page 193.

### Procedure

1. On a Web browser, type the following URL: `https://ipaddress/webconsole`, where `ipaddress` is the IP address of the Console Domain that you configured during installation of System Platform.

**\* Note:**

This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

2. In the User ID box, enter `admin`.
3. Click **Continue**.
4. Enter the password for this account.

5. Click **Log On**.

If your system is configured with the High Availability Failover feature, go to step 6.

If the High Availability Failover feature is not configured, go to step 7.

## 6. If you are upgrading the AE Services template in the High Availability Failover configuration, you must stop High Availability Failover before upgrading the AE Services template. Do the following:

- a. Click **Server Management > Failover**.
- b. Click the **Stop Failover Mode** button.

7. Click **Virtual Machine Management > Solution Template**.

## 8. On the Search Local and Remote Template page, select a location from the list in the Install Template From box.

\* **Note:**

If the template installation files are located on a different server (for example, Avaya PLDS or HTTP), you may be required to configure a proxy depending on your network.

9. Click **Upgrade**.10. Click **OK** to confirm that you want to upgrade the template.11. On the Select Template page, click the **AES** template, and then click **Select**.

The system displays the current template installed. Do one of the following:

- If you have completed the AE Services Electronic Pre-installation Worksheet (EPW), go to Step 12.
- If you have not completed the AE Services Electronic Pre-installation Worksheet (EPW), click **Continue without EPW file**. The system displays the Template Details page with information on the AES template and its Virtual Appliances. Go to Step 13.

## 12. If you have completed the AE Services Electronic Pre-installation Worksheet (EPW), do the following:

- a. Click **Browse EPW File**.
- b. From the Choose File to Upload dialog box, select the EPW file, and click **Open**.
- c. Click **Upload EPW file**.

The system displays the Template Details page with information on the AES template and its Virtual Appliances.

13. On the Template Details page, click **Upgrade**.

The Template Installation page shows the status of the installation.

14. When **Commit Installation** and **Rollback Installation** buttons appear at the bottom of the page, do one of the following:

- Click **Commit Installation** to continue the upgrade process by committing to the newly upgraded template.

- Click **Rollback Installation** to cancel the upgrade process and go back to the previous version of the software.

---

## Using RPM Only installer for installing the Application Enablement Services 6.3.3 feature pack from the System Platform Web Console

### Before you begin

The AE Services 6.3.3 feature pack zip file consists of the RPMs required to apply the AE Services 6.3.3 updates to an installed AE Services 6.3.0 or 6.3.1 server

You can download the AE Services 6.3.3 feature pack from the following Web sites:

- [Avaya Support Web site](#)
- [Avaya Product Licensing and Delivery System \(PLDS\) Web site](#)

### About this task

Use this procedure to install the AE Services 6.3.3 feature pack from the System Platform Web Console.

### Procedure

1. On a Web browser, type the following URL: `https://ipaddress/webconsole`, where `ipaddress` is the IP address of the Console Domain that you configured during installation of System Platform.

 **Note:**

This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

2. In the User ID box, enter `admin`.
3. Click **Continue**.
4. Enter the password for this account.
5. Click **Log On**.

If your system is configured with the High Availability Failover feature, go to Step 6.

If the High Availability Failover feature is not configured, go to Step 7.

6. If you are upgrading the AE Services template in the High Availability Failover configuration, you must stop High Availability Failover before upgrading the AE Services template. Do the following:
  - a. Click **Server Management > Failover**.
  - b. Click the **Stop Failover Mode** button.



7. Download the AE Services 6.3.3 feature pack. For more information, see [Downloading patches](#) on page 95.

8. Click **Server Management > Patch Management**.

9. Click **Manage**.

The Patch List page displays the list of patches and the current status of the patches.

10. On the Patch List page, click on the patch ID to see the details.

11. On the Patch Details page, click **Install**.

12. Click **Server Management > Patch Management**.

13. Click **Manage**.

The Patch List page appears.

14. Click the AE Services 6.3.3 feature pack.

The Web Console displays the Server Management Patch Details page.

15. Click **Commit**.

The Server Management Patch Detail page displays an in-progress message. The Patch Detail page then displays a completion page.

---

## Using RPM Only installer for uninstalling the AE Services 6.3.3 feature pack from the System Platform Web Console

For steps to uninstall the AE Services 6.3.3 feature pack from System Platform Web Console, refer to [Removing patches](#) on page 99

 **Note:**

To update the feature patch in GRHA solution, start the uninstalling update on the active server. The update script automatically finds and updates the stand by server. After updating the stand by server, the update script finds and updates the active server.

---

## Using RPM Only installer for installing AE Services 6.3.3 feature pack from the AE Services shell console

### Before you begin

AE Services 6.3 or 6.3.1 must be installed.

## About this task

Use this procedure to install the AE Services 6.3.3 feature pack from the AE Services shell console. AE Services 6.3.3 feature pack consists of a ZIP file of RPMs.

You can download the AE Services 6.3.3 feature pack from the following Web sites:

- Avaya Support Web site: <http://www.avaya.com/support>
- Avaya Product Licensing and Delivery System (PLDS) Web site: <https://plds.avaya.com>.

## Procedure

1. From the AE Services Management Console, back up the server data before you install the feature pack.
2. Open an ssh session to the AE Services server and access an account with root privileges.
3. Download the AE Services 6.3.3 feature pack to the /tmp directory.
4. On the command line, type `cd /tmp`.
5. On the command line, type `update -u --force xxxx.zip` where `xxxx` is the name of the downloaded AE Services 6.3.3 feature pack ZIP file.

The system displays the feature pack ID and the RPMs contained in the package. The system then prompts you to confirm the installation of the RPMs.

- If you enter `y`, the installation of the feature pack proceeds. The system:
  - stops AE Services, Tomcat service, and DBService.
  - installs the RPMs contained in the feature pack.
  - restarts AE Services, Tomcat service, and DBService.
- If you enter `n`, the installation of the feature pack terminates.

---

## Using RPM Only installer for uninstalling AE Services 6.3.3 feature pack from the AE Services shell console

### About this task

Use this procedure to uninstall the AE Services 6.3.3 feature pack from the AE Services shell console.

#### Note:

To update the feature patch in GRHA solution, start the uninstalling update on the active server. The update script automatically finds and updates the stand by server. After updating the stand by server, the update script finds and updates the active server.

### Procedure

1. From the AE ServicesManagement Console, back up the server data before you install the feature pack.

2. Open an ssh session to the AE Services server and access an account with root privileges.
3. From the command prompt, type `swversion -a` to find the version of feature pack to remove.
4. At the command prompt, type `update -e feature pack version`.

The screen displays a list of all the RPMs to be uninstalled. The system prompts you for confirmation before it uninstalls these RPMs.

- If you enter `y`, the system uninstalls the feature pack. The system:
  - stops AE Services, Tomcat service, and DBService
  - rolls back to the previous feature pack.
  - restarts AE Services, Tomcat service, and DBService.
- If you enter `n`, the update script exits without uninstalling the feature pack.

# Chapter 15: Troubleshooting the installation

---

## Template DVD does not mount

The template DVD does not mount automatically.

---

### Troubleshooting steps

#### Procedure

1. Log in to the Console Domain as `admin`.
2. Enter `su -`
3. Enter the root password.
4. Run the following commands:

```
> ssh dom0.vsp /opt/avaya/vsp/template/scripts/udomAttachCd
> mount /dev/xvde /cdrom/
```

---

## Cannot ping Console Domain or get to the Web Console

Use this procedure to determine if the state of the Console Domain virtual machine is the reason why you cannot get to the System PlatformWeb Console.

---

### Troubleshooting steps

#### Procedure

1. Log in to the System Domain (Dom-0) as `admin`.
2. Enter `su -` to log in as root.
3. At the prompt, type `xm list`.

The `xm list` command shows information about the running virtual machines in a Linux screen.

You should see two virtual machines running at this time: System Domain (shown as `Domain-0`) and Console Domain (shown as `udom` in `xm list`).

A state of `r` indicates that the virtual machine is running. A state of `b` indicates that the virtual machine blocked.

**\* Note:**

The blocked state does not mean that there is a problem with the virtual machine. It only means that the virtual machine is currently not using any CPU time.

Other possible virtual machine states are:

- `p`: paused
- `s`: shutdown
- `c`: crashed

For more information on the information displayed, see the Linux manual page for the `xm` command.

4. On the Linux screen, type `exit` to log off as root. Type `exit` again to log off from System Domain (`Domain-0`).

### Example

#### `xm list` output:

Name	ID	Mem	VCPUs	State	Time (s)
Domain-0	0	512	2	r-----	60227.8
aes	15	1024	1	-b-----	12674.4
udom	16	1024	1	-b-----	9071.6
Domain-0	0	512	2	r-----	21730.2
aes		1024	1		2786.0
udom		1024	1		2714.1

---

## SAL does not work

SAL will not work until product registration is complete.

Complete product registration before proceeding with the troubleshooting steps.

## Troubleshooting steps

If the Secure Access Link (SAL) in your Avaya Aura solution is not operating normally, Avaya Support does not receive alarms and other important messages originating from the various components and applications in your system. Neither will Avaya Support be able to connect to your system for remote diagnosis.

### About this task

If you do not see results similar to those shown in the **ping** and **wget** examples following these troubleshooting steps, contact your corporate IT organization.

### Procedure

1. Ping the DNS server in the customer network.
2. Ping the proxy server in the customer network.
3. Ping [support.avaya.com](http://support.avaya.com) to check DNS is working.
4. Enter the command **wget** using the proxy from the command line to check if the proxy is working correctly.

### Example

*Ping for server DNS or proxy server reachability:*

```
ping 135.9.69.123
Pinging 135.9.69.123 with 32 bytes of data:
Reply from 135.9.69.123: bytes=32 time=111ms TTL=54
Reply from 135.9.69.123: bytes=32 time=101ms TTL=54
Reply from 135.9.69.123: bytes=32 time=100ms TTL=54
Reply from 135.9.69.123: bytes=32 time=100ms TTL=54
Ping statistics for 135.9.69.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 100ms, Maximum = 111ms, Average = 103ms
```

*Ping for Avaya support server reachability*

```
ping support.avaya.com
Pinging support.avaya.com [198.152.212.23] with 32 bytes of data:
Reply from 198.152.212.23: bytes=32 time=101ms TTL=244
Reply from 198.152.212.23: bytes=32 time=101ms TTL=244
Reply from 198.152.212.23: bytes=32 time=101ms TTL=244
```

```
Reply from 198.152.212.23: bytes=32 time=102ms TTL=244
```

```
Ping statistics for 198.152.212.23:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 101ms, Maximum = 102ms, Average = 101ms
```

*WGET for HTTP response from Avaya support*

```
wget http://support.avaya.com
```

```
HTTP request sent, awaiting response... 200 OK
```

---

## Multiple reinstallations can result in an out of memory error

If you use an installation wizard to install a template and you reinstall the template by deleting and installing it multiple times, an out of permanent generation memory space (PermGen) error can occur.

---

### Troubleshooting steps

Perform the following steps to ensure that a PermGen error does not occur.

#### Procedure

1. Delete the template.
2. Restart Tomcat by performing the following steps:
  - a. Log in to Console Domain as admin.
  - b. Enter `su`
  - c. Enter `/sbin/service tomcat restart`
3. Start the preinstallation Web application.
4. Install the template.


# Appendix A: Preinstallation checklist for System Platform

Before starting System Platform installation, ensure that you complete the tasks from the following preinstallation checklist.

No.	Task	Notes	✓
1	Complete and submit the Universal Install/SAL Product Registration Request form. When opening the Excel based form, click <b>Enable Macros</b> ; otherwise, the form automation will not work. Submit the completed form using the built in email button. See <a href="#">Registering the system</a> on page 34.	<b>!</b> <b>Important:</b> Submit the registration form three weeks before the planned installation date.	
2	Gather the required information about installation, such as IP configuration information, DNS addresses, and address information for Network Time Protocol (NTP) servers.  See <a href="#">Installation worksheet for System Platform</a> on page 202.		
3	Register for PLDS unless you have already registered. See <a href="#">Registering for PLDS</a> on page 35.		
4	Download the System Platform installer ISO image file from PLDS.  See <a href="#">Downloading software from PLDS</a> on page 36.		
5	Download the appropriate solution template and licenses from PLDS.  See <a href="#">Downloading software from PLDS</a> on page 36.		
6	Verify that the downloaded ISO images match the images on the PLDS website.  See <a href="#">Verifying the ISO image on a Linux-based computer</a> on page 36 and <a href="#">Verifying the ISO image on a Windows-based computer</a> on page 37.		

*Table continues...*



No.	Task	Notes	✓
7	Write the ISO images to separate DVDs. See <a href="#">Writing the ISO image to DVD or CD</a> on page 38.	<p> <b>Note:</b></p> <p>If the software files you are writing on media are less than 680 Mb in size, you can use a CD instead of a DVD.</p>	

# Appendix B: Installation worksheet for System Platform

Use the System Platform preinstallation worksheet to help you gather in advance vital configuration values for successful installation, and for initial administration immediately following installation.


The System Platform installer application requires you to fill in various fields. Having the values required for these fields in advance helps the installation to progress more efficiently and accurately. It is likewise important and useful to gather information in advance about other key fields important for System Platform administration immediately following installation.

Print out the following tables and work with your network administrator to fill in the rows.

## System Configuration

Name	Value	Description
<b>Proxy Configuration:</b>		
<b>Status</b>		Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform.
<b>Address</b>		The address for the proxy server.
<b>Port</b>		The port address for the proxy server.
<b>Cdom Session Timeout</b>		
<b>Session Timeout Status</b>		Specifies whether Cdom session timeout is enabled or disabled.
<b>Session Timeout (minutes)</b>		The maximum time in minutes that a Cdom session remains open after the last user transaction with the System Platform Web Console or Cdom CLI.
<b>WebLM Configuration:</b>		
<b>SSL</b>		Specifies whether the Secure Sockets Layer (SSL) protocol will

*Table continues...*

Name	Value	Description
		be used to invoke the WebLM server. Select <b>Yes</b> if the alternate WebLM application has an HTTPS web address. Otherwise, select <b>No</b> if the alternate WebLM application has an HTTP web address. Default value = <b>Yes</b> .
<b>Host</b>		The IP address or host name extracted from the web address of the WebLM application. Default value = <code>&lt;cdom_IP_address&gt;</code> .
<b>Port</b>		The logical port number extracted from the web address of the WebLM application, for example, 4533. Default value = 52233
<b>AES Configuration:</b>		
<b>CM alarmid</b>		Specifies the alarm ID for Communication Manager.
<b>audix alarmid</b>		Specifies the alarm ID for Communication Manager Messaging.
<b>aes alarmid</b>		Specifies the alarm ID for AES.
<b>Other System Configuration:</b>		
<b>Syslog IP Address</b>		IP address of the Syslog server, which collects log messages generated by the System Platform operating system.
<b>Keyboard Layout</b>		Determines the specified keyboard layout for the keyboard attached to the System Platform server.
<b>Statistics Collection</b>		If you disable this option, the system stops collecting the statistics data.   <b>Note:</b> If you stop collecting statistics, the system-generated alarms will be disabled automatically.
<b>SNMP Discovery</b>		By default, this feature enables SNMPv2 management systems to automatically discover any System Platform server in an

*Table continues...*

Name	Value	Description
		<p>Avaya Aura<sup>®</sup> based network, including retrieval of server status and vital statistics. This is useful, for example, when using System Manager to view the entire inventory of System Platform servers across multiple Avaya Aura<sup>®</sup> enterprise solutions at a glance. This feature eliminates the tedious and error-prone task of manually adding extra System Platform servers to an SNMP management system, where that system often requires three or more IP addresses for each System Platform server. SNMP management systems can also query any recognized System Platform server for the logical server configuration.</p> <p>System Platform supports network discovery of values for the following MIB objects:</p> <ul style="list-style-type: none"> <li>• <a href="#">RFC 1213</a> (MIB-2, autodiscovery): sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, and sysServices</li> <li>• <a href="#">RFC 2737</a> (Entity MIB) get/getnext/getbulk:             <ul style="list-style-type: none"> <li>entPhysicalTable – One table entry for the Dom0 physical interface.</li> <li>entLogicalTable – One table entry for the Cdom virtual machine, and one table entry for each virtual machine associated with the installed solution template. Each entry contains the virtual machine name, type, software version, and IP address.</li> </ul> </li> </ul> <p>If you disable this option, SNMP manager systems will be unable to automatically discover this System Platform server.</p>

## Enable IPv6 Configuration

Name	Value	Description
Turn On IPv6		Enables IPv6.

## General Network Settings Configuration

Name	Value	Description
Default Gateway		The default gateway IP address.
Primary DNS		The primary Domain Name System (DNS) server address.
Secondary DNS		(Optional) The secondary DNS server address.
Domain Search List		The search list, which is normally determined from the local domain name. By default, it contains only the local domain name. You can change this by listing the domain search path that you want following the <i>search</i> keyword, with spaces or tabs separating the names.
Cdom Hostname		Depending on requirements of your solution template, you may need to enter the host name for Console Domain as a fully qualified domain name (FQDN), for example, <code>SPCdom.mydomainname.com</code> . Otherwise, just enter the IP address for Console Domain or enter the hostname for Console Domain in non-FQDN format.
Dom0 Hostname		Depending on requirements of your solution template, you might need to enter the host name for System Domain as a fully qualified domain name (FQDN), for example, <code>SPDom0.mydomainname.com</code> . Otherwise, just enter the IP address for System Domain, or enter the hostname for System Domain in non-FQDN format. When using a Domain Name System (DNS) server in your network, the System Domain hostname must be FQDN format.

*Table continues...*

Name	Value	Description
<b>Physical Network Interface</b>		The physical network interface details for eth0 and eth1 (and eth2 if High Availability Failover is enabled).
<b>Domain Dedicated NIC</b>		<p>Applications with high network traffic or time-sensitive traffic often have a dedicated NIC. This means the virtual machine connects directly to a physical Ethernet port and usually requires a separate cable connection to the customer network.</p> <p>See template installation topics for more information.</p>
<b>Bridge</b>		<p>The bridge details for the following:</p> <ul style="list-style-type: none"> <li>• <b>avprivate</b>: This is called a private bridge because it does not use any Ethernet interface, so it is strictly internal to the server. The System Platform installer attempts to assign IP addresses that are not in use.</li> <li>• <b>avpublic</b>: This bridge uses the Ethernet interface associated with the default route, which is usually eth0, but can vary based on the type of the server. This bridge usually provides access to the LAN for System Platform elements (System Domain (Dom-0) and Console Domain) and for any guest domains that are created when installing a template. The IP addresses specified during System Platform installation are assigned to the interfaces that System Domain (Dom-0) and Console Domain have on this bridge.</li> <li>• <b>template bridge</b>: These bridges are created during the template installation and are specific to the virtual machines installed.</li> </ul>

*Table continues...*

Name	Value	Description
<b>Domain Network Interface</b>		The domain network interface details for System Domain (Dom-0) or Console Domain that are grouped by domain based on your selection.
<b>Global Template Network Configuration</b>		The set of IP addresses and host names of the applications hosted on System Platform. Also includes the gateway address and network mask.
<b>VLAN</b>		Required only when installing System Platform on the S8300D server.

### Services Virtual Machine Configuration

Name	Value	Description
<b>Enable Services VM</b>		<p>Enables or disables remote access. Also supports local or centralized alarm reporting.</p> <p>Default value: <b>Enabled</b></p> <p>Leave the <b>Enable services VM</b> option enabled (checkmark) for remote access and local SAL support, or disabled (no checkmark) if you have a separate server dedicated for independent/centralized remote access and SAL support.</p> <p>In a System Platform High Availability configuration, the active node automatically propagates to the standby node, any change in the setting for this field</p>
<b>Hostname</b>		The name assigned to the Services Virtual Machine
<b>Static IP address</b>		The IP address assigned to the Services Virtual Machine. The address must be on the same subnetwork assigned to the Domain 0 (dom0) and Console Domain (cdom) virtual machines.
<b>Virtual devices</b>		The virtual device (port) assigned to the Services Virtual Machine.

*Table continues...*

Name	Value	Description
		Default value (eth0) automatically assigned. No user input necessary.

### Ethernet Configuration

Name	Value	Description
<b>Speed</b>		<p>Sets the speed in MB per second for the interface. Options are:</p> <ul style="list-style-type: none"> <li>• 10 Mb/s half duplex</li> <li>• 10 Mb/s full duplex</li> <li>• 100 Mb/s half duplex</li> <li>• 100 Mb/s full duplex</li> <li>• 1000 Mb/s full duplex</li> </ul> <p>Auto-Negotiation must be disabled to configure this field.</p>
<b>Port</b>		<p>Lists the available Ethernet ports.</p> <p>Auto-Negotiation must be disabled to configure this field.</p>
<b>Auto-Negotiation</b>		<p>Enables or disables autonegotiation. By default it is enabled, but might cause some problems with some network devices. In such cases you can disable this option.</p>

### Bonding Interface Configuration

Name	Value	Description
<b>Name</b>		<p>Is a valid bond name.</p> <p>It should match regular expression in the form of "bond[0-9]+".</p>
<b>Mode</b>		<p>Is a list of available bonding modes that are supported by Linux.</p> <p>The available modes are:</p> <ul style="list-style-type: none"> <li>• Round Robin</li> <li>• Active/Backup</li> <li>• XOR Policy</li> <li>• Broadcast</li> <li>• IEEE 802.3ad</li> </ul>

*Table continues...*



Name	Value	Description
		<ul style="list-style-type: none"> <li>Adaptive Transmit Load Balancing</li> <li>Adaptive Load Balance</li> </ul> <p>For more information about bonding modes, see <a href="http://www.linuxhorizon.ro/bonding.html">http://www.linuxhorizon.ro/bonding.html</a>.</p> <p><b>* Note:</b> The default mode of new bonding interface is Active/Backup.</p>
<b>Slave 1/Primary</b>		<p>Is the first NIC to be enslaved by the bonding interface.</p> <p>If the mode is Active/Backup, this will be the primary NIC.</p>
<b>Slave 2/Secondary</b>		<p>Is the second NIC to be enslaved by the bonding interface.</p> <p>If the mode is Active/Backup, this will be the secondary NIC.</p>

## Static Route Configuration

**\* Note:**

A network restart or VM reboot is necessary to enable static route updates in the web console.

Name	Value	Description
<b>Interface</b>		The bridge through which the route is enabled.
<b>Network Address</b>		The IP address of a destination network associated with an Avaya (or Avaya Partner) remote services host.
<b>Network Mask</b>		The subnetwork mask for the destination network.
<b>Gateway</b>		The address of a next-hop gateway that can route System Platform traffic to or from a remote services host on the destination network.

### SNMP Trap Receiver Configuration

Name	Value	Description
Product Id		Product ID for System Platform Console Domain.  When you install System Platform, a default Product ID of 1001119999 is set. You must change this default ID to the unique Product ID that Avaya provides.  * <b>Note:</b> VSPU is the model name for Console Domain.
IP Address		IP address of the trap receiver.
Port		Port number on which traps are received.
Community		SNMP community to which the trap receiver belongs. Must be <code>public</code> .
Device Type		Default setting is <b>INADS</b> . Do not change this settings.
Notify Type		Default setting is <b>TRAP</b> . Do not change this setting.
Protocol Version		Default setting is <b>V2c</b> . Do not change this setting.

### Password Configuration

\* **Note:**

Passwords must be at least six characters long. Use uppercase and lowercase alphabetic characters and at least one numeral or special character.

Name	Value	Description
root Password		The password for the root login.
admin Password		The password for the admin login.
cust Password		The password for the cust login.  The cust login is for audit purposes. It has read-only access to the Web Console, except for changes to its password, and no command line access.
Idap Password		The password for the Idap login.

*Table continues...*

Name	Value	Description
		System Platform uses a local LDAP directory to store login and password details. Use this login and password to log in to the local LDAP directory. This login does not have permissions to access the System Platform Web Console.

## Network Time Protocol Configuration

Name	Value	Description
<b>NTP server 1</b>		<p>The host name or IP address of an NTP server, visible in the Web Console when you click <b>Query State</b> in the Date and Time Configuration page, under <b>Server Management</b>. When displayed, either of the following special characters precede each server host name or IP address. Each character has a special meaning, as follows:</p> <ul style="list-style-type: none"> <li>• Asterisk character (*): The preferred server (referenced by the local system), chosen by System Platform.</li> <li>• Plus character (+): Indicates a high-quality candidate for the reference time that System Platform can use if the selected time source becomes unavailable.</li> </ul> <p>Avaya preconfigures several server names before system delivery. You can add more NTP reference servers by clicking <b>Add</b> in the Date and Time Configuration page under <b>Server Management</b>.</p>
<b>NTP server 2</b>		
<b>NTP server 3</b>		
<b>NTP server 4</b>		

**Cdom and network interface configuration for System Platform High Availability configurations**

Name	Value	Description
Remote cdom IP address		IP Address of Console Domain on the standby node.
Remote cdom user name		User name for Console Domain on the standby node.
Remote cdom password		Password for Console Domain on the standby node.
Primary network interface		Network interface connected to the customer network.
Crossover network interface		Network interface connected to the standby server.

**Ping targets configuration**

Name	Value	Description
Ping Target (IP Address/ HostName)		IP address or host name of the gateway to the network. You can add multiple ping targets to verify if the System Platform server is connected to network.
Interval (sec)		Interval after which the local System Platform server sends ICMP pings to listed ping targets.
Timeout (sec)		Timeout interval after which no ICMP reply indicates a network failure.

# Appendix C: Managed element worksheet for SAL Gateway

Use this worksheet to record the information required by an administrator to add managed devices to the SAL Gateway.

System Domain (Domain-0) does not have alarming enabled; however, the System Domain has its own Product ID (Alarm ID).

Console Domain (cdom or udom) has alarming enabled. System Domain sends all syslog (system logs) to Console Domain, which then triggers alarms for System Domain.

**! Important:**

For High Availability Failover configurations, you must have two different solution element IDs (SEIDs) for System Domain (Domain-0): one for the active System Domain and one for the standby System Domain. You must administer both SEIDs in the SAL Gateway user interface.

Managed device (virtual machine)	IP Address	SE ID	Product ID	Model	Notes
System Domain (Domain-0)				VSP_2.0.0.0	
Console Domain (cdom or udom)				VSPU_2.1.1.2	

## Related links

[Adding a managed element](#) on page 136

# Appendix D: Managing license entitlements from PLDS

---

## Activating license entitlements

### Before you begin

Obtain the Host ID of WebLM if you are activating license entitlements on a new License Host.

### About this task

Use License Activation Code (LAC) to activate one or more license entitlements. You can activate all of the licenses, or you can specify a number of licenses to activate from the quantity available. Upon successful activation of the license entitlements, PLDS creates an Activation Record and sends an Activation Notification email message to the customer who is registered with the entitlements. The Activation Record and Activation Notification provide details on the number of activated licenses and the License Host. The license file can be accessed on the License/Keys tab of the Activation Record in PLDS and is also an attachment to the Activation Notification email message. You must install the license file on WebLM to use the licenses.

### Procedure

1. Type <http://plds.avaya.com> in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. In the **LAC(s)** field of the Quick Activation section, enter the LAC that you received in an email message.

 **Note:**

If you do not have an email message with your LAC, follow the steps in the Searching for Entitlements section and make a note of the appropriate LAC from the LAC column.

 **Note:**

The Quick Activation automatically activates all license entitlements on the LAC. However, you can remove line items or specify a number of licenses to activate from the quantity available.

4. Enter the License Host information.  
You can either create a new license host or use an existing license host.
5. Click **Next** to validate the registration detail.

6. Enter the License Host Information.
  - The Host ID of the WebLM server. The Host ID is obtained from the Server Properties page of the WebLM server where the license file is installed.
  - If you are using Centralized Licensing, enter the Centralized Licensing ID of the WebLM server where the license file is installed. Obtain the Centralized Licensing ID from the Server Properties page of the System Manager WebLM server.
7. Enter the number of licenses to activate.
8. Review the Avaya License Agreement and accept the agreement if you agree.
9. Perform the following steps to send an activation notification email message:
  - a. In the **E-mail to** field, enter the email addresses of the additional activation notification recipients.
  - b. Enter the comments or special instructions in the **Comments** field.
  - c. Click **Finish**.
10. Click **View Activation Record**.
  - The **Overview** tab displays a summary of the license activation information.
  - The **Ownership** tab displays the registration information.
  - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application. From the **License/Key** tab, you can view and download the license file. Install each license file on the WebLM server associated with the License Host.

---

## Searching for license entitlements

### About this task

Use this functionality to search for an entitlement by using any one or all of the following search criteria:

- Company name
- Group name
- Group ID
- License activation code

In addition to these search criteria, PLDS also provides other additional advanced search criteria for searching license entitlements.

#### **Note:**

Avaya associates or Avaya Partners can search license entitlements only by company name.

## Procedure

1. Type <http://plds.avaya.com> in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. Click **Assets > View Entitlements**.

The system displays Search Entitlements page.

4. To search license entitlements by *company name*, enter the company name in the **%Company: field**. To see a complete list of companies before searching for their corresponding entitlements, do the following:
  - a. Click the **magnifying glass** icon.
  - b. Enter the name or several characters of the name and a wildcard (%) character.
  - c. Click **Search Companies**.
  - d. Select the desired company name from the list of options.

**+ Tip:**

You can use a wildcard (%) character if you do not know the exact name of the company you are searching for. For example, if you enter `Av%`, the system searches for all the company names starting with the letter Av. You can enter a wildcard character at any position in the search criteria.

5. To search license entitlements by *group name*, enter the appropriate information in the **%Group name:** or **%Group ID:** fields.

Group Names or IDs are specific to Functional Locations and Sold-To's that define the actual location of equipment and software.

**+ Tip:**

You can use a wildcard character if you do not know the exact name of the group you are searching for. For example, if you enter `Gr%`, the system searches for all the groups starting with the characters Gr. You can enter a wildcard character at any position in the search criteria.

6. To search license entitlements by *LAC*, enter the specific LAC in the **%LAC:** field.

**+ Tip:**

You can use a wildcard character if you do not know the exact LAC you are searching for. For example, if you enter `AS0%`, the system searches for all the LACs starting with AS0. You can enter a wildcard character at any position in the search criteria.

You will receive LACs in an e-mail if you have supplied the e-mail address to your sales order. If you do not have this code, search by using one of the other search criteria.

7. To search license entitlements by *application, product* or *license status*, select the appropriate application, product, and/or status from the field.
8. Click **Search Entitlements**.



## Result

All corresponding entitlement records appear at the bottom of the page.

---

# Moving activated license entitlements

## Before you begin

Host ID or License Host name of the move from/to License Host.

## About this task

Use this functionality to move activated license entitlements from one License Host to another. You can choose to move all or a specified quantity of license entitlements.

### \* Note:

If you move a specified number of activated license entitlements from one host to another by using the Rehost/Move transaction in PLDS, two new license files are generated:

- One license file reduces the number of license entitlements on the License Host from which you are moving license entitlements.
- One license file increases the number of license entitlements on the License Host to which you are moving license entitlements.

Install each of these license files on the appropriate server.

If you move all activated license entitlements, only one license file is generated. Install this new license file on the License Host to which you are moving license entitlements. Remove the license file from the License Host from which you are moving all license entitlements.

## Procedure

1. Type <http://plds.avaya.com> in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. Click **Activation > Rehost/Move** from the Home page.
4. Click **View Activation Record information** to find and select licenses to rehost or move.

You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

### \* Note:

If you are an Avaya associate or Avaya Partner, enter the search criteria and click **Search Activation Records**.

5. Select **Rehost/Move** for the License Host from which you are moving license entitlements.
6. In the **Search License Hosts** field, enter the License Host to which you are moving license entitlements.

Alternatively, you can click **Add a License Host** to select an existing License Host.

7. Validate the Registration Detail, and click **Next**.
8. Enter the License Host Information.
  - The Host ID of the WebLM server. The Host ID is obtained from the Server Properties page of the WebLM server where the license file is installed.
  - If you are using Centralized Licensing, enter the Centralized Licensing ID of the WebLM server where the license file is installed. Obtain the Centralized Licensing ID from the Server Properties page of the System Manager WebLM server.
9. Enter the number of Licenses to move in the **QTY column** field and click **Next**.
10. Accept the Avaya Legal Agreement.

You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.
11. Perform the following steps to send an activation notification email message:
  - a. In the **E-mail to** field, enter the email addresses of the additional activation notification recipients.
  - b. Enter the comments or special instructions in the **Comments** field.
  - c. Click **Finish**.
12. Click **View Activation Record**.
  - The **Overview** tab displays a summary of the license activation information.
  - The **Ownership** tab displays the registration information.
  - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application. From the **License/Key** tab, you can view and download the license file. Install each license file on the WebLM server associated with the License Host.

---

## Regenerating a license file

### Procedure

1. Type <http://plds.avaya.com> in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. Click **Activation > Regeneration** from the Home page.
4. Search License Activations to Regenerate.

You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

5. Click **Regenerate** from the appropriate record.
6. Validate the Registration Detail, and click **Next**.

7. Validate the items that will regenerate and click **Next**.
8. Accept the Avaya Legal Agreement.

You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

9. Perform the following steps to send an activation notification email message:
  - a. In the **E-mail to** field, enter the email addresses of the additional activation notification recipients.
  - b. Enter the comments or special instructions in the **Comments** field.
  - c. Click **Finish**.
10. Click **View Activation Record**.
  - The **Overview** tab displays a summary of the license activation information.
  - The **Ownership** tab displays the registration information.
  - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application. From the **License/Key** tab, you can view and download the license file. Install each license file on the WebLM server associated with the License Host.

# Appendix E: Enterprise-wide licensing

---

## Overview of enterprise-wide licensing

Starting with Release 4.2, AE Services supports enterprise-wide licensing. With enterprise-wide licensing, AE Services customers are able to purchase any number of licenses and then allocate those licenses to various AE Services at their own discretion. This means that AE Services customers are able to pool or share all AE Services features and Rights To Use (RTU) among AE Services. This applies only to AE Services features licensed in the AE Services license file and not those licensed in the Communication Manager license file.

**\* Note:**

Enterprise-wide licensing is not supported in System Platform High Availability Failover configurations.

- To compare standard licensing with enterprise-wide licensing, see [Comparison of standard licensing and enterprise-wide licensing](#) on page 220.
- For examples of licensing configurations, see [Licensing configuration examples](#) on page 221.
- For the procedures required to set up an AE Services configuration that uses enterprise-wide licensing, see [Setting up a configuration for allocating licenses](#) on page 224.

---

## Comparison of standard licensing and enterprise-wide licensing

Standard licensing	Enterprise-wide licensing
AE Services has used the standard license file since the introduction of the platform (Release 3.0). The standard license file continues to be used for standalone AE Services server licensing.	AE Services introduced support for enterprise-wide licensing with Release 4.2.
A standard license is generated by the Product Licensing and Delivery System (PLDS) from the system record for an AE Services server.	Enterprise-wide licensing includes a master enterprise license file (ELF) and an allocation license file (ALF). <ul style="list-style-type: none"><li>• The master enterprise license file (ELF) is generated by the PLDS from the system record</li></ul>

*Table continues...*

Standard licensing	Enterprise-wide licensing
	<p>from the enterprise. The master license file can reside on an AE Services server or a dedicated WebLM server.</p> <ul style="list-style-type: none"> <li>The allocation license file (ALF) is generated by WebLM based on features in the master license file and user allocations on the AE Services server. The ALF or ALFs can reside on one or more AE Services servers.</li> </ul>
The standard license file is installed on the AE Services server. In a standard licensing arrangement, AE Services and the WebLM server are normally co-resident.	With enterprise wide licensing, the WebLM server does not have to be co-resident with AE Services, but each local WebLM server is normally co-resident with the AE Services server that it licenses.
With standard licensing, a license can not be moved from one server to another, and capacities can not be reallocated.	With enterprise-wide licensing, you can reallocate enterprise capacities and features as desired.

---

## Licensing configuration examples

To understand how licensing configurations work, this section provides a description of standard licensing and enterprise-wide licensing.

---

### Standard licensing

In a standard licensing configuration for Bundled and Software-only offers, the standard license file (SLF) is installed on the AE Services server and is controlled by the WebLM server running on the AE Services server. For System Platform installations, the standard license file is normally installed on, and controlled by, the WebLM server running in the Console Domain (c-dom).

**\* Note:**

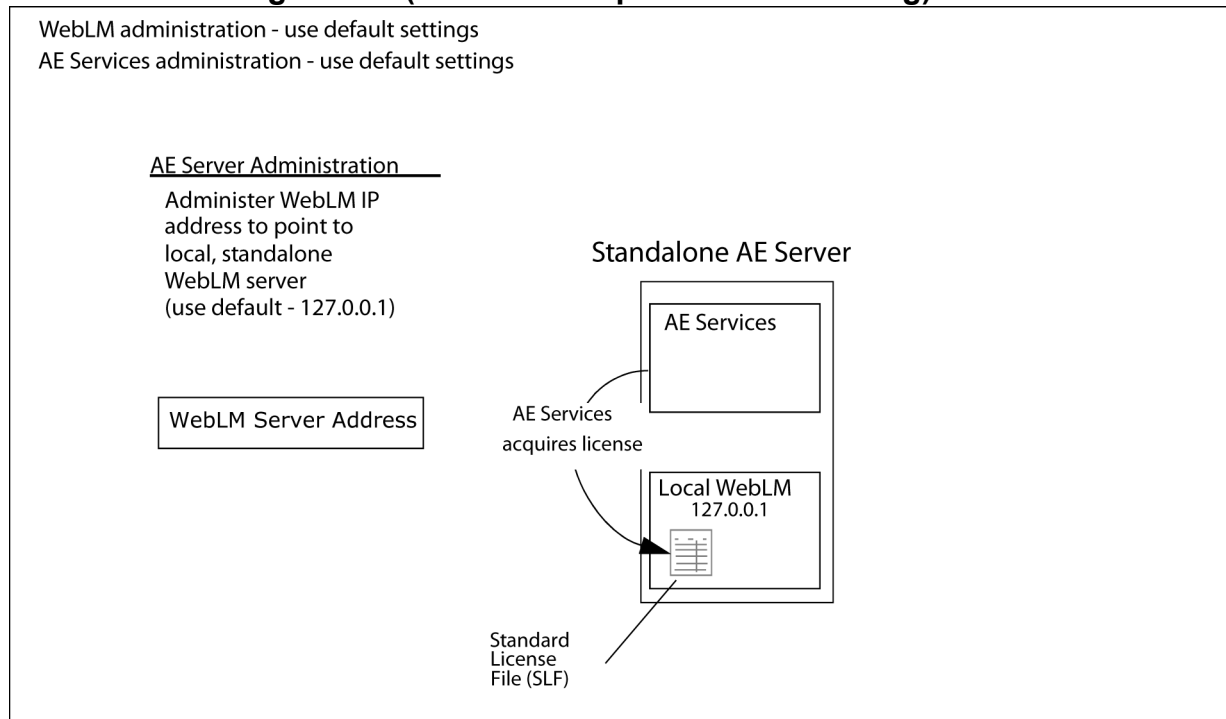
For System Platform installations, when using the WebLM server in c-dom, port 52233 should be used for licensing.

The following figure illustrates the standard licensing configuration.

**\* Note:**

If you use the standalone configuration, use the default settings on the WebLM Server Address page in the AE Services Management Console.

## Standalone configuration (without enterprise-wide licensing)



### \* Note:

The default IP address, 127.0.0.1, shown in the illustration above is only for the AE Services Bundled and AE Services Software-only offers. The default IP address for the AE Services on System Platform offer is the IP address of the c-dom on System Platform. For the AE Services on VMware offer, there is no default WebLM address. The user must enter an appropriate IP address for the WebLM server.

## Enterprise-wide licensing — allocating licenses or features

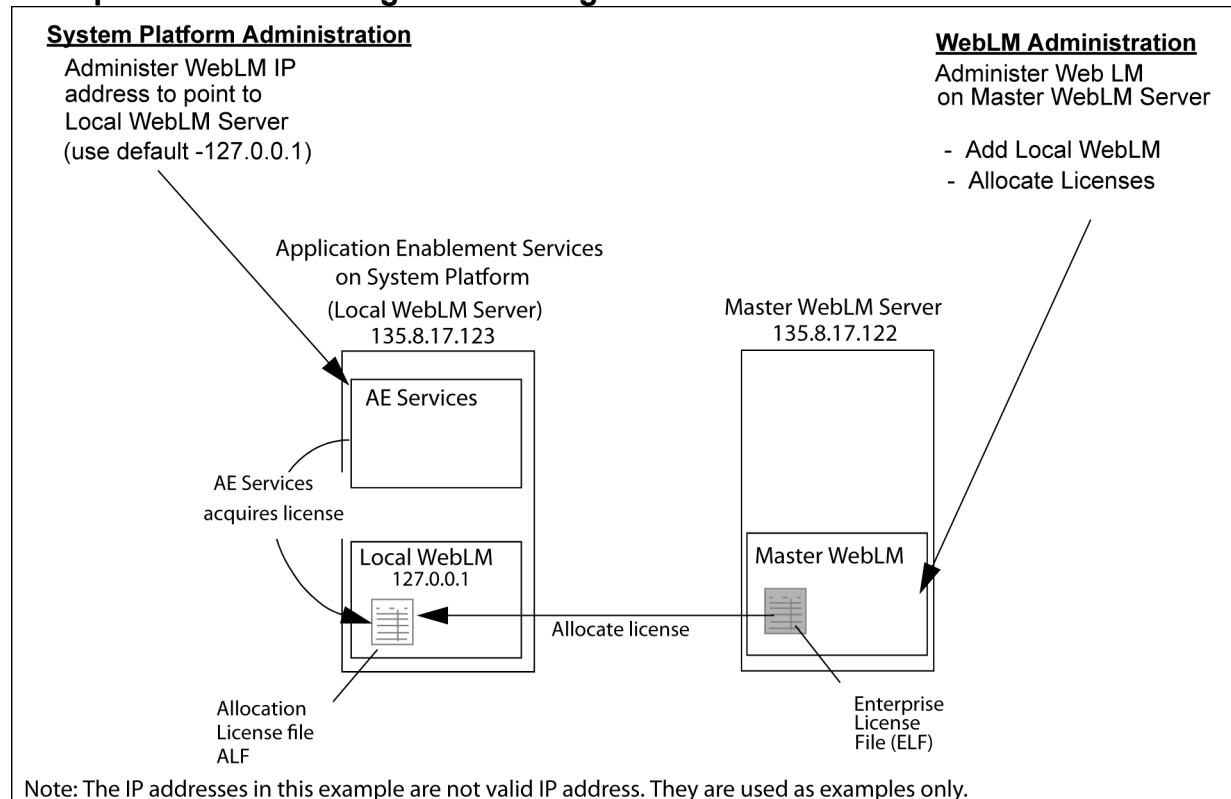
Starting with Release 4.2, AE Services expanded its licensing capabilities to include enterprise-wide licensing. Enterprise-wide licensing provides the flexibility to move capacities and features from one AE Services server to another. For example, prior to AE Services 4.2, if you had purchased 3 AE Services servers with different licensing capacities, you could not move capacity purchased for one AE Services server to another AE Services server. With enterprise-wide licensing, you can move capacities or features from one server to another by using a master WebLM server to allocate license features to different AE Services servers.

Because this configuration relies on a master enterprise license file (ELF), which generates allocation license files (ALF), it is referred to as an ELF/ALF configuration. Each ALF will reside on an AE Services server with a Local WebLM Server. This is the recommended model for AE Services enterprise configurations. If you use the ELF/ALF model, you do not need to change the default settings on the WebLM Server Address page.

For this configuration you must use WebLM Administration to configure the master WebLM server so that it can allocate licenses to each local WebLM server on the AE Services servers. (In the WebLM Administration, select **Licensed Products > Application Enablement (CTI) > Configure Local WebLMs > Add Local WebLM.**)

The following figure illustrates an ELF/ALF configuration.

### Enterprise-wide licensing — allocating licenses or features



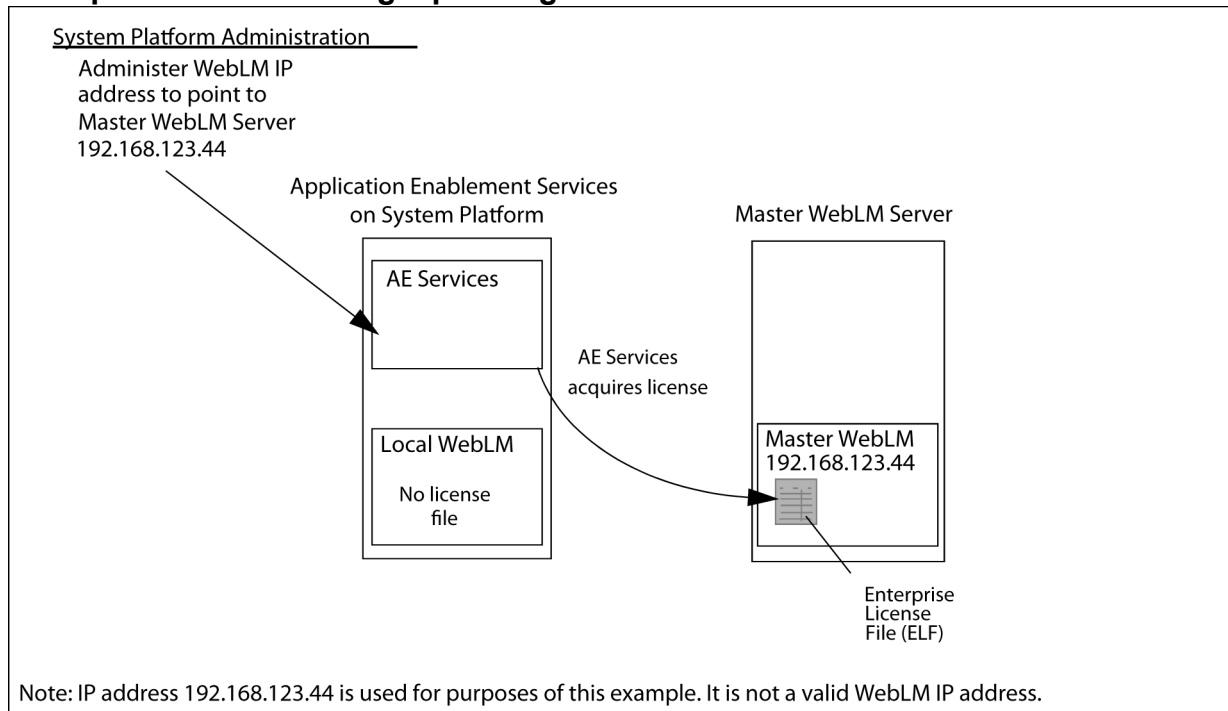
### Enterprise-wide licensing — pointing to a master license on a remote server

Another type of enterprise licensing configuration is an enterprise license file (ELF)-only configuration. In an ELF-only configuration, the enterprise license file resides on a master WebLM server, and one or more AE Services servers point to the IP address of the master WebLM server. No allocation license files (ALFs) reside on AE Services servers.

If you use the ELF-only configuration, you must administer the WebLM Server Address page in the AE Services Management Console with the WebLM IP address and WebLM port number for the master WebLM server that hosts the ELF.

The following figure illustrates an ELF-only configuration.

## Enterprise-wide licensing – pointing to a master license on a remote server



**⚠ Caution:**

Using the ELF-only configuration is not recommended because network latency and outages can affect the ability of the AE Services server to acquire licenses, and it creates a single point of failure for licensing.

---

## Setting up a configuration for allocating licenses

### About this task

Use the following procedures to set up a configuration for allocating licenses.

---

## Installing the license file and configuring the master WebLM server

### About this task

This procedure applies to a configuration where the master WebLM server allocates licenses to local AE Services servers (see [Enterprise-wide licensing — allocating licenses or features](#) on page 222). You will need to use this procedure to install the master enterprise license file (ELF) on the master WebLM server.



Follow these steps to install the enterprise license file (ELF) on the server that hosts the enterprise license file (ELF). For Bundled and Software-only offers, this server can be an AE server or a computer dedicated to WebLM. For System Platform installations, this server can be running on the c-dom or on a computer dedicated to WebLM.

## Procedure

1. Log in to the computer that has the license file stored on it.
2. From a web browser, type the fully qualified domain name or IP address of the AE Services server, for example `https://aserver.example.com`.

In terms of this configuration example, the IP address would be 135.8.17.122.

3. Press **Enter**.
4. On the Application Enablement Services welcome page, click **Licensing > WebLM Server Access**.
5. On the Web License Manager Log on screen, enter your WebLM user name and password, and click the arrow.
6. On the WebLM main menu, click **Browse**.
7. Locate the license file and click **Open**.
8. Click **Install**.

WebLM uploads the license file to the WebLM server. When the process is complete, the server displays the message: License file installed successfully. Notice that the WebLM main menu now displays Application\_Enablement under Licensed Products.

9. From the WebLM main menu, select **Application\_Enablement > Enterprise Configuration**.
10. Complete the Configure Enterprise page as follows:
  - a. For the Master WebLM Configuration settings, which are required, accept the defaults.
    - Name: Master WebLM Server
    - Description: leave blank
    - IP Address: <IP address of the local c-dom>.
  - b. For the Default Periodic Operation Settings settings, which are required, accept the defaults.
  - c. For the SMTP Server Settings, which are optional, provide the name of the SMTP Server (Server Name), the user ID of the administrator (Admin Account), and the password of the administrator (Admin Password).
 

These are the authentication settings for the SMTP server that sends email notifications for periodic operation failures.
  - d. For the Email Notification Settings for Periodic Operation, complete the settings (Email Notification and Email Addresses) based on your operational requirements.
 

By default, email notification is disabled (off).

- e. For the Default Periodic License Allocation Schedule, select the day and time, based on your operational requirements.
- f. For the Default Period Usage Query Schedule, select the day and time, based on your operational requirements.
- g. Click **Submit**.

### Next steps

Continue with [Adding a local WebLM server](#) on page 226.

---

## Adding a local WebLM server

### About this task

From the Master WebLM Server Web page, follow this procedure to add a local WebLM server.

#### **Note:**

- You can allocate feature licenses only if the connection between the master WebLM server and the local WebLM server is validated and established.
- The AE Services on VMware offer does not support a local WebLM.

### Procedure

1. From the WebLM main menu, select **Application Enablement > Local WebLM Configuration > Add Local WebLM**.
2. Complete the Add Local WebLM page as follows:
  - Local WebLM Settings:
    - Name: the *<name of the local AE Services server>*, for example, lzbundled05. (Although this name is required, it can be any name you choose.)
    - Description: a descriptive term for the local AE Services server (optional)
    - IP Address:
      - For Bundled and Software-only offers: *<IP address of the Local AE Services server>*. For purposes of this example, the IP address is 135.8.17.123.
      - For System Platform installations: *<IP address of the c-dom hosting the Local AE Server>*. For purposes of this example, the IP address is 135.8.17.123.

#### **Note:**

The AE Services on VMware offer does not support a local WebLM.

- Port: 8443 (the default)
- Periodic License Allocation Schedule: Accept the defaults. Note that the default settings refer to the settings that you administered on the Master WebLM Server.
- Periodic Usage Query Schedule: Accept the defaults. Note that the default settings refer to the settings that you administered on the Master WebLM Server.

3. Click **Configure and Validate**.

### Next steps

Continue with [Setting up the Local WebLM Server in your configuration](#) on page 227.

### \* Note:

Before you can uninstall an Enterprise-Wide License from the master WebLM, you must first de-allocate all of its licenses and delete all local WebLM servers associated with the license.

---

## Setting up the Local WebLM Server in your configuration

### About this task

Use the following procedure to change the default WebLM password and to verify the settings on the WebLM Server Address page in the AE Services Management Console.

### Procedure

1. From a web browser, type the fully qualified domain name or IP address of the AE Server, for example `https://aserver.example.com`.

In terms of this configuration example, the IP address would be 135.8.17.123.

2. Press **Enter**.
3. At the Security Alert, click **Yes** to accept the SSL certificate.
4. From the Application Enablement Services Welcome page, click **Licensing > WebLM Server Access**.
5. On the Web License Manager log on screen, log in to WebLM with the default user name and password.

The default user name is `admin`, and the default password is `weblmadmin`. The first time you log in to WebLM, the WebLM server displays the Change Password page.

6. On the Change Password page, complete the fields and click **Submit**.  
The password must contain 6 to 14 characters. White spaces are not permitted in the password, and the password itself must not be blank.
7. On the Web License Manager log on screen, log in as `admin` with the new password.
8. From the WebLM main menu, select **Logout** to log out of WebLM.
9. Log on to the AE Services server (local WebLM server) again.

10. From the AE Services Management Console main menu, select **Licensing > WebLM Server Address**.
11. Verify that the WebLM Server address page displays the following settings:
  - For Bundled and Software-only offers:
    - WebLM IP Address: 127.0.0.1

- WebLM Port: 443
- For System Platform installations:
  - WebLM IP Address: <IP address of the local c-dom>
  - WebLM Port: 52233

### Next steps

Continue with [Changing the allocations of a license file](#) on page 228.

---

## Changing the allocations of a license file

### About this task

The master WebLM server provides you with the ability to change license file allocations for your local WebLM servers. From the Master WebLM Server web page, follow this procedure to change the license allocations.

### Procedure

1. From a web browser, type the fully qualified domain name or IP address of the AE Server, for example `https://aserver.example.com`.  
  
In terms of this configuration example, the IP address would be 135.8.17.123.
2. Press **Enter**.
3. At the Security Alert, click **Yes** to accept the SSL certificate.
4. On the Application Enablement Services welcome page, click **Licensing > WebLM Server Access**.
5. On the Web License Manager log on screen, enter your WebLM user name and password, and click the arrow.
6. From the WebLM main menu, select **Application Enablement > Allocations**.
7. On the Allocations by Features page, click **Change Allocations**.
8. On the Change Allocations page, enter an appropriate value in the New Allocation box and click **Submit Allocations**.

For example, assume that you want to allocate 20 TSAPI Simultaneous User licenses to the local WebLM server. Enter 20 in the New Allocations text box, and click **Submit Allocations**.

WebLM processes the allocation request, and displays the updated Allocations by Features page.

### Next steps

Continue with [Verifying the license allocations on the Local WebLM Server](#) on page 229.

---

## Verifying the license allocations on the Local WebLM Server

### About this task

Follow these steps to verify that the license allocations that you administered are in effect.

### Procedure

1. From a web browser, type the fully qualified domain name or IP address of the AE Server, for example `https://aserver.example.com`.

In terms of this configuration example, the IP address would be 135.8.17.123.

2. Press **Enter**.
3. At the Security Alert, click **Yes** to accept the SSL certificate.
4. From the Application Enablement Services Welcome page, click **Licensing > WebLM Server Access**.
5. On the Web License Manager log on screen, enter your WebLM user name and password, and click the arrow.
6. From the WebLM main menu, select **Licensed Products > Application Enablement**.
7. Verify that the licensed features on the local WebLM server are consistent with the settings you administered on the master WebLM server.

 **Note:**

The Allocation license is valid for up to 30 days. The master WebLM will push the ALF to the local WebLM based on the administered schedule (Periodic License Allocation Schedule).

# Appendix F: Installing and connecting the S8800 server

---

## Overview of the Avaya S8800 Server

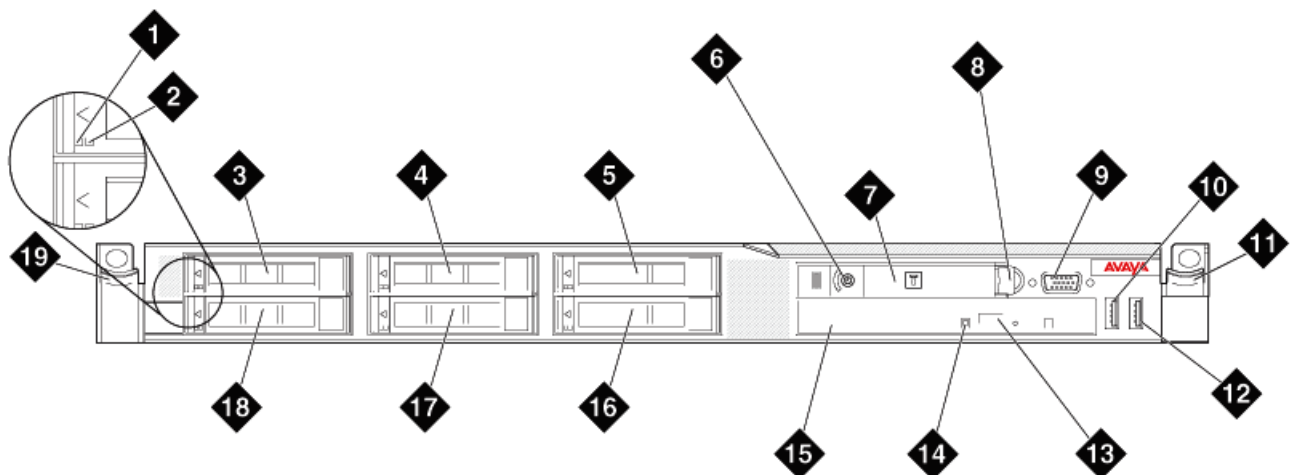
---

### Avaya S8800 Server overview

The Avaya S8800 Server supports several Avaya software applications. The server is available in a 1U model or 2U model and with various hardware components. The server model and specific hardware components in your server depend on the requirements of the software application that will run on the server.

---


### Front of server



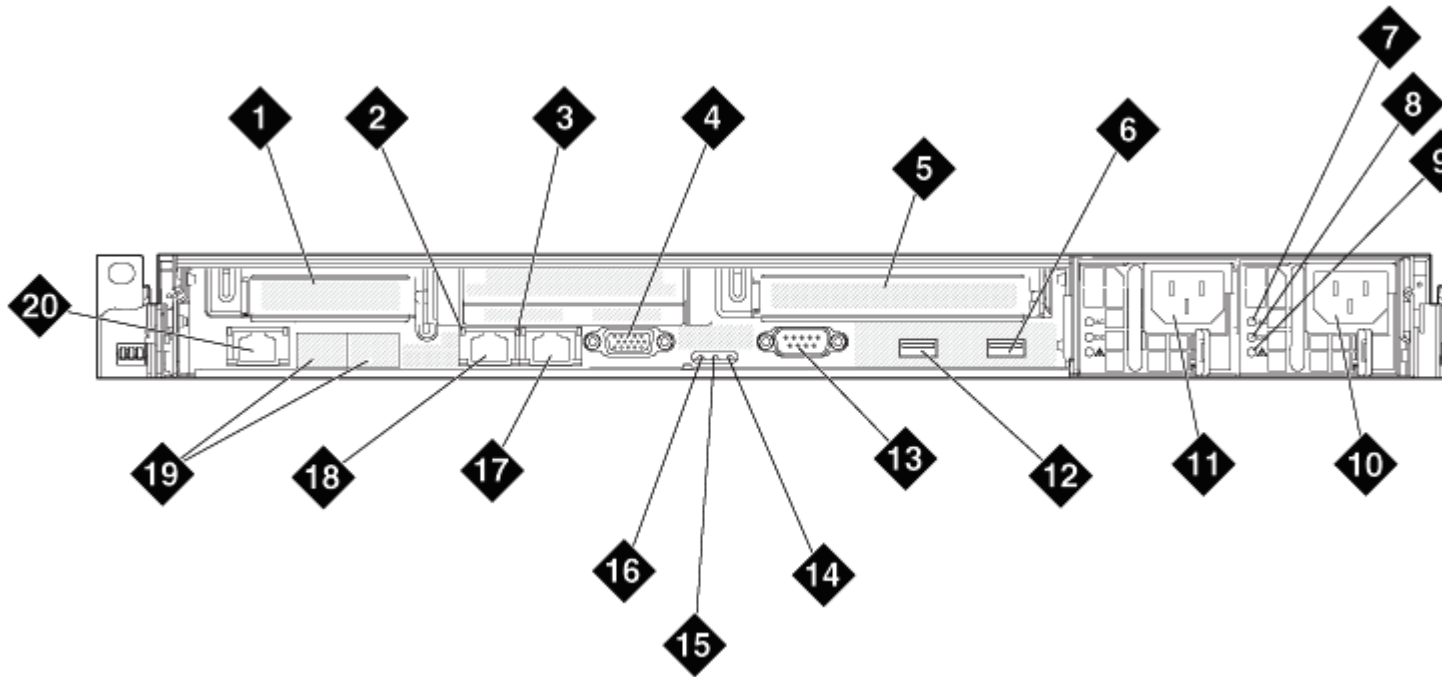
hw881fn LAO 092209

1	Hard disk drive activity LED (green)
2	Hard disk drive status LED (amber)
3	Drive bay 0

*Table continues...*

4	Drive bay 2
5	Drive bay 4
6	Power control button and LED
7	Operator information panel  <b>Note:</b> The operator information panel is shown in the pushed in position.
8	Operator information panel release latch
9	Video connector
10	USB connector 1
11	Rack release latch
12	USB connector 2
13	DVD eject button
14	DVD drive activity LED
15	DVD drive
16	Drive bay 5
17	Drive bay 3
18	Drive bay 1
19	Rack release latch

## Back of server



hw881bk LAO 100

1	PCIe slot 1 (used for optional Ethernet connectors 5 and 6)
2	Ethernet activity LED
3	Ethernet link LED
4	Video connector
5	PCIe slot 2
6	USB connector 4
7	AC power LED (green)
8	DC power LED (green)
9	Power supply error LED (amber)
10	Power supply 2 (redundant power supply)
11	Power supply 1 (primary power supply)
12	USB connector 3
13	Serial connector
14	System error LED (amber)
15	System locator LED (blue)
16	Power LED (green)
17	Ethernet connector 2

Table continues...



18	Ethernet connector 1
19	Ethernet connectors 3 and 4 (with optional 2-port Ethernet daughter card)  <span style="color: green;">*</span> <b>Note:</b> The optional 2-port daughter card is not applicable to Application Enablement Services on System Platform.
20	System management Ethernet connector (IMM)

## Avaya S8800 1U Server specifications

Type	Description
Dimensions	Height: 43 mm (1.69 inches, 1U) Depth: 711 mm (28 inches) Width: 440 mm (17.3 inches)
Weight	Maximum weight: 15.4 kg (34 lb.), when fully configured.
Heat output	Approximate heat output: <ul style="list-style-type: none"> <li>• Minimum configuration: 662 Btu per hour (194 watts)</li> <li>• Maximum configuration: 1400 Btu per hour (400 watts)</li> </ul> Heat output varies depending on the number and type of optional features that are installed and the power-management optional features that are in use.
Acoustic noise emissions	Declared sound power, operating: 6.1 bel  The sound levels were measured in controlled acoustical environments according to the procedures specified by the American National Standards Institute (ANSI) S12.10 and ISO 7779 and are reported in accordance with ISO 9296. Actual sound-pressure levels in a given location might exceed the average values stated because of room reflections and other nearby noise sources. The declared sound-power levels indicate an upper limit, below which a large number of computers will operate.
Electrical input requirements	<ul style="list-style-type: none"> <li>• Sine-wave input (47–63 Hz) required</li> <li>• Input voltage low range:                             <ul style="list-style-type: none"> <li>- Minimum: 100 V AC</li> <li>- Maximum: 127 V AC</li> </ul> </li> <li>• Input voltage high range:                             <ul style="list-style-type: none"> <li>- Minimum: 200 V AC</li> <li>- Maximum: 240 V AC</li> </ul> </li> <li>• Input kilovolt-amperes (kVA), approximately:                             <ul style="list-style-type: none"> <li>- Minimum: 0.194 kVA</li> </ul> </li> </ul>

*Table continues...*

Type	Description
	- Maximum: 0.700 kVA
Front connectors	<ul style="list-style-type: none"> <li>• Two USB</li> <li>• Video</li> </ul>
Back connectors	<ul style="list-style-type: none"> <li>• Two Ethernet (RJ 45). Optionally, two or four additional Ethernet.</li> <li>• Serial</li> <li>• Two USB</li> <li>• Video</li> <li>• Systems management Ethernet (IMM)</li> </ul>

## Server components

Component	Minimum specification	Upgrade options based on product requirements
Microprocessor	One Intel E5520 quad core, 2.26 GHZ processor	<ul style="list-style-type: none"> <li>• One additional E5520 processor for a total of two processors</li> <li>• Higher speed E5570 processor that runs at 2.93 Ghz.</li> </ul>
Memory	4 GB of 1333 Mhz, fully-buffered DDR-3 RDIMMs (Two 2GB DIMMs): <ul style="list-style-type: none"> <li>• ECC registered</li> <li>• Slots: 16 dual inline</li> </ul>	Up to 32 GB with specified 2GB DIMMs (16 GB per processor)
Media drive	DVD-R/W SATA slimline	No additional options
Hard disk drive expansion bays	Six 2.5-inch hot-swap SAS hard disk drive bays	No additional options
Hard disk drive	Two 146 GB SAS 2.5" 10K RPM hard drives	<ul style="list-style-type: none"> <li>• Additional 146-GB 10K RPM drives</li> <li>• High performance 146-GB 15K RPM drives</li> </ul>
RAID controllers	ServeRAID-MR10i RAID SAS adapter that provides RAID level 1 or 5. Includes 256 MB cache module and battery for write cache	ServeRAID-BR10i SAS RAID adapter that provides RAID level 1 (used for AES)
PCI expansion slots	Two PCI Express x16 Gen 2 slots: <ul style="list-style-type: none"> <li>• Slot 1 supports half-height, half-length cards</li> <li>• Slot 2 supports full-height, half-length cards</li> </ul>	No additional options
Hot-swap fans	Six	No additional options

*Table continues...*

Component	Minimum specification	Upgrade options based on product requirements
Power supply	One 675W, 12V AC power supply	Redundant 675W, 12V AC power supply
Video controller	<p>Integrated Matrox G200 (two analog ports, one front and one back, that can be connected at the same time)</p> <p>The maximum video resolution is 1280 x 1024 at 75 Hz.</p> <ul style="list-style-type: none"> <li>• SVGA compatible video controller</li> <li>• DDR2 250 MHz SDRAM video memory controller</li> <li>• Avocent Digital Video Compression</li> <li>• Video memory is not expandable</li> </ul>	No additional options

---

## S8800 Server environmental requirements

Server status	Air temperature	Maximum altitude	Relative humidity
Server on	10° C to 35° C (50° F to 95° F) at altitude of up to 914.4 m (3,000 feet)	2,133 m (7,000 feet)	8% to 80%
	10° C to 32° C (50° F to 90° F) at altitude of 914.4 m to 2,133 m (3,000 to 7,000 feet)		
Server off	10° C to 43° C (50.0° F to 109.4° F)	2,133 m (7,000 feet)	8% to 80%

---

## Safety instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system and working environment from potential damage.

Observe the following precautions for rack stability and safety. Also refer to the rack installation documentation accompanying the rack for specific caution statements and procedures.

Systems are considered to be components in a rack. Thus, *component* refers to any system as well as to various peripherals or supporting hardware.

 **Danger:**

- Before installing systems in a rack, install front and side stabilizers on stand-alone racks or the front stabilizer on racks that are joined to other racks. Failure to install stabilizers before installing systems in a rack could cause the rack to tip over, potentially resulting in bodily injury.
- After installing components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack because the slide rails can pinch your fingers.

 **Note:**

- Your system is safety-certified as a free-standing unit and as a component for use in a rack cabinet using the customer rack kit. It is your responsibility to ensure that the final combination of system and rack complies with all applicable safety standards and local electric code requirements.
- System rack kits are intended to be installed in a rack by trained service technicians.

 **Important:**

- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack:
  - Do not block any air vents. Usually 15 cm (6 in.) of space provides proper airflow.
  - Install the server only in a rack cabinet with perforated doors.
  - Do not leave open spaces above or below an installed server in your rack cabinet. To help prevent damage to server components, always install a blank filler panel to cover the open space and to help ensure proper air circulation.
- Do not step on or stand on any component when servicing other components in a rack.
- Do not place any object on top of rack-mounted components.

---

## Avaya-provided equipment

Avaya provides the following equipment:

- Server and power cord or cords
- Slide rails
- Cable management arm assembly
- Cable management arm stop bracket
- Cable management arm mounting bracket

- Cable management support arm
- Two 10–32 screws
- Four M6 screws
- Five small cable ties
- One large cable tie
- Compact flash reader, USB cable, and flashcard (for backing up files. Included when required by the product ordered.)
- Modem and USB or serial cable (for remote maintenance. Included when required by the product ordered.)
- Other hardware as ordered, such as uninterruptible power source (UPS).

---

## Customer-provided equipment

The customer must provide the following equipment:

- Standard 19-inch four-post equipment rack that is properly installed and solidly secured. The rack must meet the following standards:
  - American National Standards Institute and Electronic Industries Association standard ANSI/EIA-310–D-92.
  - International Electrotechnical Commission standard IEC 297
  - Deutsche Industrie Norm standard DIN 41494
- Screws that come with the racks for installing the rails
- #2 cross-point (Phillips) screwdriver or 3/8 inch flathead screwdriver
- USB keyboard, USB mouse, and monitor must be available on the site for advanced installation or troubleshooting.
- Power from a nonswitched electrical outlet
- Access to the network

---

## Clearance requirements

Install the server in a rack that meets the following requirements:

- Minimum depth of 70 mm (2.76 inches) between the front mounting flange and inside of the front door if the server is installed in a cabinet.
- Minimum depth of 157 mm (6.18 inches) between the rear mounting flange and inside of the rear door if the server is installed in a cabinet.
- Minimum depth of 718 mm (28.27 inches) and maximum depth of 762 mm (30 inches) between the front and rear mounting flanges to support the use of the cable-management arm.

---

## Server installation checklist

No.	Task	Notes	✓
1	Verify that all equipment is on site.	Compare the list of items that were ordered to the contents of the boxes. Use the inventory list provided by your project manager. Do not rely on the packing slips inside the boxes for the correct information.	
2	Verify that the rack is installed according to the manufacturer's instructions and in accordance with all local codes and laws.		
3	Verify that the rack is grounded in accordance with local electrical code.	See <i>Approved Grounds</i> (555-245-772), available at <a href="http://support.avaya.com">http://support.avaya.com</a> .	
4	Remove the cabinet doors, if necessary.	See the cabinet manufacturer's documentation.	
7	<a href="#">Attach rails to the rack.</a> on page 239		
8	<a href="#">Install the server in the rack.</a> on page 242		
	<a href="#">Install the cable management arm</a> on page 243 (optional)		
9	Replace the cabinet doors, if necessary.	See the cabinet manufacturer's documentation.	
10	<a href="#">Turn on the server.</a> on page 248		
11	Troubleshoot the installation.		

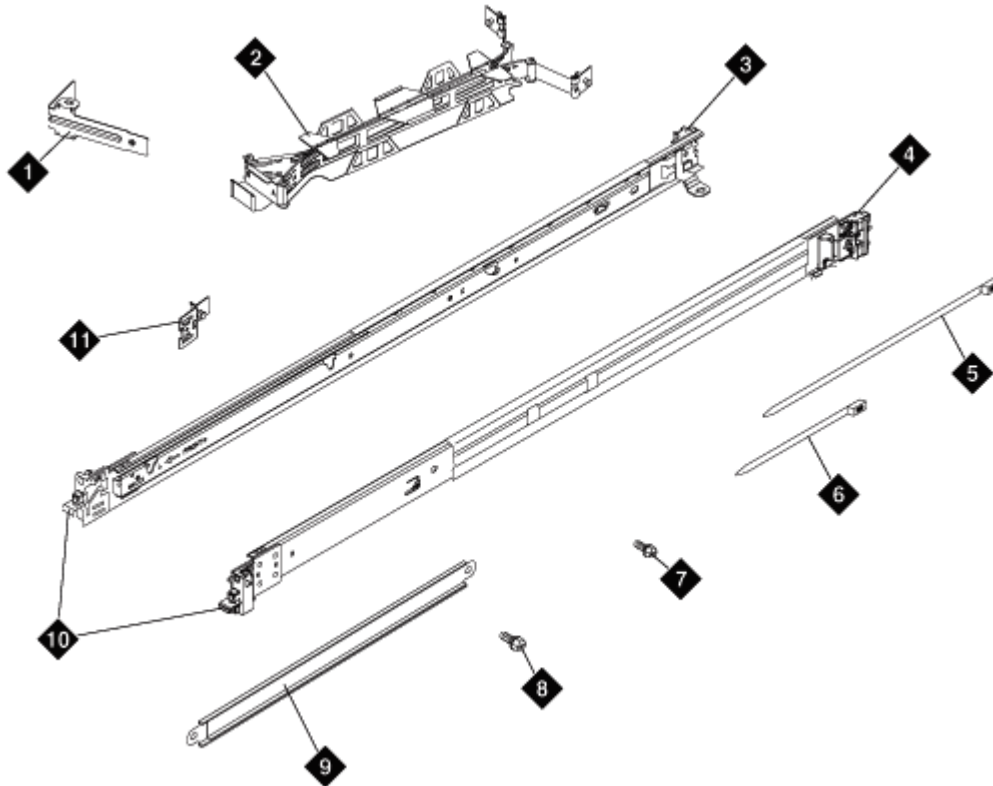
---

## Installing the Avaya S8800 Server

---

### Rack installation components

The following figure shows the items that you need to install the server in the rack cabinet.



hw88rokincmp LAO100209

1	Cable-management arm stop bracket (1)
2	Cable-management arm assembly
3	Slide rail (left)
4	Slide rail (right)
5	Large cable tie (1)
6	Cable ties (5)
7	M6 screws (4)
8	10–32 screws (2)
9	Cable-management support arm
10	Front of rails
11	Cable-management arm mounting bracket (1)

## Attaching the rails to the rack

### Before you begin

If the slide rails in your rack installation kit came with thumbscrews installed, remove them before you begin the following installation procedure.

## About this task

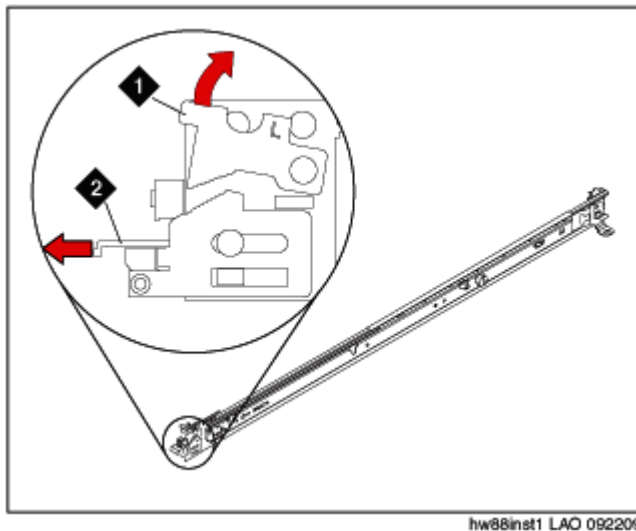
Each slide rail is marked with either an R (right) or an L (left).

### ! Important:

The slide rails that come with the server are compatible with standard 19-inch, 4-post racks that have *square* holes. If you are installing the server in any other type of rack, Avaya requires that the customer provide the appropriate rails or shelf for their rack. Rack Solutions has numerous rail kits and shelf options. This slide rail kit or a shelf would replace the Avaya-supplied slide rail kit that ships with the server .

## Procedure

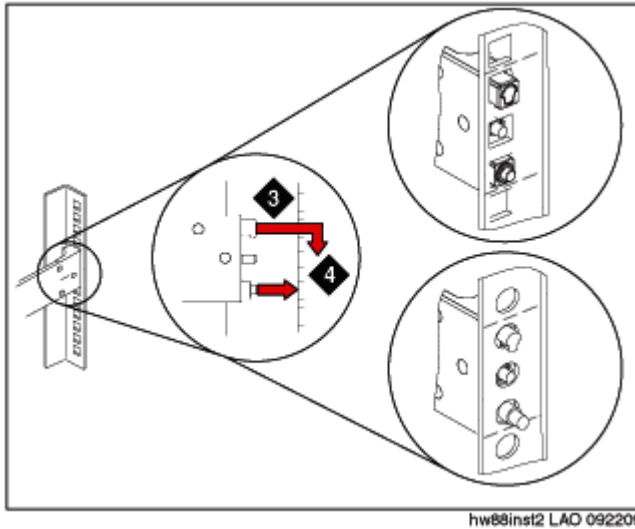
1. Select one of the slide rails and push up on the front moveable tab. See 1 in [Figure 2: Sliding out front side rail](#) on page 240.
2. Pull out the front latch to slide out the front side rail. See in 2 [Figure 2: Sliding out front side rail](#) on page 240.



**Figure 2: Sliding out front side rail**

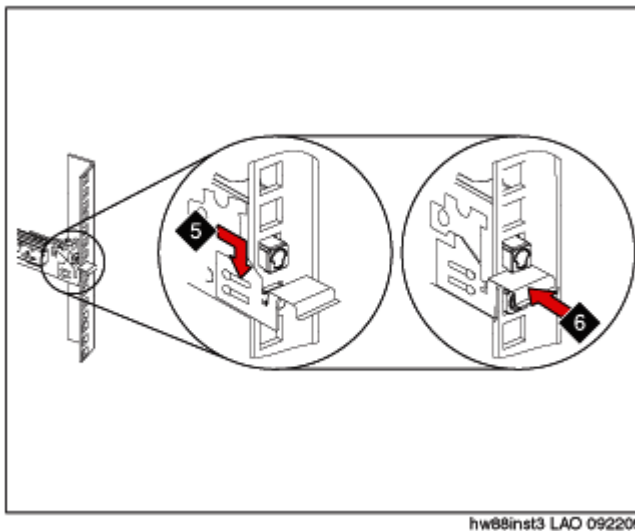
3. From the front of the rack, line up the three pins on the rear of the slide rail with the three holes in the selected U on the rear of the rack. Push the rails so that the pins go into the holes. See 3 in [Figure 3: Attaching slide rail to rear of rack](#) on page 241.
4. Drop the slide rail down until it latches into place. See 4 in [Figure 3: Attaching slide rail to rear of rack](#) on page 241.





**Figure 3: Attaching slide rail to rear of rack**

5. Pull the slide rail forward, and insert the two pins on the front of the rail into the two lower holes in the U on the front of the rack. See 5 in [Figure 4: Attaching slide rail to front of rack](#) on page 241. Drop the rail into place until it clicks.
6. Push the front latch in all the way. See 6 in [Figure 4: Attaching slide rail to front of rack](#) on page 241.



**Figure 4: Attaching slide rail to front of rack**

7. Repeat this procedure to install the other rail onto the rack.
8. Make sure that each front latch is fully engaged.

### Next steps

Install the server in the rack.

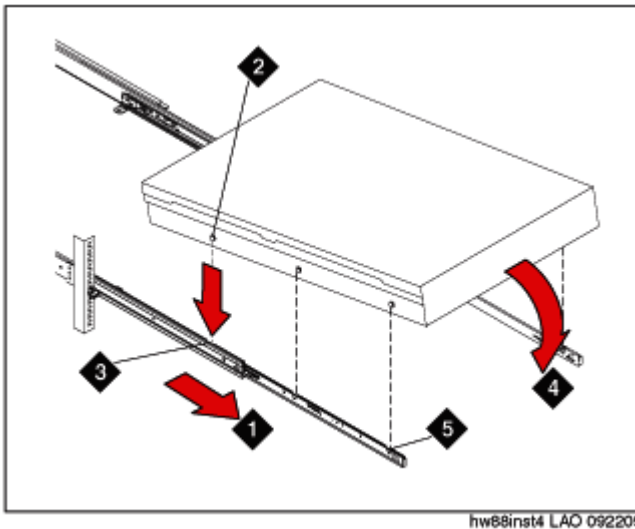
## Installing the server in the rack

### Before you begin

Attach rails to the rack.

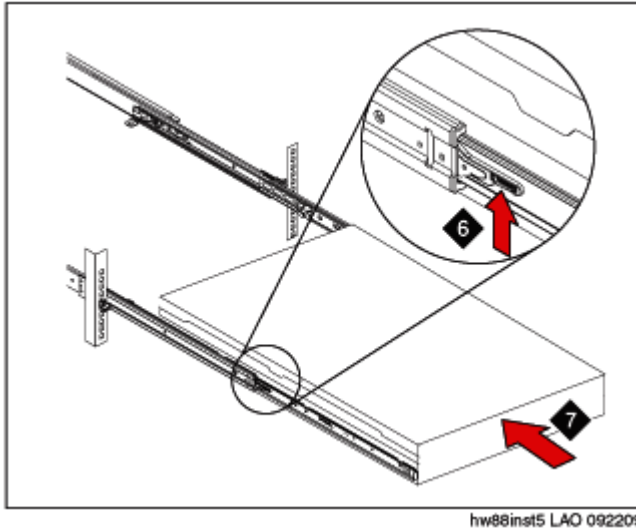
### Procedure

1. Pull the slide rails forward until they click, two times, into place. See 1 in [Figure 5: Attaching server to slide rails](#) on page 242.
2. Carefully lift the server and tilt it into position over the slide rails so that the rear nail heads on the server line up with the rear slots on the slide rails. See 2 and 3 in [Figure 5: Attaching server to slide rails](#) on page 242.
3. Slide the server down until the rear nail heads slip into the two rear slots.
4. Slowly lower the front of the server until the other nail heads slip into the other slots on the slide rails. See 4 in [Figure 5: Attaching server to slide rails](#) on page 242.
5. Make sure that the front latch slides over the nail heads. See 5 in [Figure 5: Attaching server to slide rails](#) on page 242.



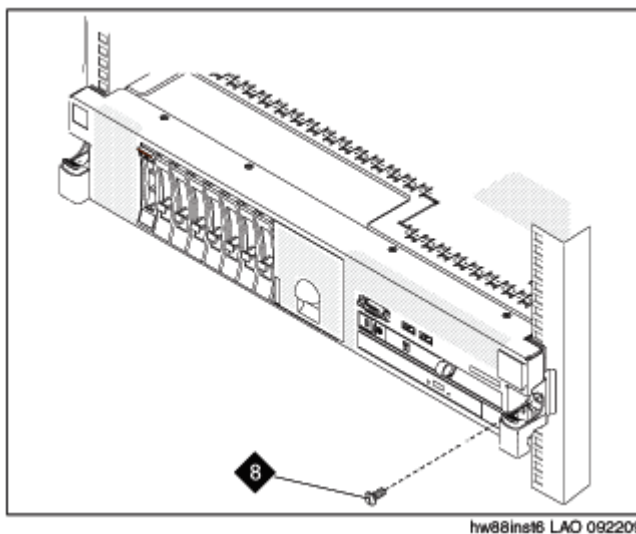
**Figure 5: Attaching server to slide rails**

6. Lift the locking levers on the slide rails. See 6 in [Figure 6: Locking server to slide rails](#) on page 243.
7. Push the server all the way into the rack until it clicks into place. See 7 in [Figure 6: Locking server to slide rails](#) on page 243.



**Figure 6: Locking server to slide rails**

8. Insert the optional M6 screws in the front of the server when you move the rack cabinet or if you install the rack cabinet in a vibration-prone area. See [Figure 7: Installing M6 screws](#) on page 243.



**Figure 7: Installing M6 screws**

### Next steps

Install the cable management arm if desired.

---

## Installing the cable management arm

### Before you begin

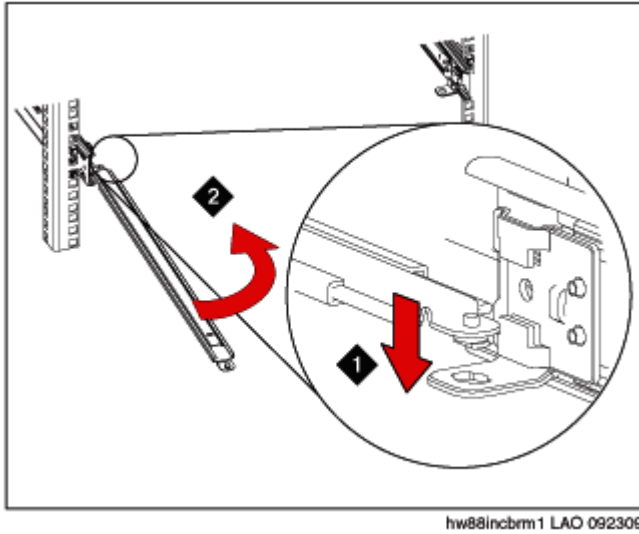
Attach rails to the rack and install the server in the rack.

## About this task

The cable-management arm can be installed on either side of the server. This procedure shows it being installed on the left side. To install the cable-management arm on the right side, follow the instructions and install the hardware on the opposite side.

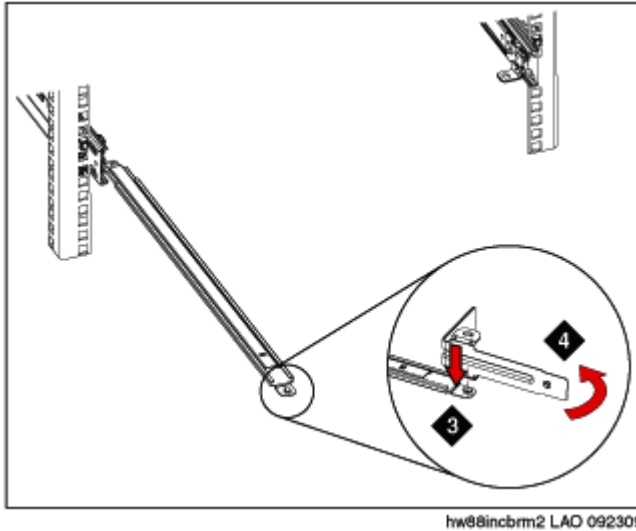
## Procedure

1. Connect one end of the support arm to the same slide rail to which you plan to attach the cable-management arm so that you can swing the other end of the support arm toward the rack. See [Figure 8: Attaching one end of support arm](#) on page 244.



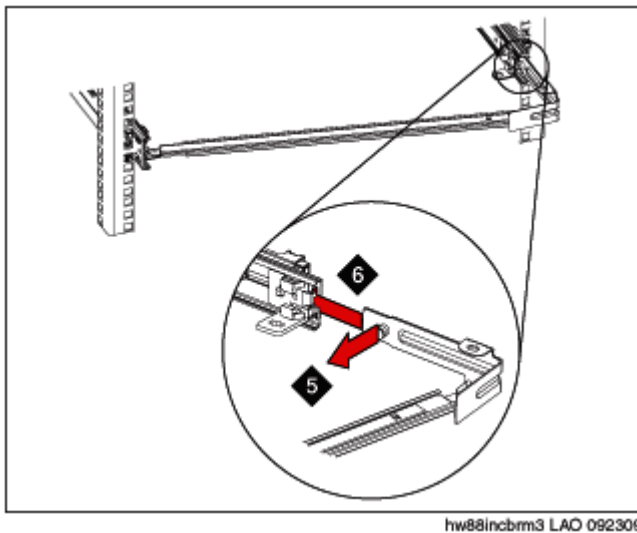
**Figure 8: Attaching one end of support arm**

2. Install the L-shaped cable-management stop bracket on the unattached end of the support arm. See 3 in [Figure 9: Installing stop bracket](#) on page 245
3. Turn the bracket to secure it to the support arm. See 4 in [Figure 9: Installing stop bracket](#) on page 245.



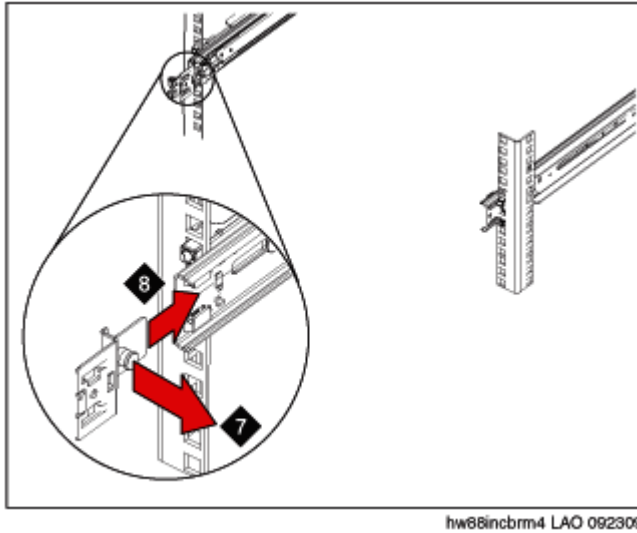
**Figure 9: Installing stop bracket**

4. To attach the other side of the support arm to the backside of the slide rail, pull the pin out, and then slide the bracket into the slide rail. See [Figure 10: Attaching other side of support arm](#) on page 245.



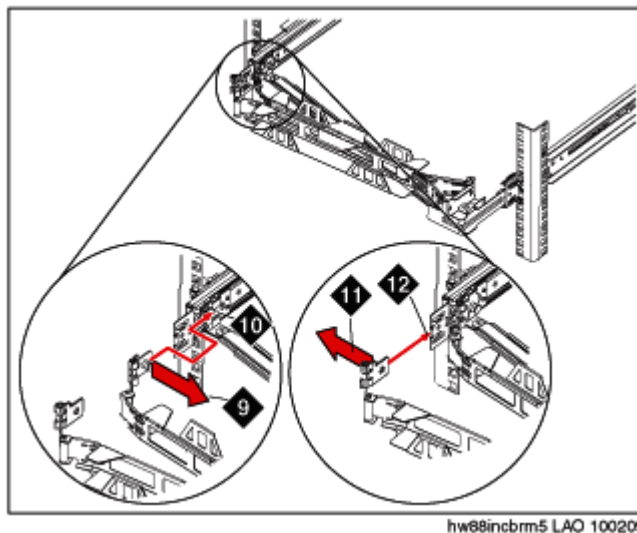
**Figure 10: Attaching other side of support arm**

5. Pull out the mounting bracket pin and slide the mounting bracket into the slide rail onto which you are installing the cable-management arm. See [Figure 11: Attaching mounting bracket](#) on page 246.



**Figure 11: Attaching mounting bracket**

6. Push the bracket into the slide rail until the spring-loaded pin snaps into place.
7. Place the cable-management arm on the support arm.
8. Pull out the cable-management arm pin, and then slide the cable-management arm tab into the slot on the inside of the slide rail. See 9 and 10 in [Figure 12: Attaching cable management arm to slide rail](#) on page 246.
9. Push the tab until it snaps into place.
10. Pull out the other cable-management arm pin, and then slide that cable management arm tab into the slot on the outside of the slide rail. See 11 and 12 in [Figure 12: Attaching cable management arm to slide rail](#) on page 246.



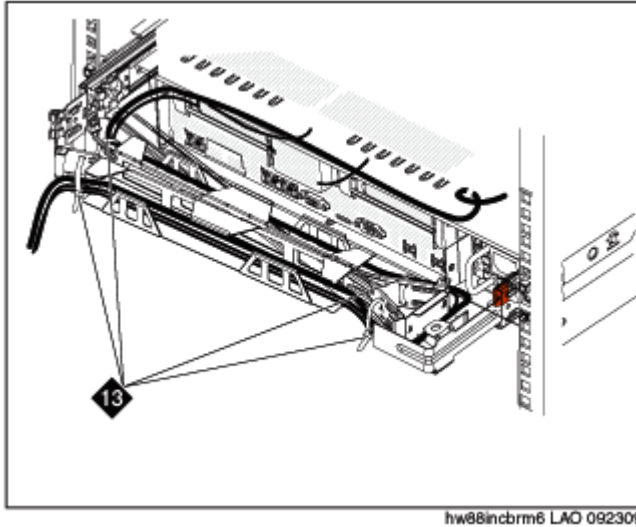
**Figure 12: Attaching cable management arm to slide rail**

11. Push the tab until it snaps into place.

12. Attach the power cords and other cables to the rear of the server (including keyboard, monitor, and mouse cables, if required).
13. Route the cables and power cords on the cable-management arm and secure them with cable ties or hook-and-loop fasteners. See [Figure 13: Routing cables on cable management arm](#) on page 247.

**\* Note:**

Allow slack in all cables to avoid tension in the cables as the cable-management arm moves.



**Figure 13: Routing cables on cable management arm**

14. Slide the server into the rack until it snaps into place.
15. Insert the optional M6 screws in the front of the server when you move the rack cabinet or if you install the rack cabinet in a vibration-prone area. See [Figure 14: Inserting M6 screws](#) on page 248.

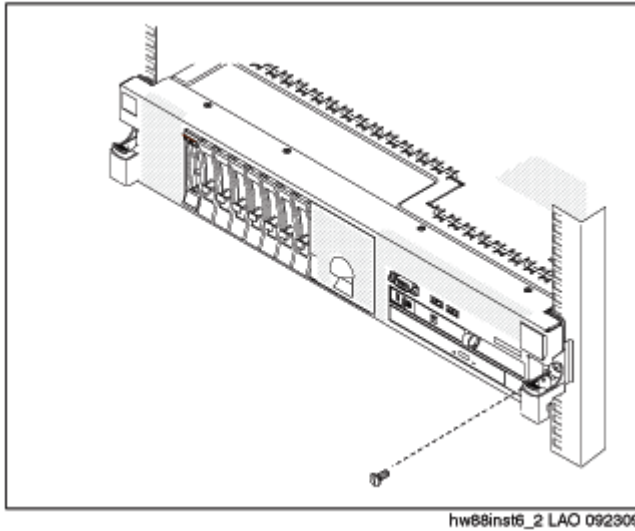


Figure 14: Inserting M6 screws

---

## Turning on the server

### About this task

After the server is installed in the rack, turn on the server to make sure that it powers up properly. Once you determine that it powers up properly, turn it off before you start any software installation procedure.

### ! Important:

You must wait for the power-on LED to blink slowly (one flash per second) before pressing the power button. If you press the power button while the power-on LED is blinking quickly (three flashes per second), the server will not turn on.

### Procedure

1. Plug one end of the power cord into the server power supply and the other end into a UPS or nonswitched outlet.

Approximately 5 seconds after the server is connected to power, one or more fans might start running to provide cooling, and the power-on LED will blink quickly (three flashes per second). Approximately 3 minutes after the server is connected to power, the power-on LED will blink slowly (one flash per second), and one or more fans might start running.

2. Once the power-on LED begins to blink slowly, press the power button on the front of the server.

The power-on LED will stop blinking and stay lit. After you press the power button, the server takes approximately 5 minutes to initialize.



## Next steps

See the specific product documentation for information on installing the operating system and software.

---

# Connecting the server to the network

## Procedure

1. To connect a monitor and a keyboard to the server, use the video connector and USB ports in the server. See [Front of server](#) on page 230.
2. To connect the servers to the customer's network, connect the cable to Ethernet connector port (eth0). See [Back of server](#) on page 232.
3. To connect the server for High Availability Failover, connect the eth cables to the Dual NIC High Availability Failover configured port. See [Back of server](#) on page 232.

For High Availability Failover, both servers must be in close proximity so that they can be connected with the crossover cable. The Ethernet specification limit for this distance is 100 meters.

# Index

## Numerics

10 Gb network-interface card  
installing .....59

## A

Access Security Gateway  
reinstalling the default authentication file .....121  
replacing the default authentication file .....121  
activating license entitlements .....214  
active server  
manually changing to standby .....115  
adding a local WebLM server .....226  
admin password .....85  
AE Services  
documentation .....11  
AE Services 6.3.3 feature pack  
installing .....193  
AES Ethernet interface .....20  
AES on System Platform offer .....16  
AES template  
prerequisites for installing .....117  
altitude .....45  
altitude requirements .....235  
Application Enablement Services on System Platform High  
Availability Failover (High Availability Failover) .....16  
Application Enablement Services on System Platform  
installation overview .....27

## B

backup  
about .....159  
back view .....43  
baseline specifications, configuration, and options .....44  
browser  
System Platform support .....88  
btu .....46

## C

cable management arm  
installing .....243  
Cdom and SAL Gateway  
IP address assignments .....160  
Change Password page in WebLM .....227  
changing the allocations of a license file .....228  
checklist  
installation .....53, 65  
reinstallation .....33, 200  
clearance requirements .....237

client application computer  
requirements .....23  
command line  
accessing Console Domain .....90  
accessing System Domain .....89  
commit  
template upgrade .....188  
Commit .....172  
Communication Manager  
requirements .....23, 24  
comparison of standard licensing and enterprise-wide  
licensing .....220  
computer requirements .....23  
Configure HA  
field descriptions .....110  
console domain  
configuring network settings .....77  
Console Domain  
accessing command line .....90  
Console Domain Network Configuration screen  
configuring .....77  
craft password .....85  
CTI link requirements .....23  
cust password .....85

## D

date  
configuring .....82  
Date/Time and NTP setup screen  
configuring .....82  
delays on communications channel .....23  
Dell R610 server .....58  
Del R610 server  
specifications .....58  
documentation  
document set .....41, 49  
downloading .....40, 49  
downloading software .....36  
Dual NIC configuration guidelines .....21  
duplex settings for AES .....22  
DVD  
does not mount automatically .....196  
requirements .....37  
writing ISO image .....38

## E

electrical specifications .....46  
electric input requirements .....233  
enabling Services-VM .....188  
enterprise-wide licensing .....220  
environmental specifications .....46, 235

equipment		
Avaya provided	<a href="#">236</a>	
Avaya-provided	<a href="#">28</a>	
customer provided	<a href="#">237</a>	
customer-provided	<a href="#">29</a>	
<b>F</b>		
fan		
specifications	<a href="#">234</a>	
feature pack 6.3.3		
installing	<a href="#">193</a>	
feature packs	<a href="#">92</a> , <a href="#">165</a>	
installation	<a href="#">93</a> , <a href="#">166</a>	
field descriptions		
Managed Element page	<a href="#">137</a>	
Patch Detail page	<a href="#">102</a>	
Patch List page	<a href="#">102</a>	
Platform Upgrade page	<a href="#">173</a>	
Proxy Server page	<a href="#">129</a>	
Search Local and Remote Patch page	<a href="#">100</a>	
Firefox		
disabling proxy servers	<a href="#">70</a>	
System Platform support	<a href="#">88</a>	
front view	<a href="#">41</a>	
<b>G</b>		
Gateway Configuration		
field descriptions	<a href="#">127</a>	
<b>H</b>		
hard disk drive		
specifications	<a href="#">234</a>	
hashing passwords	<a href="#">182</a>	
heat output	<a href="#">233</a>	
High Availability		
and template configuration	<a href="#">105</a>	
applying System Platform patches	<a href="#">97</a> , <a href="#">176</a>	
common prerequisites	<a href="#">106</a>	
configuring local	<a href="#">108</a>	
FRHA/LMHA/MPHA prerequisites	<a href="#">107</a>	
manually interchanging node roles	<a href="#">115</a>	
prerequisites	<a href="#">106</a>	
removing configuration	<a href="#">115</a> , <a href="#">176</a>	
start/stop	<a href="#">113</a>	
starting	<a href="#">113</a> , <a href="#">178</a>	
stopping	<a href="#">114</a> , <a href="#">158</a>	
stopping and starting for upgrades	<a href="#">175</a>	
High Availability;		
System Platform	<a href="#">105</a>	
High Availability systems		
about platform upgrades	<a href="#">144</a>	
upgrading System Platform	<a href="#">177</a>	
HP DL360 G7 server		
specifications	<a href="#">50</a>	
HP DL360 G7 Server		
back view	<a href="#">52</a>	
electrical specifications	<a href="#">50</a>	
environmental specifications	<a href="#">51</a>	
front view	<a href="#">51</a>	
physical specifications	<a href="#">50</a>	
power specifications	<a href="#">50</a>	
humidity requirements	<a href="#">46</a> , <a href="#">235</a>	
<b>I</b>		
installation		
checklist	<a href="#">65</a>	
process	<a href="#">25</a>	
using laptop	<a href="#">70</a>	
using server console	<a href="#">71</a>	
worksheet	<a href="#">29</a> , <a href="#">202</a>	
installation checklist		
server	<a href="#">238</a>	
installing	<a href="#">47</a>	
installing AES 6.3.1 template	<a href="#">192</a>	
installing AE Services 6.3.1 feature pack	<a href="#">193</a>	
installing AES template	<a href="#">118</a>	
installing the license file	<a href="#">224</a>	
interface speed for AES	<a href="#">22</a>	
Internet Explorer		
disabling proxy servers	<a href="#">69</a>	
System Platform support	<a href="#">88</a>	
IP address		
assignments for Cdom and SAL Gateway	<a href="#">160</a>	
IP forwarding		
disabling	<a href="#">88</a>	
enabling	<a href="#">88</a>	
IP settings		
configuring on laptop	<a href="#">68</a>	
ISO image		
verifying on DVD	<a href="#">74</a>	
verifying on Linux-based computer	<a href="#">36</a>	
verifying on Windows-based computer	<a href="#">37</a>	
writing to DVD or CD	<a href="#">38</a>	
<b>K</b>		
keyboard		
selecting type	<a href="#">72</a>	
Keyboard Type screen	<a href="#">72</a>	
<b>L</b>		
laptop		
configuring to connect to server	<a href="#">68</a>	
connecting to server	<a href="#">87</a>	
using to install System Platform	<a href="#">70</a>	
ldap password	<a href="#">85</a>	
legal notices		

## Index

license entitlements	
activating .....	<a href="#">214</a>
searching for .....	<a href="#">215</a>
licensing	
change in System Platform 6.3.1 .....	<a href="#">181</a>
comparison of standard licensing and enterprise-wide .....	
licensing .....	<a href="#">220</a>
configuration examples .....	<a href="#">221</a> , <a href="#">223</a>
enterprise-wide .....	<a href="#">222</a>
standard .....	<a href="#">221</a>
<b>M</b>	
managed element	
adding in SAL Gateway .....	<a href="#">136</a>
worksheet for SAL Gateway .....	<a href="#">136</a> , <a href="#">213</a>
Managed Element page	
field descriptions .....	<a href="#">137</a>
MD5 hashing .....	<a href="#">182</a>
media drive	
specifications .....	<a href="#">234</a>
media server requirements .....	<a href="#">23</a> , <a href="#">24</a>
memory	
specifications .....	<a href="#">234</a>
microprocessor	
specifications .....	<a href="#">234</a>
<b>N</b>	
network	
interface speed and duplex settings .....	<a href="#">22</a>
latency requirements .....	<a href="#">23</a>
Network interfaces .....	<a href="#">19</a>
Network interfaces, required settings .....	<a href="#">22</a>
Network Management Systems page	
field descriptions .....	<a href="#">134</a>
network settings	
configuring for console domain .....	<a href="#">77</a>
configuring for system domain (domain-0) .....	<a href="#">74</a>
NIC	
installing .....	<a href="#">59</a>
NIC, recommended settings .....	<a href="#">22</a>
NMS	
configuring for SAL Gateway .....	<a href="#">133</a>
field descriptions .....	<a href="#">134</a>
noise emissions .....	<a href="#">233</a>
notices, legal .....	
NTP server	
configuring in System Platform .....	<a href="#">82</a>
<b>P</b>	
packet delivery time .....	<a href="#">23</a>
passwords	
configuring in System Platform .....	<a href="#">82</a>
default .....	<a href="#">82</a>
hashing .....	<a href="#">182</a>
Passwords screen	
configuring .....	<a href="#">82</a>
field descriptions .....	<a href="#">85</a>
patch	
commit and rollback .....	<a href="#">93</a>
Patch Detail page	
field descriptions .....	<a href="#">102</a>
patches	
about .....	<a href="#">93</a>
committing .....	<a href="#">98</a>
downloading .....	<a href="#">95</a>
installing .....	<a href="#">96</a>
removing .....	<a href="#">99</a>
rolling back .....	<a href="#">99</a>
solution template .....	<a href="#">155</a>
System Platform .....	<a href="#">155</a>
Patch List page	
field descriptions .....	<a href="#">102</a>
PCI slot	
specifications .....	<a href="#">234</a>
periodic spiked delays .....	<a href="#">23</a>
ping, measure round-trip packet delivery time .....	<a href="#">23</a>
Platform upgrade	
verifying .....	<a href="#">170</a>
Platform Upgrade page	
field descriptions .....	<a href="#">173</a>
PLDS .....	<a href="#">35</a>
downloading software .....	<a href="#">36</a>
power specifications .....	<a href="#">46</a>
power supply	
specifications .....	<a href="#">234</a>
preinstallation checklist .....	<a href="#">33</a> , <a href="#">200</a>
prerequisite	
assigning new IP addresses to Cdom VM and embedded SAL Gateway on-site .....	<a href="#">163</a>
assigning new IP addresses to the Cdom VM and embedded SAL Gateway remotely .....	<a href="#">161</a>
prerequisites	
for System Platform upgrade .....	<a href="#">155</a>
for System Platform upgrade on HA systems .....	<a href="#">157</a>
Product ID	
changing for System Platform .....	<a href="#">125</a>
product registration .....	<a href="#">124</a>
proxy	
configuring .....	<a href="#">96</a>
configuring for System Platform .....	<a href="#">117</a>
proxy server	
configuring for SAL Gateway .....	<a href="#">129</a>
Proxy Server page	
field descriptions .....	<a href="#">129</a>
proxy servers	
disabling in Firefox .....	<a href="#">70</a>
disabling in Internet Explorer .....	<a href="#">69</a>

**R**

rack	
attaching rails	<a href="#">239</a>
installing server	<a href="#">242</a>
RAID controller	
specifications	<a href="#">234</a>
rails	
attaching to rack	<a href="#">239</a>
regenerating a license file	<a href="#">218</a>
registering	<a href="#">35</a>
registration	
of system	<a href="#">34</a>
rehosting	<a href="#">217</a>
remote server	
configuring	<a href="#">132</a>
field descriptions	<a href="#">133</a>
Remote Server	
field descriptions	<a href="#">133</a>
Removing the HA configuration	<a href="#">115</a> , <a href="#">176</a>
requirements	
client application computer	<a href="#">23</a>
for System Platform installation	<a href="#">28</a> , <a href="#">29</a>
media server	<a href="#">23</a> , <a href="#">24</a>
rollback	
template upgrade	<a href="#">188</a>
Rollback	<a href="#">172</a>
root password	<a href="#">85</a>

**S**

safety instructions	<a href="#">235</a>
SAL Core Server	
configuring	<a href="#">131</a>
field descriptions	<a href="#">131</a>
SAL gateway	
deployment on Services Virtual Machine	<a href="#">144</a>
SAL Gateway	<a href="#">123</a>
adding a managed element	<a href="#">136</a>
applying configuration changes	<a href="#">135</a>
browser requirements	<a href="#">125</a>
configuring	<a href="#">126</a>
configuring a proxy server	<a href="#">129</a>
configuring Concentrator Core Server	<a href="#">131</a>
configuring network management system	<a href="#">133</a>
configuring NMS servers	<a href="#">134</a>
configuring remote server	<a href="#">132</a> , <a href="#">133</a>
configuring SAL Core Server	<a href="#">131</a>
disabling	<a href="#">139</a>
enabling	<a href="#">187</a>
managing service control and status	<a href="#">134</a>
prerequisites for configuration	<a href="#">124</a>
registering	<a href="#">34</a>
starting user interface	<a href="#">126</a>
worksheet for managed elements	<a href="#">136</a> , <a href="#">213</a>
SAL troubleshooting	<a href="#">197</a>
searching for license entitlements	<a href="#">215</a>

Search Local and Remote Patch page	
field descriptions	<a href="#">100</a>
Search Local and Remote Template page	
field descriptions	<a href="#">119</a>
Secure Access Gateway Server	<a href="#">123</a>
server	
back view	<a href="#">232</a>
components	<a href="#">234</a>
connecting laptop	<a href="#">87</a>
dimensions	<a href="#">233</a>
front view	<a href="#">230</a>
hardware requirements	<a href="#">64</a>
installing in rack	<a href="#">242</a>
manually interchanging node roles	<a href="#">115</a>
specifications	<a href="#">50</a> , <a href="#">58</a> , <a href="#">233</a>
turning on	<a href="#">248</a>
weight	<a href="#">233</a>
Server	
hardware checks	<a href="#">73</a>
server console	
using to install System Platform	<a href="#">71</a>
server overview	<a href="#">39</a>
service packs	
System Platform	<a href="#">155</a>
services port	
accessing System Platform through	<a href="#">88</a>
Services virtual machine (VM)	
installing	<a href="#">79</a>
Services VM	
about upgrade	<a href="#">182</a>
network configuration	
field descriptions	<a href="#">81</a>
Services-VM	
enabling	<a href="#">188</a>
upgrade	<a href="#">182</a>
Services-VM upgrade	
verify	<a href="#">186</a>
SHA2 hashing	<a href="#">182</a>
Single NIC configuration guidelines	<a href="#">21</a>
SNMP	<a href="#">179</a>
configuring v2c or v3 version support	<a href="#">180</a>
Master Agent configuration	<a href="#">180</a>
SNMP configuration	<a href="#">179</a>
SNMP trap receivers	
adding	<a href="#">139</a>
solution template	
and High Availability Failover	<a href="#">105</a>
patches	<a href="#">155</a>
registering applications	<a href="#">34</a>
Status	
SAL Gateway service	<a href="#">134</a>
support	
contact	<a href="#">14</a>
System Domain	
accessing command line	<a href="#">89</a>
system domain (domain-0)	
configuring network settings	<a href="#">74</a>

## Index

System Domain Network Configuration screen		
field descriptions .....	<a href="#">76</a>	
System Platform		
applying patches to HA systems .....	<a href="#">97</a> , <a href="#">176</a>	
High Availability		
field descriptions .....	<a href="#">110</a>	
High Availability field descriptions .....	<a href="#">110</a>	
prerequisites for upgrade .....	<a href="#">155</a>	
prerequisites for upgrade on HA systems .....	<a href="#">157</a>	
registering .....	<a href="#">34</a>	
service packs and patches .....	<a href="#">155</a>	
upgrade checklist .....	<a href="#">145</a>	
upgrade checklist for HA system .....	<a href="#">147</a>	
upgrade files and patches .....	<a href="#">148</a>	
upgrade paths .....	<a href="#">150</a> , <a href="#">151</a>	
upgrade process for different deployments .....	<a href="#">166</a>	
upgrading .....	<a href="#">167</a>	
System Platform upgrade		
service continuity .....	<a href="#">143</a>	
to 6.3.4 .....	<a href="#">143</a>	
System Platform Web Console		
accessing .....	<a href="#">88</a>	
<b>T</b>		
Telnet		
opening session from laptop to System Platform server		
.....	<a href="#">70</a>	
temperature requirements .....	<a href="#">46</a> , <a href="#">235</a>	
template		
and High Availability Failover .....	<a href="#">105</a>	
committing or rolling back upgrade .....	<a href="#">188</a>	
prerequisites for installing .....	<a href="#">117</a>	
time		
configuring .....	<a href="#">82</a>	
time zone		
configuring .....	<a href="#">81</a>	
Time Zone Selection screen		
configuring .....	<a href="#">81</a>	
training .....	<a href="#">13</a>	
troubleshooting		
DVD does not mount .....	<a href="#">196</a>	
failure to access Web console .....	<a href="#">196</a>	
failure to ping Console Domain .....	<a href="#">196</a>	
multiple reinstallations can result in an out of memory		
error .....	<a href="#">199</a>	
SAL not working .....	<a href="#">197</a>	
turning on server .....	<a href="#">248</a>	
<b>U</b>		
upgrade		
checklist for System Platform .....	<a href="#">145</a>	
checklist for System Platform HA system .....	<a href="#">147</a>	
files and patches .....	<a href="#">148</a>	
service continuity during System Platform .....	<a href="#">143</a>	
Services-VM .....	<a href="#">182</a>	
System Platform 6.3.4 .....	<a href="#">143</a>	
verifying .....	<a href="#">170</a>	
upgrade paths		
System Platform .....	<a href="#">150</a> , <a href="#">151</a>	
upgrade process for System Platform		
different deployments .....	<a href="#">166</a>	
upgrades		
Services VM .....	<a href="#">182</a>	
stopping and starting High Availability .....	<a href="#">175</a>	
upgrading .....	<a href="#">141</a>	
System Platform .....	<a href="#">167</a>	
upgrading AES template .....	<a href="#">190</a>	
upgrading System Platform		
on High Availability systems .....	<a href="#">177</a>	
<b>V</b>		
verify		
Services-VM upgrade .....	<a href="#">186</a>	
verifying the license allocations on the local WebLM server		
.....	<a href="#">229</a>	
video controller		
specifications .....	<a href="#">234</a>	
videos .....	<a href="#">14</a>	
Virtual Machine Management page		
field descriptions .....	<a href="#">119</a>	
voltage .....	<a href="#">46</a>	
VSP Console Domain Network Configuration screen		
configuring .....	<a href="#">77</a>	
field descriptions .....	<a href="#">78</a>	
vspmediacheck .....	<a href="#">74</a>	
<b>W</b>		
Web browser		
System Platform support .....	<a href="#">88</a>	
Web Console		
accessing .....	<a href="#">88</a>	
WebLM license .....	<a href="#">141</a>	
worksheet		
installation .....	<a href="#">29</a> , <a href="#">202</a>	
SAL Gateway managed elements .....	<a href="#">136</a> , <a href="#">213</a>	