# Deploying Avaya Aura® Messaging for Single Server Systems

Release 6.3.3
Issue 1
August 2015

**Notice**

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

**Documentation disclaimer**

“Documentation” means information published 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.

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

**Hosted Service**

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, 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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a 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.

**Licence 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.

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.

**Virtualization**

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

**Third Party Components**

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: 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.

**Note to Service Provider**

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

**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.

**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.

**Trademarks**

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

Avaya is a registered trademark of Avaya Inc.

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

# Contents

# Chapter 1: Introduction

## Purpose

This document provides installation, configuration, initial administration, and basic maintenance checklists and procedures.

## Intended audience

This document is intended for people who install and configure a verified reference configuration at a customer site.

## Document changes since last issue

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

- Added Release 6.3.3 enhancements

## Related resources

### Documentation

You can download the documents you need from the Avaya Support website at http://support.avaya.com. In addition to the documentation listed here, you can download a zip file that is a compilation of the Avaya Aura® Messaging documentation library. You can install this library on a computer or on your corporate network.

The Avaya Support website also includes the latest information about product compatibility, ports, and Avaya Aura® Messaging releases.

## Security

| Title | Description | Audience |
|---|---|---|
| *Avaya Aura® Messaging Security Design* | Discusses security issues to consider when designing a corporate security strategy. Topics include network security, toll fraud, and recommendations for maintaining a secure system. | Solution architects, deployment engineers, and administrators |

## Single server configurations

| Title | Description | Audience |
|---|---|---|
| *Avaya Aura® Messaging Single Server Reference Configuration* | Describes the design, capacities, interoperability, and limitations of single-server configurations. | Sales and deployment engineers, solution architects, and support personnel |
| *Upgrading Avaya Aura® Messaging for Single Server Systems* | Describes end-to-end upgrade scenarios for this configuration. | Deployment engineers and support personnel |

You might find the following Avaya Aura® documents useful:

- *Installing and Configuring Avaya Aura® System Platform*
- *Administering Avaya Aura® System Platform*
- *Secure Access Link Gateway Implementation*

## Administration

| Title | Description | Audience |
|---|---|---|
| *Administering Avaya Aura® Messaging* | Explains how to use the System Management Interface (SMI) to configure your system, use reports and diagnostic tools, manage software and users, and perform routine maintenance tasks.<br>The content is available in two formats: HTML and PDF. | Administrators |
| *Job aid for Administering Avaya Aura® Messaging* | Includes routine administration tasks. This job aid is a subset of the administration guide. | Administrators |
| *Avaya Aura® Messaging Alarms and Events* | Describes system alarms, events, and repair procedures. | Administrators and support personnel |

## User functions

| Title | Description | Audience |
|---|---|---|
| *Using Avaya Aura® Messaging* | Explains how to set up and use User Preferences and the Messaging toolbar in your email client.<br>The content is available in two formats: HTML and PDF. | Users |
| *Using Avaya Aura® Messaging Job Aid* | Includes the most common user tasks. This job aid is a subset of the user guide. | Users and support personnel |
| *Avaya Aura® Messaging Quick Reference (Aria)* | Describes how to use the Aria telephone user interface. | Users |
| *Avaya Aura® Messaging Quick Reference (Audix®)* | Describes how to use the Audix® telephone user interface. | Users |
| *Avaya Aura® Messaging Quick Reference (CallPilot®)* | Describes how to use the CallPilot telephone user interface. | Users |

## Hardware

### New installations

| Title | Description | Audience |
|---|---|---|
| *Installing the Dell™ PowerEdge™ R610 server* | Describes the components, specifications, and configurations for this server. | Deployment engineers and support personnel |
| *Installing the Dell™ PowerEdge™ R620 server* | Describes the components, specifications, and configurations for this server. | Deployment engineers and support personnel |
| *Installing the HP ProLiant DL360 G7 server* | Describes the components, specifications, and configurations for this server. | Deployment engineers and support personnel |
| *Installing the HP ProLiant DL360p G8 server* | Describes the components, specifications, and configurations for this server. | Deployment engineers and support personnel |

### Maintenance

| Title | Description | Audience |
|---|---|---|
| *Maintaining the Avaya S8800 1U Server for Avaya Aura® Messaging* | Describes how to add, replace, and repair hardware components for this server. | Deployment engineers and support personnel |
| *Maintaining and Troubleshooting the Dell™ PowerEdge™ R610 server* | Describes how to add, replace, and repair hardware components for this server. Also provides | Deployment engineers and support personnel |

*Table continues…*

| Title | Description | Audience |
|---|---|---|
| | information about LCD status messages. | |
| *Maintaining and Troubleshooting the Dell™ PowerEdge™ R620 server* | Describes how to add, replace, and repair hardware components for this server. | Deployment engineers and support personnel |
| *Maintaining and Troubleshooting the HP ProLiant DL360 G7 server* | Describes how to add, replace, and repair hardware components for this server. | Deployment engineers and support personnel |
| *Maintaining and Troubleshooting the HP ProLiant DL360p G8 server* | Describes how to add, replace, and repair hardware components for this server. | Deployment engineers and support personnel |

# Training

You can get the following Messaging courses at https://www.avaya-learning.com. Enter the course code in the **Search** field and click **Go** to search for the course.

The course titles might differ from the titles shown.

| Course code | Course title |
|---|---|
| 2U00230W | Avaya UC Messaging — Overview |
| 2U00231W | Avaya UC Messaging — Heritage |
| 2U00232W | Avaya UC Messaging — Avaya Aura® Messaging |
| 2U00233O | Selling Avaya UC Messaging Learning Bytes |
| 3U00141W | Designing UC Messaging — Avaya Aura® Messaging |
| 5U00140E | Avaya Aura® Messaging Implementation and Support |
| 5U00141E | Avaya Aura® Messaging Administration |
| ATI01674VEN | Avaya Aura® Messaging — Caller Applications |

# Viewing Avaya Mentor videos

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

### About this task

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

### Procedure

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

**Note:**

Videos are not available for all products.

# Support

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

# Chapter 2: Single server configuration overview

## Avaya Aura® Messaging overview

Avaya Aura® Messaging is an enterprise-class messaging solution that is flexible, scalable, and resilient. Messaging can improve your business through quick and effective communication and collaboration.

Messaging provides powerful capabilities that deliver tangible benefits such as:

- Sending important calls to the right person, at the right time
- Alerting employees to critical new messages
- Providing fast and easy access to all messages
- Lowering the cost of acquisition, deployment, and ownership through standards-based interfaces that facilitate easy integration with your networks, administrative systems, and security processes
- Providing multiple configuration choices for scalability and resiliency

You can deploy Messaging on either:

- Avaya-provided hardware that runs Linux® and Avaya Aura® System Platform or
- Customer-provided hardware using VMware® in a virtualized environment

## Single server

In the single-server configuration, the application and storage roles are both active within one physical server. This configuration is an ideal solution for organizations up to a maximum of 6000 users. This configuration works well for small or distributed organizations and can accommodate the growth of these organizations.

The default Avaya-provided physical server comes on standard capacity hardware.

Customers with a Microsoft Exchange Server can configure their Avaya-provided physical server to send messages to their Exchange server.

# Avaya components

| Component | Version | Platform | Description |
|---|---|---|---|
| Avaya Aura® components | | | |
| Avaya Aura® Communication Manager | 6.3<br>6.3.2<br>6.3.6<br>6.3.8<br>7.0 | System Platform | The IP telephony foundation on which Avaya delivers intelligent communications to large and small enterprises. |
| Avaya Aura® Messaging | 6.3.2<br>6.3.3 | System Platform | A part of the Avaya Aura® architecture, but Messaging can also be used in other environments |
| Avaya Aura® Session Manager | 6.3.2<br>6.3.4<br>6.3.8<br>6.3.9<br>7.0 | System Platform | A SIP routing and integration tool that integrates SIP entities across the enterprise network. You can view and manage each location, branch, and application in totality, not as separate units within the enterprise. |
| Avaya Aura® System Manager | 6.3.2<br>6.3.4<br>6.3.8<br>6.3.9<br>6.3.10<br>7.0 | System Platform | A product that takes a solution-level approach to network administration.<br>System Manager centralizes provisioning, maintenance, and troubleshooting to simplify and reduce management complexity and solution servicing. System Manager provides a common management framework that reduces the complexity of operations for distributed multisite networks with multiple control points inherent in SIP. |
| Other Avaya components | | | |
| Avaya Voice Message Form | 6.3.1 | Microsoft Exchange Server | A component that provides a toolbar for Microsoft Office Outlook and Exchange Server. The tool supports playback of voice messages on your telephone through the computer. |
| Avaya WebLM | - | System Platform | A web-based license manager that manages licenses of one or more Avaya software products. |
| Message Networking | 5.2<br>6.3 | Avaya provided Server | A component that supports interoperability with legacy voice mail products. |
| one-X Speech | 5.2<br>6.3 | Avaya provided Server | A component that supports speech-based commands and text-to-speech functions for voice mail, email, calendar, and telephony functions. |
| Avaya service components | | | |
| Secure Access Link | 2.1 | | A component that remotely manages Messaging and sends alarms to Avaya Services. |

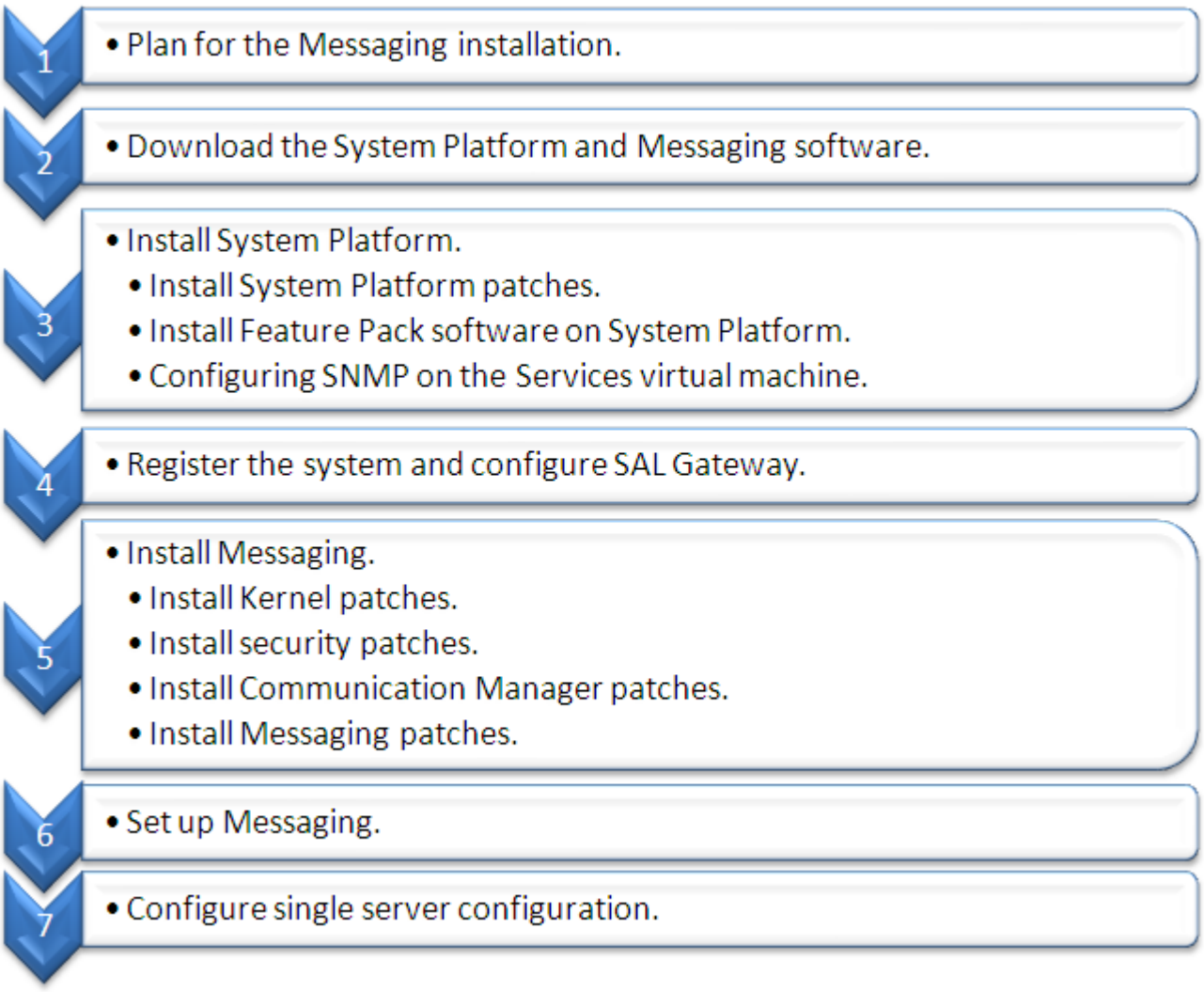
For more information about interoperability between these products, see *Avaya Aura® Messaging Overview and Specification* at the Avaya Support website: http://support.avaya.com.

## Product compatibility

For the latest and most accurate compatibility information go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

# Chapter 3: Deployment process

The following image shows the high-level tasks for deploying single server configuration.



# Chapter 4: Planning and preconfiguration

## Planning checklist

| No. | Tasks | References | Notes | ✔ |
|---|---|---|---|---|
| 1 | Download the required documentation. | See Documentation on page 6. | — | |
| 2 | Verify that all equipment is onsite. | — | Do not rely on the packing slip. Match the contents of the boxes shipped to you with the list of hardware and components that you ordered. If you find any discrepancy, immediately inform Avaya. | |
| 3 | Obtain the System Platform and Messaging software. | See Obtaining and Messaging software on page 31. | For more information on Messaging templates, see Messaging templates overview on page 28. | |

## Key customer configuration information

### Configuration information for System Platform installation

To record the System Platform installation information, print the following table and work with your network administrator to fill the empty cells.

## Proxy Configuration

| Name | Value | Description |
|---|---|---|
| **Status** | | Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform. |
| **Address** | | The address for the proxy server. |
| **Port** | | The port address for the proxy server. |

## 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 desired domain search path following the *search* 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, `SPCdom.mydomainname.com`. 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, `SPDom0.mydomainname.com`. Otherwise, just enter the IP |

*Table continues…*

| Name | Value | Description |
|---|---|---|
| | | 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. |
| **Physical Network Interface** | | The physical network interface details for eth0 and eth1 (and eth2 in case of High Availability Failover is enabled). |
| **Domain Dedicated NIC** | | 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 typically requires a separate cable connection to the customer network.<br>See template installation topics for more information. |
| **Bridge** | | The bridge details for the following:<br>• **avprivate**: 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.<br>• **avpublic**: 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 generally 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 |

*Table continues…*

| Name | Value | Description |
|---|---|---|
| | | Console Domain have on this bridge.<br>• **template bridge**: These bridges are created during the template installation and are specific to the virtual machines installed. |
| **Domain Network Interface** | | The domain network interface details for System Domain (Dom-0) or Console Domain that are grouped by domain based on your selection. |

## Services Virtual Machine Configuration

| Name | Value | Description |
|---|---|---|
| **Enable Services VM** | | Enables or disables remote access. Also supports local or centralized alarm reporting.<br>Default value: **Enabled**<br>Leave the **Enable services VM** 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. |
| **Hostname** | | The name assigned to the Services Virtual Machine |
| **Static IP address** | | 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. |
| **Virtual devices** | | The virtual device (port) assigned to the Services Virtual Machine. Default value (eth0) automatically assigned. No user input necessary. |

## 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. |
| **ldap Password** | | The password for the ldap login.<br>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 |
|---|---|---|
| **NTP server 1** | | The hostname or IP address of an NTP server, visible in the Web Console when you click **Query State** in the Date and Time Configuration page, under **Server Management**. When displayed, either of the following special characters precede each server hostname or IP address. Each character has a special meaning, as follows:<br>• Asterisk character (*): The preferred server (currently referenced by the local system), chosen by System Platform.<br>• Plus character (+): Indicates a high-quality candidate for the reference time that System Platform can use if its currently selected time source becomes unavailable.<br>Avaya preconfigures several server names prior to system delivery. You can add more NTP reference servers by clicking **Add** in the Date and Time Configuration page under **Server Management**. |

*Table continues…*

| Name | Value | Description |
|---|---|---|
| **NTP server 2** | | |
| **NTP server 3** | | |
| **NTP server 4** | | |

## Configuration information for the SAL Gateway configuration

To record the SAL Gateway configuration information, print the following table and work with your network administrator to fill the empty cells.

| Managed device (virtual machine) | IP address | SE ID | Product ID | Model | Notes |
|---|---|---|---|---|---|
| SAL | | | | | |
| System Domain (Dom 0) | | | | | System Domain, Dom 0, is not enabled with alarming but has a Product ID, that is Alarm ID.<br>Console Domain, cdom or udom, is enabled with alarming. System Domain sends all system logs to Console Domain, which then triggers alarms on behalf of System Domain. |
| Console Domain (cdom or udom) | | | | | |
| Messaging | | | | | |

## Configuration information for the Messaging installation

To record the Messaging installation information, print the following table and work with your network administrator to fill the empty cells.

| Field | Value | Notes |
|---|---|---|
| Host name | | The host name for Messaging.<br>The host name must be the Fully Qualified Domain Name (FQDN) of the Messaging virtual machine. |
| Msg IPv4 Address | | |

# Configuration information for the initial administration of Messaging

To record the Messaging initial administration information, print the following table and work with your network administrator to fill the empty cells.

## License management

| Field | Value | Notes |
|---|---|---|
| WebLM user ID | | |
| WebLM password | | |
| License Activation Code (LAC) | | The order number of the Primary Host ID. |
| License host | | |
| E-mail | | Email addresses of additional recipients of activation notification. |

## Authentication file management

| Field | Value | Notes |
|---|---|---|
| Communication Manager 6.x | | The FQDN of the Messaging virtual machine. |
| Utility Server 6.x | | The FQDN of System Platform Console Domain. |
| E-mail | | If you want to send the authentication file in an email message, use this field. |

## Privileged administrator login

| Field | Value | Notes |
|---|---|---|
| Privileged administrator user ID | | |
| Privileged administrator password | | |

## Software installer login

| Field | Value | Notes |
|---|---|---|
| Software installer user ID | | |

*Table continues…*

| Field | Value | Notes |
|---|---|---|
| Software installer password | | |

# Configuration tools and utilities

You must have the following tools and utilities for deploying and configuring Messaging:

- A laptop connected to the services port on the server.
- Video monitor, keyboard, and mouse connected to the appropriate ports on the server.
- A browser for accessing the Messaging System Management Interface pages.
- An sftp client for Windows, for example WinSCP.
- An ssh client, for example, PuTTy.

# Site preparation

## Hardware requirements

### 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

## Supported hardware

Messaging software runs on the following Avaya-provided servers:

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

If you already have the following servers in your network, you can use them with Messaging. However, you must first get an upgrade kit from your Avaya Services representative.

| Server | Supporting documentation |
|---|---|
| S8730 | *Maintaining the S8730 server for Modular Messaging* |
| CallPilot 1006r | *CallPilot 1006r Hardware Upgrade Instructions* |
| HP ProLiant DL360 G7 | *Maintaining and Troubleshooting the HP ProLiant DL360 G7 server* |
| S8800 1U | *Maintaining the Avaya S8800 1U Server for Avaya Aura® Messaging* |

You can download these documents from the Avaya Support website at http://support.avaya.com.

### Dell™ PowerEdge™ R620 specifications

| Component name | Standard server | High capacity server |
|---|---|---|
| Chassis | 1U | 1U |
| Processor speed | E5-2630 2.3 GHz 6-core | E5-2630 2.3 GHz 6-core |

*Table continues…*

| Component name | Standard server | High capacity server |
|---|---|---|
| Number of processors | 1 | 1 |
| Ethernet ports | 6 | 4 |
| RAID type | RAID 1 | RAID 5 |
| Disk | 2 x 300 GB 10K | 3 x 300 GB 15K |
| Standard power supply | 1 x 495 W | 2 x 495 W |

## Dell™ PowerEdge™ R610 specifications

| Component name | Standard server | High capacity server |
|---|---|---|
| Chassis | 1U | 1U |
| Processor speed | E5620 2.4 GHz 4-core | E5620 2.4 GHz 4-core |
| System memory | 12 GB | 12 GB |
| Ethernet ports | 2 | 2 |
| RAID type for phase 1 and 2 servers | RAID 5 | RAID 5 |
| Disk for phase 1 servers | 3 x 146 GB 10K | 4 x 146 GB 15K |
| Disk for phase 2 servers | 3 x 146 GB 15K | 4 x 146 GB 15K |
| Standard power supply | 1 x 502 W | 2 x 502 W |

**Note:**

Phase 1 servers shipped for the first half of the Dell Power Edge R610 general availability life cycle. Phase 2 servers shipped for the second half. The disk configuration for the phases are different.

## HP ProLiant DL360p G8 specifications

| Component name | Standard server | High capacity server |
|---|---|---|
| Chassis | 1U | 1U |
| Processor speed | E5-2630 2.3 GHz | E5-2630 2.3 GHz |
| Number of processors | 1 | 1 |
| Ethernet ports | 6 | 4 |
| RAID type | RAID 1 | RAID 5 |
| Disk | 2 x 300 GB 10K | 3 x 300 GB 15K |
| Standard power supply | 1 x 460 W | 2 x 460 W |

## HP ProLiant DL360 G7 specifications

| Component name | Standard server | High capacity server |
|---|---|---|
| Chassis | 1U | 1U |
| Processor speed | E5620 2.4 GHz 4–core | E5620 2.4 GHz 4–core |

*Table continues…*

| Component name | Standard server | High capacity server |
|---|---|---|
| Number of processors | 1 | 1 |
| System memory | 12 GB | 12 GB |
| Ethernet ports | 2 | 2 |
| RAID type for phase 1 servers | RAID 5 | RAID 5 |
| Disk for phase 1 servers | 3 x 146 GB 10k | 4 x 146 GB 15k |
| RAID type for phase 2 servers | RAID 1 | RAID 5 |
| Disk for phase 2 servers | 2 x 300 GB 10k | 4 x 146 GB 15k |
| Standard power supply | 1 x 460 W | 2 x 460 W |

**Note:**

Phase 1 servers shipped for the first half of the HP ProLiant DL360 G7general availability life cycle. Phase 2 servers shipped for the second half. The disk configuration for the phases are different.

### S8800 1U specifications

| Component name | Standard server | High capacity server |
|---|---|---|
| Chassis | 1U | 1U |
| Processor speed | E5520 Quad-core 2.26 GHz | E5520 Quad-core 2.26 GHz |
| Number of processors | 1 | 1 |
| System memory | 12 GB | 12 GB |
| Ethernet ports | 2 | 2 |
| RAID type | RAID 5 | RAID 5 |
| Disk | 3 x 146 GB 10k rpm SAS hard disk drives | 4 x 146 GB 15k rpm SAS hard disk drives |
| Standard power supply | Single power supply | Dual power supplies |

# Environmental requirements

## 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.

## 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.

# Security requirements

## Security specification

Before implementing a Messaging system, ensure that the customer security staff reviews and approves the Messaging deployment plan. Customers must engage the expertise of their security staff early in the implementation process. The security staff must decide how to incorporate the Messaging system into the routine maintenance for virus protection, patches, and service packs.

## Additional security information

For security information and documentation about all Avaya products, see the Avaya Security Advisories website at http://support.avaya.com/security. The website includes information about the following topics:

- Avaya Product Security Vulnerability Response Policy
- Avaya Security Vulnerability Classification
- Security advisories for Avaya products
- Software patches for security issues
- Reporting a security vulnerability
- Automatic email notifications of security advisories

For information about Messaging security, see *Avaya Aura® Messaging Security Design*.

For additional information about security practices, see the National Security Agency Security Configuration Guides at http://www.nsa.gov/.

# Software download checklist

**Note:**

Downloading software from PLDS is optional if you already have System Platform and Messaging software on the optical media.

| No. | Task | References | Notes | ✔ |
|---|---|---|---|---|
| 1 | Register for PLDS. | See Registering for PLDS on page 32. | — | |
| 2 | Download System Platform and Messaging software from PLDS. | See Downloading software from PLDS on page 32. | — | |

*Table continues…*

| No. | Task | References | Notes | ✔ |
|---|---|---|---|---|
| 3 | Verify that the downloaded ISO images match the images on the PLDS website. | See Verifying the ISO image on a Linux-based computer on page 33 and Verifying the ISO image on a Windows-based computer on page 33. | — | |
| 4 | Write the ISO images to separate DVDs. | See Writing the ISO image to DVD or CD on page 34. | — | |

# Messaging templates overview

Avaya offers product-specific templates to install different products on System Platform. A template defines the set of applications to be installed on System Platform. Messaging offers the following templates:

- Msg_Standard. The Messaging template for the *standard* server.
- Msg_4x146GB_HDD. The Messaging template for the *high-capacity storage* server.

You can install Messaging from one of the following locations.

- **Avaya Downloads (PLDS)**: The template files located on the Avaya PLDS website contain all the templates to which your company is entitled. Each line in the list of templates begins with the sold-to number. For more information about the sold-to number, point the mouse to the selected template.
- **HTTP**: You can copy the template files to an http server and install the files on several System Platform servers.
- **SP Server**: Messaging does not support this option.
- **SP CD/DVD**: The template files are located on a CD-ROM or DVD either supplied with the system or created onsite.
- **SP USB Disk**: The template files are located in a USB flash drive connected to the server. The format of the USB flash drive must be *ext3*.

You must decide the location that works best in a specific scenario. For more information, contact an Avaya-certified business partner or an Avaya technician.

# Software requirements

## Required software for Messaging

For more information about the required software, see *Avaya Aura® Messaging Release Notes* on the Avaya Support website at https://support.avaya.com/Products/P0792 before you install Messaging.

**Table 1: Avaya software**

| Software | Supported versions | References |
|---|---|---|
| System Platform | 6.3.4 | For more information about<br>• Obtaining System Platform software, see Obtaining System Platform and Messaging software on page 31.<br>• Downloading System Platform software from PLDS, see Software download checklist on page 27. |
| Messaging | 6.3.3 | For more information about<br>• Messaging template, see templates overview on page 28.<br>• Obtaining Messaging software, see Obtaining System Platform and Messaging software on page 31.<br>• Downloading Messaging software from PLDS, see Software download checklist on page 27. |
| System Platform patch | As described in *Avaya Aura® Messaging Release Notes*. | To download the latest patches and get the necessary information, see *Avaya Aura® Messaging Release Notes* on the Avaya Support website at https://support.avaya.com/Products/P0792. |
| Communication Manager patch | As described in *Avaya Aura® Messaging Release Notes*. | To download the latest patches and get the necessary information, see *Avaya Aura® Messaging Release Notes* on the Avaya Support website at https://support.avaya.com/Products/P0792. |
| Messaging patch | As described in *Avaya Aura® Messaging Release Notes*. | To download the latest patches and get the necessary information, see *Avaya Aura® Messaging Release Notes* on the Avaya Support website at https://support.avaya.com/Products/P0792. |

**Table 2: Web browser**

| Software | Supported versions | References |
|---|---|---|
| System Platform | • Microsoft Internet Explorer 8 and 9<br>• Mozilla Firefox 10 and later | — |
| Messaging System Management Interface | • Microsoft Internet Explorer 8, 9, and 10<br>• Mozilla Firefox 27 | — |
| Messaging User Preference | • Microsoft Internet Explorer 8, 9, 10, and 11<br>• Mozilla Firefox 27<br>• Safari 6<br>• Google Chrome 23 | — |
| Messaging Web Access | • Microsoft Internet Explorer 9, 10, and 11<br>• Mozilla Firefox 30<br>• Safari 6<br>• Google Chrome 36 | |

**Table 3: Language packs**

| Software | Supported version | References |
|---|---|---|
| Language packs | As described in *Avaya Aura®* *Messaging Release Notes*. | To download the latest language packs and get the necessary information, see *Avaya Aura®* *Messaging Release Notes* on the Avaya Support website at https://support.avaya.com/Products/P0792. |

**Table 4: System requirements for Caller application**

| Software | Supported version | References |
|---|---|---|
| Operating systems | • Microsoft Windows 7 Professional Edition 32–bit<br>• Microsoft Windows 7 Professional Edition 64–bit<br>• Microsoft Windows 8 Pro 32–bit<br>• Microsoft Windows 8 Pro 64–bit | — |

*Table continues…*

| Software | Supported version | References |
|---|---|---|
| Software | • Microsoft Management Console (MMC 3.0)<br>• .NET 3.5 | — |

**Table 5: Third-party software**

In addition to the Avaya storage server that is shipped with Messaging, you can configure your system to use the following third-party servers to store your messages.

| Software | Supported versions | References |
|---|---|---|
| Microsoft Exchange Server | • 2007<br>• 2010<br>• 2013 | See the Microsoft Exchange Server product page of the official Microsoft website. |

## Obtaining the System Platform and Messaging software

You can obtain the System Platform and Messaging software from one of the following sources:

- Avaya-provided optical media (CD/DVDs). When you purchase Messaging, you get one System Platform software DVD and one Messaging Template DVD.
- PLDS website. The content on the DVD and PLDS might change over time. Download the latest version from PLDS. Before installing the software, see Software download checklist on page 27.

## Supported versions of third-party software

Avaya supports use of the documented software versions with the current release of this product. These software versions are the minimum versions that Avaya requires.

This release does not support operating systems, databases, Web servers, switches, or other software platforms that are not documented here, unless stated otherwise in a Product Support Notice.

Avaya will support subsequent updates and service packs that provide corrections for a bug, defect, or problem for the documented software versions. The support depends on the following:

- The manufacturer must guarantee that the updates and service packs are backwards compatible with the supported.
- The updates and service packs do not include changes to the core functionality or new features.

**Note:**

Before you apply the updates and service packs to a production environment, you must test all updates and service packs that follow the supported versions in a development environment.

# 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 prmadmin@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 by using one of the following:
   - Select an application type from the list and the version number.
   - By download name
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: Initial setup and connectivity

## Connectivity

Messaging is a SIP-based messaging system. However, with a SIP gateway, Messaging supports a wide variety of analog and digital telephony servers and telephones.

In large organizations with specialized administration roles, the switch and messaging administrators might be different individuals. If this is true for your organization, you might need to coordinate integration activities because some telephony parameters must be identical on the telephony and application servers.

**Note:**

You must disable multicast while configuring data switch ports.

- Avaya provides configuration notes with switch-specific configuration information. To download these configuration notes, go to the Avaya Support website at http://www.avaya.com/support.
- For the System Platform ports, see *Administering Avaya Aura® System Platform* on the Avaya Support website at http://support.avaya.com.
- For complete port matrix information, see Avaya Aura® Messaging Port Matrix available on the Avaya Support website at http://support.avaya.com.

## Software installation checklist

| No. | Tasks | References | Notes | ✔ |
|---|---|---|---|---|
| 1 | Install System Platform. | See System Platform Installation Checklist on page 36. | — | |
| 2 | Use System Platform Web Console to install System Platform patches. | See Patch installation overview on page 79. | — | |
| 3 | Configure SNMP on the Services virtual machine. | See Configuring SNMP version support on the Services VM on page 60. | — | |

*Table continues…*

| No. | Tasks | References | Notes | ✔ |
|---|---|---|---|---|
| 4 | Register the system and configure SAL Gateway. | See Configuring the SAL Gateway on page 64. | — | |
| 5 | Use System Platform Web Console to install Messaging. | See Installing Messaging on page 75. | — | |
| 6 | Use System Platform Web Console to install Communication Manager and Messaging patches. | See Patch installation overview on page 79. | — | |

# Installing System Platform

## System Platform installation checklist

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | If you are installing System Platform from a laptop, perform the following tasks:<br>• 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.<br>• Configure the IP settings of the laptop for direct connection to the server.<br>See Configuring the laptop for direct connection to the server on page 39.<br>• Disable use of proxy servers in the Web browser on the laptop.<br>See Disabling proxy servers in Microsoft Internet Explorer on page 40 or Disabling proxy servers in Mozilla Firefox on page 40 . | | |
| 2 | If you are installing System Platform from a laptop, connect your laptop to the services port with an Ethernet crossover cable. | If you do not have a crossover cable, use an IP hub.<br>**Note:**<br>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 | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| | | documentation for your laptop computer to determine whether this option is available. | |
| 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.<br>See Starting the installation from your laptop on page 41 or Starting the installation from the server console on page 42 depending on your selection of installation method. | | |
| 6 | If using the server console to install System Platform, enter the **vspmediacheck** command and press **Enter**.<br>The **vspmediacheck** command verifies that the image on the System Platform DVD is not corrupt.<br>See Starting the installation from the server console on page 42. | | |
| 7 | If using your laptop to install System Platform, establish a Telnet connection to the server.<br>See Starting the installation from your laptop on page 41. | | |
| 8 | Select the required keyboard type.<br>See Selecting the type of keyboard on page 42. | | |
| 9 | Verify the System Platform server hardware.<br>See Verifying the System Platform server hardware on page 43. | | |
| 10 | Verify that the image on the System Platform DVD is not corrupt.<br>See Verifying the System Platform image on the DVD on page 44. | | |
| 11 | Configure the network settings for the System Domain (Domain-0).<br>See Configuring network settings for System Domain on page 44. | | |
| 12 | Configure the network settings for the Console Domain. | | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| | See Configuring network settings for Console Domain on page 47. | | |
| 13 | Install the Services Virtual Machine (services_vm).<br>See Installing the Services virtual machine on page 49. | | |
| 14 | Configure the time zone for the System Platform server.<br>See Configuring the time zone for the System Platform server on page 51. | | |
| 15 | Configure the date and time and specify an NTP server if using one.<br>See Configuring the date and time for the System Platform server on page 51 | | |
| 16 | Configure the System Platform passwords.<br>See Configuring System Platform passwords on page 51. | | |
| 17 | Verify that System Platform installed correctly.<br>See Verifying installation of on page 54. | | |

## 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 39.

## Server requirements

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

**Note:**

Because each Avaya Aura® solution template has different requirements for server resources, configuration, capacity, and performance, see customer documentation specific to the Avaya Aura® 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.)

# 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 42.

## 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 42.

# 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 44.

- 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 44.

### Next steps

- Verify that the System Platform image copied correctly to the DVD. See Verifying the System Platform image on the DVD on page 44.

  OR

- Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 44

## 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 42

### About this task

After Selecting the type of keyboard on page 42, 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 44. 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 44

## 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 44.

## Configuring network settings for System Domain

### Procedure

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

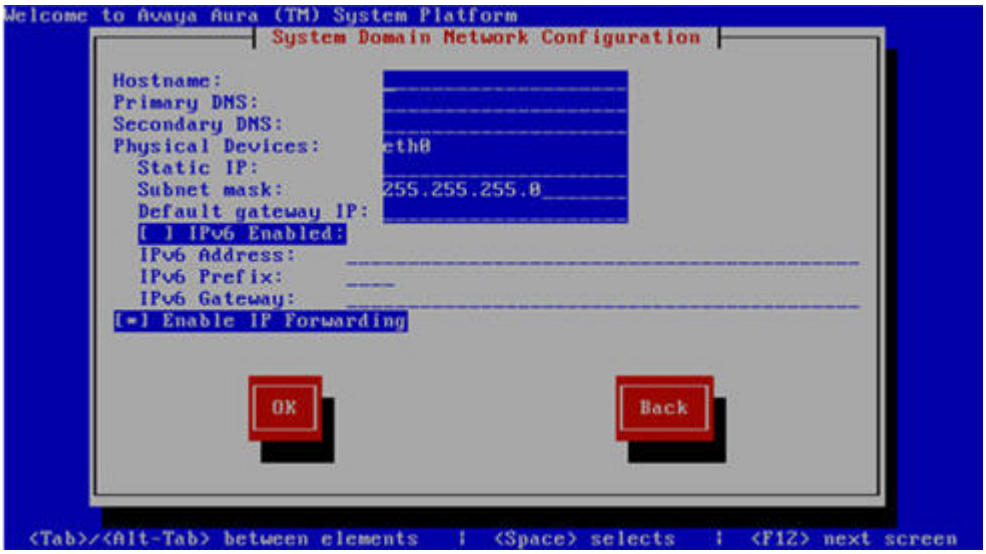
   - **Hostname**

     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 46.




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.

   **Note:**

   Messaging does not support IPv6. Ensure that IPv6 is disabled.
5. If you have enabled IPv6, fill in the following fields:
   - **IPv6 Address**
   - **IPv6 Prefix**
   - **IPv6 Gateway**
6. 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).

7. Use the `Tab` key to highlight **OK** and press **Enter** to accept the configuration.
8. 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 47.

## System Domain Network Configuration field descriptions

| Name | Description |
|---|---|
| **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** | The primary Domain Name System (DNS) server address. |
| **Secondary DNS** | (Optional) The secondary DNS server address. |
| **Physical Devices** | This field displays the physical Ethernet interface (NIC) that connects to the customer network. You must configure this interface for IP.<br>The specific Ethernet interface number depends on the server model being used. |
| **Static IP** | The static IP address for the Ethernet interface that connects to the customer network. |
| **Subnet Mask** | The subnet mask for the Ethernet interface that connects to the customer network. |
| **Default gateway IP** | The default gateway IP address.<br>This default gateway IP address will be used for all the virtual machines if you do not specify gateway IP addresses for them. |
| **IPv6 Enabled** | The indicator to show whether the IP addresses required by System Platform must be IPv6-compliant. |

*Table continues…*

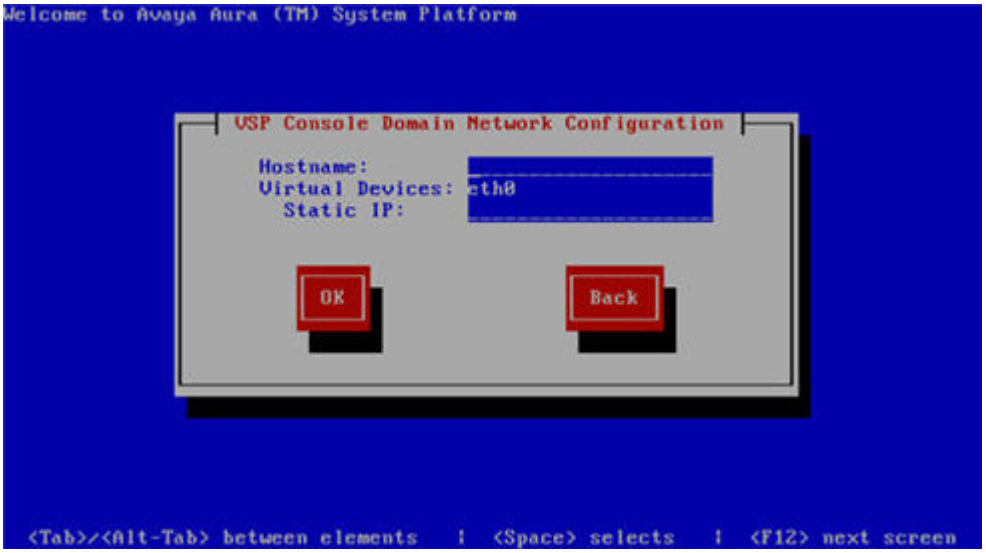
| Name | Description |
|---|---|
| | Messaging does not support IPv6. Make sure that it is disabled. |
| **IPv6 Address** | The IPv6-compliant IP address of System Domain.<br>Messaging does not support IPv6. |
| **IPv6 Prefix** | The IPv6 prefix for **IPv6 Address**.<br>Messaging does not support IPv6. |
| **IPv6 Gateway** | The IP address of the default gateway for IPv6 traffic.<br>Messaging does not support IPv6. |
| **Enable IP Forwarding** | The indicator to show whether IP forwarding is enabled.<br>An asterisk on the left of the field denotes that IP forwarding is enabled.<br>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. |

## 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 49.

## 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, `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** | The IP address for the Console Domain.<br>**Note:**<br>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). |
| 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® 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® 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.

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

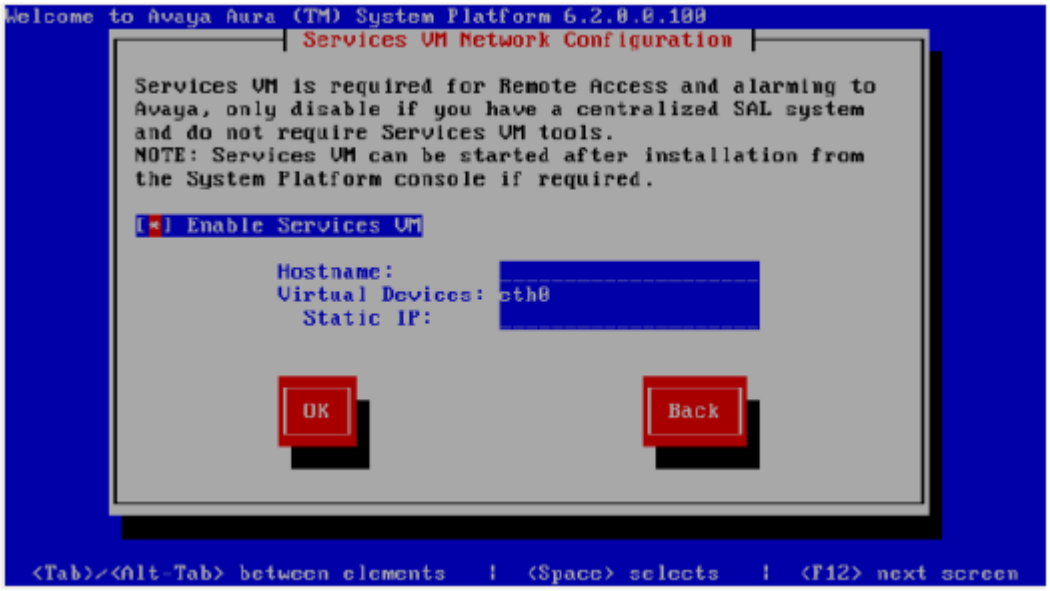
Use this procedure to install the Services VM in an enabled or disabled state, when the Services VM Network Configuration window displays during System Platform installation .

### 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 50.

   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.

## Services VM Network Configuration field descriptions

| Name | Description |
|---|---|
| **Enable Services VM** | Enables or disables remote access. Also supports local or centralized alarm reporting.<br>Default value: **Enabled**<br>Leave the **Enable services VM** 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. |
| **Hostname** | The name you assign to the Services virtual machine. |
| **Static IP address** | The IP address you assign to the Services virtual machine. The address must be on the same subnet |

*Table continues…*

| Name | Description |
|---|---|
| | assigned to the Domain 0 (dom0) and Console Domain (cdom) virtual machines. |
| **Virtual devices** | The virtual device (port) assigned to the Services virtual machine. Default value (eth0) automatically assigned. No user input necessary. |

## 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<br>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.<br>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 57.

## Next steps

Verify System Platform installation. See Verifying installation of on page 54.

### 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 |
|---|---|
| **root Password** | The password for the root login. |
| **admin Password** | The password for the admin login. |
| **cust Password** | The password for the cust login.<br>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. |
| **ldap Password** | The password for the ldap login.<br>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 56.

### 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.

# 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.

## 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 PlatformWeb 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 56.

### 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.

## 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.

# Configuring SNMP on the Services virtual machine

## SNMP configuration overview

Services-VM can support either SNMP v2c or v3 for SAL Gateway. In case of a fresh installation of Services-VM, Services-VM supports SNMP v3 by default. You can change the configuration to support the required SNMP version.

After you upgrade Services-VM from 1.0 to 2.0, Services-VM supports the SNMP version that was configured on Services-VM 1.0.

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 modify with actual values after a consultation with your network administrator.

| File | Parameter | Default value |
|---|---|---|
| `snmpv2c.conf` | Community string | avaya123 |
| `snmpv3.conf` | 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
```

# 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 Platformincludes 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 74. 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 74.

### 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.

   Avayaassigns 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.

## 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.

## 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 65.
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.

## Gateway Configuration field descriptions

| Name | Description |
|---|---|
| **Hostname** | A host name for the SAL Gateway.<br>**Warning:**<br>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. |
| **IP Address** | The IP address of the SAL Gateway.<br>This IP address must be different from the unique IP addresses assigned to either the Cdom or Dom0 virtual machines. |
| **Solution Element ID** | The Solution Element ID that uniquely identifies the SAL Gateway. Format is `(000)123-4567`.<br>If you have not obtained Solution Element IDs for the system, start the registration process.<br>The system uses the SAL Gateway Solution Element ID to authenticate the SAL Gateway and its devices with the Secure Access Concentrator Remote Server. |
| **Alarm ID** | The Product ID (also called Alarm ID) for the SAL Gateway. This ID should start with a 5 and include ten digits.<br>The system uses the value in the this field to uniquely identify the source of Gateway alarms in the Secure Access Concentrator Core Server. |
| **Alarm Enabled** | Enables the alarming component of the SAL Gateway. This check box must be selected for the SAL Gateway to send alarms. |
| **Inventory Collection** | Enables inventory collection for the SAL Gateway.<br>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 *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com |
| **Inventory collection schedule** | Interval in hours at which the SAL Gateway collects inventory data. |

# 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.

# 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. |
| **Proxy Type** | The type of proxy server that is used. Options are:<br>• **SOCKS 5**<br>• **HTTP** |
| **Host** | The IP address or the host name of the proxy server. SAL Gateway takes both IPv4 and IPv6 addresses as input. |

*Table continues…*

| Name | Description |
|---|---|
| **Port** | The port number of the Proxy server. |
| **Login** | Login if authentication is required for the HTTP proxy server.<br>**Important:**<br>SAL Gateway in System Platform does not support authenticating proxy servers. |
| **Password** | Password for login if authentication is required for the HTTP proxy server.<br>**Important:**<br>SAL Gateway in System Platform does not support authenticating proxy servers. |
| **Test URL** | 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 |
|---|---|
| **Test** | Initiates a test of the SAL Gateway connectivity through the proxy server to the URL specified in the **Test URL** field. You can initiate a test before or after applying the configuration changes. |
| **Edit** | Makes the fields on the Proxy Server page available for editing. |
| **Apply** | Saves the configuration changes. |

## 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.

### Core Server field descriptions

| Name | Description |
|---|---|
| **Passphrase** | Default passphrase is `Enterprise-production`. 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 SAL Gateway and the Secure Access Concentrator Core Server. |
| **Primary Core Server** | IP Address or the host name of the primary Secure Access Concentrator Core Server.<br>The default value is `secure.alarming.avaya.com`. |
| **Port** | Port number of the primary Secure Access Concentrator Core Server.<br>The default value is `443`. |
| **Secondary Core Server** | This value must match the value in the **Primary Core Server** field. |
| **Port** | This value must match the value in the **Port** field for the primary server. |

## 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.

### Remote Server field descriptions

| Name | Description |
|---|---|
| **Primary Remote Server** | The IP address or host name of the primary Secure Access Concentrator Remote Server.<br>The default value is `sl1.sal.avaya.com`. |
| **Port** | The port number of the primary Secure Access Concentrator Remote Server.<br>The default value is `443`. |
| **Secondary Remote Server** | This value must match the value in the **Primary Remote Server** field. |
| **Port** | This value must match the value in the **Port** field for the primary server. |

## 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.

### Network Management Systems field descriptions

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

## 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 Gatew:ay 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.

| 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 | |
| | | | | | |
| | | | | | |
| | | | | | |

*Table continues…*

| Managed device (virtual machine) | IP Address | SE ID | Product ID | Model | Notes |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

# 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.

## Managed Element field descriptions

| Name | Description |
|---|---|
| **Host Name** | Host name for the managed device. This must match the host name on the Network Configuration page of the System Platform Web Console (**Server Management** > **Network Configuration** in the navigation pane). |
| **IP Address** | IP address of the managed device. |
| **NIU** | Not applicable for applications that are installed on System Platform. Leave this field clear (not selected). |
| **Model** | The model that is applicable for the managed device. |
| **Solution Element ID** | The Solution Element ID (SE ID) of the device. |

*Table continues…*

| Name | Description |
|---|---|
| | The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely. |
| **Product ID** | The Product ID (also called Alarm ID).<br>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. |
| **Provide Remote Access to this device** | Check box to allow remote connectivity to the managed device. |
| **Transport alarms from this device** | (Optional) Check box to enable alarms from this device to be sent to the Secure Access Concentrator Core Server. |
| **Collect Inventory for this device** | Check box to enable inventory collection for the managed device.<br>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 *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com. |
| **Inventory collection schedule** | Interval in hours at which the SAL Gateway collects inventory information about the managed device. |
| **Monitor health for this device** | 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. |
| **Generate Health Status missed alarm every** | Interval in minutes at which SAL Gateway generates an alarm if it does not receive a heartbeat from the managed device.<br>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. |
| **Suspend health monitoring for this device** | Check box to suspend health monitoring for the managed device. |
| **Suspend for** | Number of minutes to suspend health monitoring for the managed device. SAL Gateway resumes |

*Table continues…*

| Name | Description |
|---|---|
| | monitoring the device after the configured time elapses. |

# 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**.

# Messaging installation

## Installing Messaging

### Before you begin

- Update System Platform with the latest patches and service packs verified for use with Messaging. To download the latest patches, see *Avaya Aura® Messaging Release Notes* on the Avaya Support website at https://support.avaya.com/Products/P0792. For more information on downloading and installing patches and Service Packs, see Installing patches on page 80.
- Print the Configuration information for Messaging installation on page 20, and enter all the required data in the planning form.
- Enable pop-up windows on the web browser. For more information, see the online help of the browser.

### Procedure

1. Log on to System Platform Web Console.
2. Click **Virtual Machine Management** > **Solution Template**.

   The system displays the Search Local and Remote Template page. Use this page to select a location from where you want to download the template.
3. From the **Install Template From** drop-down list, select the medium to search for the Messaging image files. The following table lists the available options:

| Location | Action |
|---|---|
| Avaya Downloads (PLDS) | Provide **SSO Login** and **SSO Password**. |
| HTTP | Specify the **Template Location**.<br>If the template files are located in a different server, you might need to configure a proxy depending on your network. Click **Configure Proxy** to specify a proxy server if required. |
| SP Server | Specify the **Template Location**. |
| SP CD/DVD | Click **Search**. |
| SP USB Disk | Click **Search**. |

For more information, see Search Local and Remote Template field descriptions on page 76.

4. To display a list of template descriptor files, click **Search**. Each available template has exactly one template descriptor file.

   The system displays the Select Template page.

5. From the **Select Template** list, select the template that you want to install from the following:
   - Msg_Standard. The Messaging template for the *standard* server.
   - Msg_4x146GB_HDD. The Messaging template for the *high capacity storage* server.
6. Click **Select**.
7. On the Template Details page, click **Install**.

   The Template Network Configuration page that shows the network configuration that you entered while installing System Platform.
8. Verify the network configuration, and click **Save** to continue.
9. On the Template Details page, enter the following details for the Messaging virtual machine:
   a. MSG IPv4 Address. The IPv4 address of the Messaging virtual machine.
   b. MSG IPv6 Address. The IPv6 address of the Messaging virtual machine. Leave this field blank as Messaging does not support IPv6.
   c. MSG Hostname. The host name must be the Fully Qualified Domain Name (FQDN) of the Messaging virtual machine.

   For more information, see Network settings field descriptions on page 77.
10. Click **Install**.

    The Template Installation page displays the progress of the template installation process. The template installation process takes approximately 15 minutes for the *Msg_Standard* template.

### Next steps

Verify the Messaging installation.

## Search Local and Remote Template field descriptions

| Names | Descriptions |
|---|---|
| **Install Template From** | The location where you search for a template and then install the template on System Platform. The available locations are:<br>• **Avaya Downloads (PLDS)**<br>To download the template files located on the Avaya Product Licensing and Delivery System (PLDS) website, you must enter an Avaya SSO |

*Table continues…*

| Names | Descriptions |
|---|---|
| | login and password. The list on this site contains all the templates that your company is entitled to. Each line in the list begins with the sold-to number. Use the sold-to number to select the appropriate template for your site. For more information about a sold-to number, hold the mouse pointer over the number.<br>• **HTTP**<br>To download the template files located on an HTTP server, you must enter the template location information.<br>• **SP Server**<br>To download the template files located in the `/vsp-template` directory in Console Domain of the System Platform server, you must specify the template location for the server.<br>• **SP CD/DVD**<br>To download the template files located on a CD-ROM or DVD in the CD/DVD drive on the System Platform server.<br>• **SP USB Disk**<br>To download the template files located on a USB flash drive connected to the server, format the USB flash drive as *ext3*. |
| **SSO Login** | The login ID to log on to Single Sign On. The system activates this field only when you select the **Avaya Downloads (PLDS)** option to search for a template. |
| **SSO Password** | The password for Single Sign On. The system activates this field only when you select the **Avaya Downloads (PLDS)** option to search for a template. |
| **Template Location** | The URL of the server where the template files are located. The system activates this field only when you select the **HTTP** or **SP Server** option to search for a template. |

# Network settings field descriptions

## Field descriptions

| Name | Description |
|---|---|
| **Msg IPv4 Address** | The IPv4 address of the Messaging virtual machine. |
| **MSG Hostname** | The FQDN of the Messaging virtual machine. |

# Verifying the Messaging installation

## About this task

After completing the installation, verify that the Messaging virtual machine is running.

## Procedure

1. Log on to System Platform Web Console.
2. Click **Virtual Machine Management** > **Manage**.
3. On the Virtual Machine List page, verify that the current status of the Messaging virtual machine *msg* is **Running**.

## Next steps

Install the patches.

# Logging in to Messaging

## About this task

You can gain access to Messaging System Management Interface (SMI) remotely through the corporate LAN connection or from a laptop connected to the server through the services port.

## Procedure

1. Open a compatible Web browser on your computer.
2. Depending on the server configuration, choose one of the following options:

| Options | Description |
|---|---|
| Access by System Platform Web Console | • Log on to the System Platform Web Console.<br>• Click **Virtual Machine Management** > **Manage**.<br>The system displays the Virtual Machine List page.<br>• Click the **Manage Virtual Machine** wrench icon to select the *msg* virtual machine. |
| LAN access by IP address | To log on to the corporate LAN, type the unique IP address of the Messaging server in the standard dotted-decimal notation. For example, `http://192.152.254.201`. |
| LAN access by host name | To log on using the corporate LAN that includes a DNS server administered with the hostname, type the hostname. For example, `http://avayamsg.example.com`. |
| Laptop access by IP address | To log on using the services port from a directly-connected laptop, type the unique IP address of the Messaging server in standard dotted-decimal notation. For example, `http://192.152.254.201`. |

If your browser does not have a valid security certificate, the system displays a warning screen and instructions to load the security certificate. If your connection is secure, accept the server security certificate to gain access to the logon screen. If you plan to use this computer and browser to access this or other Avaya servers again, install the root certificate

on your computer. The root certificate establishes Avaya Inc. as a trusted Certificate Authority (CA).

For more information, see Installing a root certificate on page 86.

3. Click **Continue**.

   The system displays the Logon screen.

4. In the **Logon ID** field, type `craft`.

   **Note:**

   When you gain access to Messaging System Management Interface for the first time, use the *craft* login. You must use the privileged administrator login after you add the privileged administrator login.

5. Click **Log On**.
6. In the **Password** field, type `craft01`.
7. Click **Log On**.

   After successful authentication, the system displays the Messages page that displays the last login information.

8. Click **Continue**.

   The system displays the Messaging System Management Interface home page.

# Patch management

## Patch installation overview

A Service Pack provides product updates and bug fixes. When a Service Pack is available on the Avaya Support website, the supporting information clearly states the issues addressed in the Service Pack. Even if the system does not have problems, implement the Service Packs to keep the systems up-to-date and minimize the likelihood of future issues.

A patch provides critical security, performance, and stability fixes or updates. A Service Pack is a bundle of updates, fixes, enhancements, and previously released patches. In this document, the word *patches* refers to both patches and Service Packs.

You can install, download, and manage the patches from System Platform Web Console.

You must install the following patches in addition to the currently installed software:

- Communication Manager: Messaging uses the Communication Manager platform that requires software updates.
- Messaging

You must install the following patches when available:

- Security

- Kernel

**Important:**

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

To download the latest patches and to obtain the necessary information, see *Avaya Aura® Messaging Release Notes* on the Avaya Support website at http://support.avaya.com/Products/P0792.

**Important:**

Before you apply a patch, back up the system. When you install the latest patch, the installation program automatically uninstalls the previous patch. So, if you remove a patch, the system does not reinstall the previous patch or revert the system to the previous state, that is, the state before the patch was installed. To revert the system to the previous state, you must reinstall the previous patch.

For more information, see *Administering Avaya Aura® Messaging*.

**Caution:**

The patch installation process affects the availability of the Messaging service.

## Installing patches

### Before you begin

Ensure that the Messaging system is running.

### Procedure

1. Log on to System Platform Web Console.
2. Click **Server Management** > **Patch Management** > **Download/Upload**.

   The system displays the Search Local and Remote Patch page.
3. From the **Choose Media** drop-down list, select the medium to search for a patch. The following table lists the available options.

| Option | Action |
|---|---|
| Avaya Downloads (PLDS) | Provide **SSO Login** and **SSO Password**, and then click **Search**.<br>**Note:**<br>This option is not available for Avaya Services. |
| HTTP | Specify **Patch URL**, and click **Search**.<br>If the patches are located on a different server, you might have to configure a proxy server depending on your network. Click **Configure Proxy** to specify a proxy server if required. |
| SP Server | Messaging does not support this option. |
| SP CD/DVD | Click **Search**. |

*Table continues…*

| Option | Action |
|---|---|
| SP USB Disk | Click **Search**. |
| Local File System | Click **Add** to locate the patch file on your computer, and then click **Upload**. |

For more information, see Search Local and Remote Patch field descriptions on page 81.

The system displays the Select Patches page.

4. From the **Select Patches** list, select the patch that you want to download.
5. Click **Select**.
6. On the Patch Detail page, click **Install**.

   For more information, see Patch Detail field descriptions on page 82.

   The Patch Detail page displays the progress of the patch installation.

### Next steps

Verify the patch installation.

## Search Local and Remote Patch field descriptions

| Name | Description |
|---|---|
| **Supported Patch File Extensions** | The patch that you select for installing. Ensure that the patch matches the extensions in the following list. For example, *.tar.gz,*.tar.bz,*.gz,*.bz,*.zip,*.tar,*.jar,*.rpm,*.exe,*.bin,*.patch,*.sh,*.bat,*.cmd,*.py,*.txt. |
| **Choose Media** | The media options from where you can search for a patch. The available options are:<br>• **Avaya Downloads (PLDS)**<br>To download the patch files located on Avaya PLDS website, you must enter an Avaya SSO login and password to access this site. The list on this site contains all the templates that your company is entitled to. Each line in the list begins with the sold-to number. Use the sold-to number to select the appropriate template for your site. For more information about a sold-to number, hold the mouse pointer over the number.<br>• **HTTP**<br>To download the patch files located on an HTTP server, you must enter the patch location information.<br>• **SP Server**<br>Messaging does not support this option.<br>• **SP CD/DVD**<br>To download the patch files located on a CD-ROM or DVD in the CD/DVD drive on the System Platform server. |

*Table continues…*

| Name | Description |
|---|---|
| | • **SP USB Disk**<br>To download the patch files located on a USB flash drive connected to the server.<br>• **Local File System**<br>To download the patch files located in a local file system. |
| **SSO Login** | The login ID to log on to Single Sign On. The system activates this field only when you select the **Avaya Downloads (PLDS)** option to search for a patch. |
| **SSO Password** | The password for Single Sign On. The system activates this field only when you select the **Avaya Downloads (PLDS)** option to search for a patch. |
| **Patch URL** | The URL of the server where the template files are located. The system activates this field only when you select the **HTTP** or **SP Server** option to search for a patch. |

## Patch Detail field descriptions

| Name | Description |
|---|---|
| **ID** | The file name of the patch file. |
| **Version** | The version of the patch file. |
| **Product ID** | The name of the virtual machine. |
| **Description** | The short description of the patch file. |
| **Detail** | The name of the virtual machine to which the patch is applicable.<br>This field is not applicable for Messaging patches. |
| **Dependency** | The dependency that the patch file might have on any other file.<br>This field is not applicable for Messaging patches. |
| **Applicable for** | The software load for which the patch is applicable.<br>This field is not applicable for Messaging patches. |
| **Service effecting when** | The action, if any, that causes the selected patch to restart the Messaging services. |
| **Restart this console when** | The conditions or circumstances when the System Platform Web Console must be restarted.<br>This field is not applicable for Messaging patches. |
| **Disable sanity when** | The circumstance when the condition is set to disable.<br>This field is not applicable for Messaging patches. |

*Table continues…*

| Name | Description |
|---|---|
| **Status** | The status to show whether the patch is available for installation or already installed. |
| **Patch File** | The path where the patch is cached on the Console Domain. |
| **Publication Date** | The date on which the patch file is published. |
| **License Required** | The requirement status of a license for the patch file. |
| **Rollbackable** | The option to cancel the upgrade process of the patch file and return to the previous version. |

## Verifying the patch installation

### Procedure

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

   The system displays the Patch List page.

2. Verify that the system displays the Messaging and Communication Manager patches that you installed under the *msg* heading and the status of the patch is **Active**.

   For more information, see Patch List field descriptions on page 83.

## Patch List field descriptions

The Patch List page displays the patches on the System Platform server for installation or removal. To view the details of the patch file, click the file name.

| Name | Description |
|---|---|
| **System Platform** | Lists the patches available for System Platform. |
| **Solution Template** | Lists the patches available for the respective solution templates. |
| **msg** | Lists the patches available for Messaging. |
| **Patch ID** | Lists the file name of a patch. |
| **Description** | Provides information about a patch. For example, the field describes a patch available for System Platform as SP patch. |
| **Status** | Shows the status of a patch.<br>The possible values of **Status** are **Active** and **Not Installed**. |
| **Service Affecting** | Shows if installing the patch causes the Messaging virtual machine to reboot. |

## Removing patches

### Procedure

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

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

2. On the Patch List page, click a patch that you want to remove.
3. On the Patch Detail page, you can:
   - Click **Remove** to uninstall the patch.
   - Click **Remove Patch File** to clean up the hard disk drive by deleting the installation file of an uninstalled patch.

# Licensing

To manage the licenses of one or more Avaya software products used in your organization, Avaya provides WebLM, a web-based license manager. To track and manage all the licenses, WebLM requires a license file from the PLDS website at https://plds.avaya.com.

When you install System Platform, you also install the WebLM server. The installation process automatically configures the WebLM server to work with Messaging. However, you can change this configuration to a centralized WebLM server.

In larger or more complex environments, customers might have multiple Messaging systems. You can associate each Messaging system with only one license file. You must decide how the license will be distributed before you obtain the license through PLDS.

# Chapter 6: Initial administration

## Logging in to Messaging

### About this task

You can gain access to Messaging System Management Interface (SMI) remotely through the corporate LAN connection or from a laptop connected to the server through the services port.

### Procedure

1. Open a compatible Web browser on your computer.
2. Depending on the server configuration, choose one of the following options:

| Options | Description |
|---|---|
| Access by System Platform Web Console | • Log on to the System Platform Web Console.<br>• Click **Virtual Machine Management** > **Manage**.<br>The system displays the Virtual Machine List page.<br>• Click the **Manage Virtual Machine** wrench icon to select the *msg* virtual machine. |
| LAN access by IP address | To log on to the corporate LAN, type the unique IP address of the Messaging server in the standard dotted-decimal notation. For example, `http://192.152.254.201`. |
| LAN access by host name | To log on using the corporate LAN that includes a DNS server administered with the hostname, type the hostname. For example, `http://avayamsg.example.com`. |
| Laptop access by IP address | To log on using the services port from a directly-connected laptop, type the unique IP address of the Messaging server in standard dotted-decimal notation. For example, `http://192.152.254.201`. |

If your browser does not have a valid security certificate, the system displays a warning screen and instructions to load the security certificate. If your connection is secure, accept the server security certificate to gain access to the logon screen. If you plan to use this computer and browser to access this or other Avaya servers again, install the root certificate on your computer. The root certificate establishes Avaya Inc. as a trusted Certificate Authority (CA).

For more information, see Installing a root certificate on page 86.

3. Click **Continue**.

   The system displays the Logon screen.

4. In the **Logon ID** field, type `craft`.

   **Note:**

   When you gain access to Messaging System Management Interface for the first time, use the *craft* login. You must use the privileged administrator login after you add the privileged administrator login.

5. Click **Log On**.

6. In the **Password** field, type `craft01`.

7. Click **Log On**.

   After successful authentication, the system displays the Messages page that displays the last login information.

8. Click **Continue**.

   The system displays the Messaging System Management Interface home page.

# Initial administration checklist

| No. | Tasks | References | Notes | ✔ |
|---|---|---|---|---|
| 1 | Gather all the required data. | See Configuration information for initial administration of Messaging on page 21. | — | |
| 2 | Install the license file. | See License file for Messaging on page 87. | — | |
| 3 | Add the privileged administrator login. | See Adding a privileged administrator login on page 93. | — | |
| 4 | Download and install the authentication file. | See Authentication file installation on page 90. | — | |
| 5 | Add the software installer login. | See Software installer login on page 95. | — | |

## Installing a root certificate

The Install Root Certificate page allows you to install the security certificate that contains the Avaya digital signature. The security certificate with the Avaya digitial signature prevents unauthorized users from intercepting and viewing passwords and other sensitive information.

The Root Certificate establishes Avaya Inc. as a trusted Certificate Authority (CA). You must install the Root Certificate after you log in.

**Warning:**

You must install a CA certificate as a Root Certificate.

If you do not install the Root Certificate you will get a Security Alert stating that the company is not trusted.

### Procedure

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Install Root Certificate**.
3. On the Install Root Certificate page, click **Install**.
4. In the File Download - Security Warning dialog box, click **Save**.
5. Select a location, and save the *avayaRootCert.cer* file.
6. Navigate to the *avayaRootCert.cer* file location and, double-click it.
7. In the Open File - Security Warning dialog box, click **Open**.
8. From the **General** tab in the **Certificate** dialog box, click **Install Certificate...**.
9. Accept all the default settings in the Certificate Import Wizard, and click **Finish**.

**Note:**

In this guide, the root certificate name, *avayaRootCert.cer*, is an example. The user must define the root certificate name.

# License management

## License file for Messaging

The license file is an Extensible Markup Language (XML) file with information about the product, the major release, and the license features and capacities.

You can use Avaya PLDS to generate and download license files for Messaging. PLDS provides customers, Avaya partners, distributors, and Avaya associates with easy-to-use tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

When you place an order for a PLDS-licensed software product such as Messaging, the system automatically creates license entitlements in PLDS. After the system creates license entitlements, you will receive an email from PLDS with a license activation code (LAC). Using the LAC, you can quickly find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

**Important:**

You must provide the WebLM host ID to activate the license file in PLDS. The WebLM host ID is the MAC address of the server, and you can obtain the ID from the WebLM web interface.

## Accessing WebLM from System Platform Web Console

### Procedure

1. Log on to System Platform Web Console.
2. Click **Server Management** > **License Management**.
3. On the License Management page, click **Launch WebLM License Manager**.

   The system displays WebLM License Manager in a new browser window.
4. Enter the user name and password for WebLM License Manager. For the initial login, the user name is `admin`, and the password is `weblmadmin`. Change the password the first time that you log in to WebLM License Manager.

## Obtaining the WebLM host ID

### About this task

You must provide the WebLM host ID to activate the license file in PLDS. Get the WebLM host ID from the Server Properties page of WebLM server.

### Procedure

1. Log on to WebLM License Manager.
2. In the left navigation pane, click **Server Properties**.
3. Make a note of the MAC address that is displayed in the **Primary Host ID** field.

### Next steps

Activate license entitlements in PLDS.

## Activating license entitlements in PLDS

### Before you begin

Obtain host ID of license host to activate license entitlements on a new License Host.

### About this task

Use the License Activation Code (LAC) to activate one or more license entitlements. You can activate all the licenses, or you can specify the number of licenses to activate from the available quantity. You must install the license file on WebLM to use the licenses.

For more information about PLDS, see *Getting Started with Avaya PLDS* at http://support.avaya.com.

### Procedure

1. On your web browser, type `http://plds.avaya.com` .

2. Enter your login ID.
3. In the **LAC(s)** field of the Quick Activation section, enter the LAC that you received in an email message.

   You can also look for your entitlements in the LAC.

   **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 is the MAC address of the server hosting the WebLM server. You can obtain the Host ID from the Server Properties page of the WebLM server where the license file is installed.
7. Enter the number of licenses to activate.
8. Review the Avaya License Agreement, and click **Accept**.
9. To send an activation notification email message:
   a. In the **E-mail to** field, enter email addresses of any additional activation notification recipients.
   b. In the **Comments** field, enter comments or special instructions.
   c. Click **Finish**.
10. Click **ViewActivation 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 that are generated after the license activation. You can view and download the license files. A single license file is generated for each application. Install each license file on the WebLM server associated with the License Host.

### Next steps

Install a license file in WebLM.

## Installing a license file in WebLM

### Before you begin

Obtain the license file from Avaya PLDS website at https://plds.avaya.com.

### Procedure

1. Log on to WebLM License Manager.
2. In the left navigation pane, click **Install license**.
3. On the Install license page, enter the license file path or click **Browse**, and select the license file.
4. Click **Install**.

### Result

After you install the license file, WebLM License Manager screen displays the installed license on the License Products screen.

# Authentication file management

## Authentication file installation

To grant Avaya service personnel and Avaya partners access to the customer system, you need a new authentication file with Access Security Gateway (ASG) keys and the server certificate for Messaging. Authentication file ensures system security and prevents unauthorized access to your Messaging system.

Authentication files have a plain text XML header with encrypted authentication data and an encrypted server certificate. To change the authentication information, replace the entire file. If the authentication file is missing or corrupted, the system denies all logins to the Avaya server. The Messaging system continues to run, but the system blocks further administration until you install a new authentication file.

**Note:**

If the authentication file is not installed, the system displays an error message that the system cannot display the authentication file information.

## Starting the AFS application

### Before you begin

Authentication File System (AFS) is available only to Avaya service personnel and Avaya partners. If you are a customer and need an authentication file, contact Avaya or your authorized Avaya Partner.

To start the AFS application, you must have a login ID and password. Sign up for a login ID at http://rfa.avaya.com.

### Procedure

1. Type http://rfa.avaya.com in your web browser.
2. Enter your login information and click **Submit**.
3. Click **Start the AFS Application**.

The system displays a security message.

4. Click **I agree**.

   The system starts the AFS application.

### Next steps

Create an authentication file.

## Creating an authentication file for a new system

### About this task

You can download the authentication file from AFS to your computer, or you can have the authentication file sent in an email message.

### Procedure

1. Log in to the AFS application.
2. In the **Product** field, select **SP System Platform/VE VMware**.
3. In the **Release** field, select the release number of the software, and then click **Next**.
4. Select **New System**, and then click **Next**.
5. In the **Communication Manager 6.x** field, enter the fully qualified domain name (FQDN) of the Messaging virtual machine.
6. In the **Utility Server 6.x** field, enter the FQDN of System Platform Console Domain.
7. If you want to download the authentication file directly from AFS to your computer:
   a. Click **Download file to my PC**.
   b. Click **Save** in the File Download dialog box.
   c. Select the location where you want to save the authentication file, and then click **Save**.
   d. Click **Close** in the Download complete dialog box to complete the download.

   After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID)
8. If you want to send the authentication file in an email message:
   a. Enter the e-mail address in the **Email Address** field.
   b. Click **Download file via email**.

   AFS sends the email message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.
9. To view the header information in the authentication file, go to the location where the file is saved and use WordPad to open the file.

   The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

### Next steps

Obtain the AFID from System Platform Web Console.

## Obtaining the AFID from System Platform Web Console

### Procedure

1. Log on to System Platform Web Console.
2. In the navigation pane, click **User Administration** > **Authentication File**.

   The system displays the AFID in the AFID field. The default authentication that is installed with System Platform is an AFID of 7100000000. Replace the default file with a unique file.

### Next steps

Install the authentication file.

## Installing the authentication file

### Procedure

1. Log on to System Platform Web Console.
2. Click **User Administration** > **Authentication File**.
3. Click **Upload**.
4. Click **Install**.

   The system uploads the selected authentication file and validates the file.

### Next steps

Verify the authentication file.

## Verifying the authentication file

### Procedure

1. Log on to Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Authentication File**.

   The system displays the Authentication File page that includes the following details:

   - **AFID**: The authentication file ID.
   - **Product**: The product name of the authentication file.
   - **Release**: The product major release of the authentication file.
   - **Common Name**: The host name of the Messaging server.
   - **Authentication file generation date**: The date when the system generated the authentication file.
   - **Authentication file generation time**: The time when the system generated the authentication file.

- **Authentication file request type**: The request type of the authentication file. For example, New System/Existing System, Same Release/Existing System, Upgrade.
- **ASG key type**: The type of Avaya Security Gateway, new or existing.
- **Password type**: The type of password, new or existing.
- **AFS Request ID**: The request ID of AFS.

# Account management

## Adding a privileged administrator login

### About this task

You must add a privileged administrator login that is a member of the SUSERS group. This login provides the highest level of access with the maximum permissions. A user with the privileged administrator login can gain access to all the System management Interface pages and Command Line Interface after you install the authentication file.

### Procedure

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Administrator Accounts**.
3. In the **Select Action** area, select **Add Login**.
4. Select **Business Partner Login (dadmin)**.

   This login provides the highest level of access with the maximum permissions to a user. A user can gain access to all the SMI pages and CLI. You can add this login only once.
5. Click **Submit**.

   The system displays the Administrator Accounts -- Add Login: Privileged Administrator Web page.
6. Enter information in the following fields:
   - **Date after which account is disabled-blank to ignore (YYYY-MM-DD)**: Clear this field
   - **Enter password or key**
   - **Re-enter password or key**
7. Click **Submit**.
8. Click **Continue** to go back to the Administrator Accounts Web page.

## Administrator Accounts field descriptions

| Field | Description |
|---|---|
| Select Action | |
| **Add Login** | Select this option and select the type of login to add.<br>The options are:<br>• **Privileged Administrator**: Provides the highest level of access with the maximum permissions. A user can gain access to all the SMI pages and CLI.<br>• **Unprivileged Administrator**: Provides restricted access. A user can gain access to the SMI pages that are for querying the Messaging status and backing up data and CLI.<br>• **Web Access Only**: Provides access only to the SMI pages. A user can administer the SMI pages that the user can gain access to in the **Web Access Mask** settings of the profile of the user.<br>• **CDR Access Only**: Not applicable.<br>• **Business Partner Login (dadmin)**: Provides the highest level of access with the maximum permissions to a user and is similar to **Privileged Administrator**. A user can gain access to all the SMI pages and CLI. You can add this login only once.<br>• **Business Partner Craft Login**: Provides the highest level of access with the maximum permissions and is similar to **Business Partner Login (dadmin)**. A user can gain access to all the SMI pages and CLI. With this login, the user can suppress alarms from the server when logging in to SMI.<br>• **Custom Login**: Provides customized access. You can select the level of access to the user. |
| **Change Login** | Select this option and select a login from the drop-down list. |
| **Remove Login** | Select this option and select a login from the drop-down list. |
| **Lock/Unlock Login** | Select this option and select a login from the drop-down list. |
| **Add Group** | Select this option to add a group. |
| **Remove Group** | Select this option and select a group from the drop-down list. |

## Software installer login

A privileged administrator is always assigned to profile number 18, which does not allow software installation or removal. Create a new custom profile for a privileged administrator so that the privileged administrator can obtain specific Software Management rights for software installation.

For more information on Web access profiles, see Web Access Mask on page 95.

## Web Access Mask

The Messaging Web Access Mask page specifies:

- The Messaging server webpages a user may gain access to.
- The type of webpage access available to a user. When a user with a particular profile accesses the web interface, the menu displays only the webpages for that profile.
- The read-only access or read/write access for every webpage available to a user.

The system uses numbers 0 to 69 to identify the Web profile that corresponds to a Linux group.

- Profiles 0 to 3, 18, and 19 are built into Messaging, and you cannot edit these profile numbers. In Messaging, the web profile numbers 0 to 19 correspond to the fixed profiles.
- Profiles numbers 0 to 3 and 18 are members of the Linux group: susers. Logins that are members of the susers Linux group and profile 18, which is the profile group prof18, can gain access to all the possible webpages except those that allow software installation or removal.
- Profile number 19 is a member of the Linux group: users. Logins that are members of the users Linux group and profile 19, which is the profile group prof19, can only gain access to a subset of the webpages.
- Profile numbers 4 to 17 are unused. The system reserves these numbers for future use.
- Profile numbers 20 to 69 are for customized profiles. The customer can select a profile of choice and assign this number.

## Adding a Web Access Mask

### Procedure

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Web Access Mask**.
3. On the Web Access Mask page, click **Add**.
4. On the Add Access Mask page, enter a new mask number in the **Enter new Access Mask Number** field.
5. Select **Create by copying values from Access Mask number** and enter *18* to copy super-user permissions.
6. Click **Submit**.

### Next steps

Edit profile permissions.

## Changing a Web Access Mask

### Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Web Access Mask**.
2. On the Web Access Mask page, in **User-Defined Access Masks and Names**, select the check box adjacent to an access mask.
3. Click **Change**.
4. On the Change Access Masks page, enter a new name of the mask in the text box next to the access mask number.
5. In the **Editable** column, select the check boxes to add permissions for the following:
   - Software Management: Software Install
   - Software Management: Software Removal
   - Software Management: Advanced Software Install
6. Click **Submit**.

### Next steps

Add a software installer login.

## Adding a software installer login

### Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Administrator Accounts**.
2. On the **Select Action** page, select **Add Login**.
3. Select **Privileged Administrator**.
4. Click **Submit**.
5. On the Administrator Accounts -- Add Login: Privileged Administrator page, enter information in the following fields:
   a. **Login name**
   b. **Additional groups (profile)**: Select the profile that you added in the previous step. See Adding a Web Access Mask on page 95.
   c. **Date after which account is disabled-blank to ignore (YYYY-MM-DD)**: Clear this field.
   d. **Enter password or key**
   e. **Re-enter password or key**

**Note:**

Do not change other default values in the Administrator Accounts -- Add Login: Privileged Administrator page.

6. Click **Submit**.

# Chapter 7: Single server configuration checklist

The following table describes the initial administration tasks, the administrator who performs these tasks, and the component that the administrator requires to perform the tasks.

Because IT responsibilities in large organizations are divided among different individuals, the table contains the reference information that a specific administrator requires.

Administrators must complete the *Administering Avaya Aura® Messaging* chapters in the following sequence:

| No. | Task | Chapter number | Administrator type | Location | ✔ |
|---|---|---|---|---|---|
| 1 | Prepare the network. | Chapter 1 | Network administrator | — | |
| 2 | Load the Avaya voice messaging forms onto the Exchange server. | Chapter 1 | Exchange administrator | Exchange server | |
| 3 | Prepare the telephony server. | Locate *Switch Configuration Notes for Avaya Aura® Messaging* on http://support.avaya.com/ | Switch administrator | Telephony server | |
| 4 | Set up the storage role. | Chapter 3 | Messaging administrator | Single server | |
| 5 | Set up the application role. | Chapter 4 | Messaging administrator | Single server | |
| 6 | Set up sites and topology. | Chapter 5 | Messaging administrator | Single server | |

# Appendix A: Reusing your Microsoft Exchange server

Customers who use a Microsoft Exchange server to store Avaya Modular Messaging voice mail can reuse the Exchange server when upgrading to Avaya Aura® Messaging. To make the change, you must perform the following four main tasks:

1. Install Avaya Aura® Messaging.
2. Make the Microsoft Exchange environment unavailable on the Avaya Modular Messaging system.
3. Prepare the Microsoft Exchange server for the Avaya Aura® Messaging system.
4. Integrate the Microsoft Exchange server with the Avaya Aura® Messaging system.

**Important:**

After the integration, you cannot get the voice mail messages that Avaya Modular Messaging stores on the Microsoft Exchange server using the Avaya Aura® Messaging TUIs. To access these voice mail messages, use the Microsoft Outlook client.

## Installing Avaya Aura® Messaging

| Number | Task | Reference | Notes |
|---|---|---|---|
| 1 | Install Avaya Aura® Messaging. | See Installing Messaging on page 75. | - |
| 2 | Integrate Avaya Aura® Messaging with the telephony server. | See the *Integrating with the telephony server* topic in *Administering Avaya Aura® Messaging*. | - |

## Removing Avaya Modular Messaging from service

| Number | Task | Reference | Notes |
|---|---|---|---|
| 1 | Busy out ports on Message Application Server (MAS). | See Busying out ports on page 101. | - |
| 2 | Log off all remote logins. | See Logging off all remote logins on page 102. | - |

*Table continues…*

| Number | Task | Reference | Notes |
|---|---|---|---|
| 3 | Stop Avaya Modular Messaging services. | See Stopping Modular Messaging services on page 102. | - |
| 4 | Shut down all MAS servers. | — | - |
| 5 | Remove Avaya Modular Messaging software components. | See Removing Modular Messaging software components on page 103. | |

## Preparing the Microsoft Exchange server

| Number | Task | Reference | Notes |
|---|---|---|---|
| 1 | Load the Avaya voice messaging forms onto the Exchange server. | See the *Installing the voice message form* topic in *Administering Avaya Aura® Messaging*. | The voice message form adds a dedicated toolbar to Microsoft Outlook. |
| 2 | Configure the minimum required service account permissions. | See *Administering Avaya Aura® Messaging*. | The service account is a normal Active Directory Domain User account with an Exchange mailbox. You must provide Exchange Impersonation permissions to the account. A caller can then perform operations by using permissions related to the impersonated account, not to the caller account. |
| 3 | Configure Exchange Web Services. | See the Microsoft Exchange Server website. | If you are using Microsoft Exchange as your storage destination, you must configure Exchange Web Services (EWS) to disregard client certificates. EWS provides the functionality to enable client applications to communicate with the Exchange server. EWS provides access to most data that is available through Microsoft Office Outlook.<br><br>By ignoring client certificates, any system can establish a connection with the EWS component and after authentication access the EWS component. |

## Integrating the Microsoft Exchange server with the Avaya Aura® Messaging system

| Number | Task | Reference | Notes |
|---|---|---|---|
| 1 | Configure Microsoft Exchange as your storage | See the *Configuring a storage destination* topic in | Perform this task to use Microsoft Exchange as your storage destination. |

*Table continues…*

| Number | Task | Reference | Notes |
|---|---|---|---|
| | destination for the Avaya Aura® Messaging system. | *Administering Avaya Aura® Messaging*. | |
| 2 | Integrate Avaya Aura® Messaging with the telephony server. | See the *Integrating with the telephony server* topic in *Administering Avaya Aura® Messaging*. | - |
| 3 | Add users from Active Directory. | See the *Adding users from Active Directory* topic in *Administering Avaya Aura® Messaging*. | Add Active Directory users directly to the Avaya Aura® Messaging system without manually configuring the user values. |
| 4 | Run a remote update. | See the *Running a remote update manually* topic in *Administering Avaya Aura® Messaging*. | Remote updates provide an automatic method of administering remote users.<br>Using remote updates:<br>• You can automatically add all remote users who need to exchange messages across the network.<br>• Your local Avaya Aura® Messaging system can exchange user information with each remote Avaya Aura® Messaging system that you administered on the local system. |
| 5 | Run a diagnostic test on the storage server. | See the *Running diagnostic tests on the storage server* topic in *Administering Avaya Aura® Messaging*. | - |

**Related Links**

Busying out ports on page 101
Logging off all remote logins on page 102
Stopping Modular Messaging services on page 102
Removing Modular Messaging software components on page 103

# Busying out ports

The PBX administrator must use the procedures appropriate for this PBX to busy out the ports. Depending on the switch integration, the administrator might be able to temporarily reroute calls to other MASs. If an MAS is unavailable, callers into the system might hear ring-no answer or a busy signal.

### Procedure

1. Change the monitor to display the MAS.
2. Use the port monitor to disable the MAS ports:
   a. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Port Monitor**.
   b. In the Port Monitor window, press and hold down the **Shift** key or **Control (Ctrl)** key and select all ports.
   c. Right-click the port list, and select **Disable**.
   d. Verify that the status of all ports is **Disabled**.
   e. Click **OK** to close this window.

**Related Links**

Reusing your Microsoft Exchange server on page 99

# Logging off all remote logins

### Procedure

1. Log on to the MAS using an account with administrative permissions.
2. Click **Start** > **Programs** > **Administration**.
3. Open **Windows Task Manager**, and click the **Users** tab.
4. Select remote logins, and click **Logoff**.
5. Click **Cancel** to exit.

**Related Links**

Reusing your Microsoft Exchange server on page 99

# Stopping Modular Messaging services

### Procedure

1. On the monitor, go to the first MAS.
2. To stop all the Modular Messaging services:
   a. Navigate to the `C:\Avaya_Support\tools\servicecontrol` directory.
   b. Double-click the **StopMMServices.exe** file.

   **Note:**

   This script also stops Dialogic services and some Windows services.

A command window displays the status of the Modular Messaging services shutdown. The script might take several minutes to complete.

3. To confirm that all Modular Messaging services are stopped:
   a. On the desktop, double-click the **Monitor** icon.
   b. In the left pane, click **Services (Local)**.
   c. In the right pane, scroll down to the list of installed Modular Messaging services. All services start with the abbreviation *MM*.
   d. Verify that the **Status** column is blank.
4. If a service is still running, repeat Steps 2 and 3.

**Related Links**

Reusing your Microsoft Exchange server on page 99

# Removing Modular Messaging software components

Use the Modular Messaging Uninstallation Wizard to remove Modular Messaging software components.

### Procedure

1. On MAS, click **Start** > **Settings** > **Control Panel**.
2. From the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs window, scroll down the list of currently installed programs to **MM Uninstallation Wizard**.
4. Select the Modular Messaging software components that you want to remove.
5. Click **Uninstall** and follow the prompts to confirm your choices.

**Related Links**

Reusing your Microsoft Exchange server on page 99

# Index

## I



## K



## L



## M



## N



## O



## P

## R



## S



## T

## U



## V



## W