Installing and Configuring Avaya Aura® Communication Manager

03-603558
Issue 1.3
Release 6.0.1
December 2010

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 generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by 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 Web sites 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 its Hardware and Software (“Product(s)”). 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 Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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 End User a license within the scope of the license types described below. 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 End User. “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. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

- Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, 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.
- Named User License (NU). End User 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). Customer 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”). (see “Third-party Components” for more information).

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those

Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura® are trademarks of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(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(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.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Introduction to Communication Manager

Avaya Aura® Communication Manager organizes and routes voice, data, image and video transmissions. It can connect to private and public telephone networks, Ethernet LANs, and the Internet.

Communication Manager is a key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital and IP-based communication devices. In addition, Communication Manager delivers robust PBX features, high reliability and scalability, and multi-protocol support. It includes advanced mobility features, built-in conference calling and contact center applications and E911 capabilities.

Communication Manager seeks to solve business challenges by powering voice communications and integrating with value-added applications. It is an open, scalable, highly reliable and secure telephony application. Communication Manager provides user and system management functionality, intelligent call routing, application integration and extensibility, and enterprise communications networking.

Communication Manager enables the virtual enterprise with:

- Robust voice and video call processing capabilities
- Advanced workforce productivity and mobility features
- Built-in conferencing and contact center applications
- Centralized voice mail and attendant operations across multiple locations
- Connectivity to a wide range of analog, digital, and IP-based communication devices
- Support for SIP, H.323 and many industry standard communications protocols over a variety of different networks
- More than 700 powerful features in all
- High availability, reliability and survivability.

Communication Manager installation overview

The Communication Manager installation process consists of

- identifying or procuring necessary hardware, software, and other equipment
- installing the necessary hardware and equipment
- Installing System Platform on the server

- Installing the appropriate Communication Manager template on the server
- Configuring the applications on the template, including Communication Manager, CMM, and Branch Session Manager.
- Completing the postinstallation verification tasks.

You perform installation when you did not have Communication Manager running as an application in your enterprise. Installation is also required if one or more of your current Communication Manager executable files have been corrupted.

Communication Manager can be installed on S8300D, S8510, S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 server.

Note:

Communication Manager is installed on System Platform as a template.

Upgrading Communication Manager is required when there is a new release available that you can start using by shutting down Communication Manager, replacing the executable files by the new ones and restarting Communication Manager.

The upgrade process is covered in *Upgrading Servers to Avaya Aura™ Communication Manager Templates*.

System Platform overview

Avaya Aura® System Platform technology delivers simplified deployment of Unified Communications and Contact Center applications. This framework leverages virtualization technology, predefined templates, common installation, licensing, and support infrastructure.

The advantages of System Platform include:

- Ability to install predefined templates of one or more Avaya software applications on a single server in a virtualized environment
- Simplified and faster installation of software applications and solutions
- Simplified licensing of applications and solutions
- Web Console with a common Avaya look and feel
- Remote access and alarming for Avaya Services and Avaya Partners
- Coordinated backup and restore
- Coordinated software upgrades

System Platform enables real-time communications solutions to perform effectively in a virtualized environment. System Platform effectively manages the allocation and sharing of server hardware resources, including the CPU, memory, disk storage, and network interfaces. To continue delivering the high reliability of real-time communications that Avaya customers expect, System Platform is being delivered solely through an *appliance* model, which includes an Avaya Server, System Platform, and the Avaya software applications.

Easy installation

Using solution templates on System Platform significantly reduces the installation time. During the installation, the installer program installs the predefined solution template, which takes less time then installing the applications individually. The installation process is simple and requires the staff to possess basic software installation skill. System Platform allows remote installation of product-specific templates.

Solution templates

A solution template is a set of one or more applications to be installed on System Platform. Installers must download these templates using the Product Licensing and Delivery System (PLDS) (http://plds.avaya.com). PLDS allows Avaya customers, Avaya Partners, and associates to manage software licensing and to download software for various Avaya products.

System Platform provides an installation wizard for the template. The installation wizard makes it possible for you to configure template-specific parameters, including network and server details, or to upload a preconfigured Electronic Preinstallation Worksheet (EPW) created in a stand-alone version of the installation wizard.

Note:

You must install System Platform before installing the solution template software on a single server.

Remote serviceability

System Platform can be serviced remotely, eliminating the need for a service technician to visit the customer site.

System Platform uses Secure Access Link (SAL), which is an Avaya serviceability solution for support and remote management. SAL provides remote access and alarm reception capabilities for Avaya and participating Avaya Partners.

SAL uses your existing Internet connectivity to facilitate remote support. All communication is outbound from your environment using encapsulated Hypertext Transfer Protocol Secure (HTTPS).

Avaya Partners without a SAL Concentrator must provide their own IP-based connectivity (for example, B2B VPN connection) to deliver remote services.

Important:

Avaya Partners and customers must ensure that SAL is always configured and registered with Avaya during 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.

Networking in System Platform

System Platform uses software bridging to support networking for virtual machines. Software bridging works like a network switch inside the system. During installation, System Platform creates two software bridges: avpublic and avprivate.

The avpublic bridge is connected to a physical interface and is intended to be the default connection to your LAN. Most virtual machines have a virtual interface on the avpublic bridge to connect to your network. When connected to your network, these virtual machines can be reached by ping.

The avprivate bridge is not connected to any physical interface and is intended for communication among the virtual machines in a single server. The IP addresses used on avprivate cannot be reached from your network.

Some templates require additional connections to your network. In some cases, this results in System Platform creating another software bridge. This bridge contains the name specified by the template, and this name is displayed during template installation or in the Network Configuration page.

If a virtual machine has high or real time traffic requirements, it can be assigned a dedicated network interface card (NIC) in the template file. This means the virtual machine is assigned another physical NIC on the system (for example, Avaya Aura® Media Services uses eth3) and does not use avpublic. See the respective template documentation for more information.

For using a dedicated NIC, you must have a separate cable connection to your network. Also make sure that both Ethernet interface and the dedicated NIC are connected to the network before those machines can communicate through an IP in the same way that they would do when dealing with separate physical machines. For example, in Midsize Business Template, Console Domain is on the avpublic bridge and Media Services has a dedicated NIC (eth 3). So you must connect eth0 and eth3 to the network before attempting to ping the Media Services virtual machine from the Console Domain.

Communication Manager templates overview

Communication Manager as a template is a virtualized version that runs on System Platform. This image has all the features that Communication Manager supports whether it is on a duplicated server or a branch server. The templates support Communication Manager duplication on S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Servers. The templates support Communication Manager which configures as Main, Survivable Core (formerly known as Enterprise Survivable Server - ESS), or Survivable Remote (formerly known as Local Survivable Processor - LSP). In addition, the templates allow customers to use their network infrastructure without dedicated control networks.

Note:

The Communication Manager installation and administration Web pages refer to Survivable Core as Enterprise Survivable Server (ESS) and Survivable Remote as Local Survivable Processor (LSP), respectively.

The advantages of using a solution as a template on System Platform are as follows:

- Simplified and faster installation of the solution
- Simplified licensing of applications and solutions

- Web Console with a common Avaya look and feel
- Remote access and alarming for Avaya Services and Avaya Partners
- Coordinated backup and restore
- Coordinated software upgrades

The Communication Manager templates come in two categories: Avaya Aura® for Communication Manager Main/Survivable Core and Avaya Aura® for Communication Manager Survivable Remote. The templates in each category are listed below:

- Avaya Aura® for Communication Manager Main/Survivable Core template category contains the following templates:
  - Simplex CM Main/Survivable Core
  - Duplex CM Main/Survivable Core
  - Embedded CM Main
- Avaya Aura® for Communication Manager Survivable Remote template category contains the following templates:
  - Simplex Survivable Remote
  - Embedded Survivable Remote

Avaya Aura® for Communication Manager Main/Survivable Core

The Communication Manager Main/Survivable Core templates include the following applications:

- Communication Manager
- Communication Manager Messaging

  Note:

  Communication Manager Messaging is available only if Communication Manager is configured as the main server. Communication Manager Messaging and Utility Services are not available on Duplex Main/Survivable Core.

- Utility Services

Both Simplex Main/Survivable Core and Duplex Main/Survivable Core templates can be installed on an Avaya S8800, HP ProLiant DL360 G7,or Dell™ PowerEdge™ R610 Servers. The Simplex Main/Survivable Core can be installed on an Avaya S8510 server with a total 8 Gb memory as an upgrade only. The Embedded Main template is installed on an Avaya S8300D server in either a G250, G350, G430, G450, or G700 Media Gateway.

Avaya Aura® for Communication Manager Survivable Remote

The Communication Manager Survivable Remote templates include the following applications:

- Communication Manager
- Branch Session Manager
- Utility Services

The Simplex Survivable Remote is installed on an Avaya S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server. Simplex Survivable Remote can be installed on an Avaya S8510 server with 8 Gb memory as an upgrade only. Embedded Survivable Remote is installed on Avaya S8300D server in either a G250, G350, G430, G450, or G700 Media Gateway. Both templates are used in the following two scenarios:

- Communication Manager Evolution Server
- Communication Manager Feature Server

Note:

For information on template capacities, refer to the *Avaya Aura® Communication Manager System Capacities Table*.

Checklist of hardware and software requirements

Requirement	Note	✔
Standard equipment racks	The racks are used to mount the servers and media gateways. The customer-supplied racks must be EIA-310D (or equivalent) standard 19-in. (48-cm) 4-post equipment racks. They must be properly installed and solidly secured. Ensure that the screws that come with the racks are present. If using an enclosed rack cabinet, ensure that the cabinet has adequate ventilation.	
One S8800 server / One HP ProLiant DL360 G7 / One Dell™ PowerEdge™ R610 Two S8800 servers / Two HP ProLiant DL360 G7 / Two Dell™ PowerEdge™ R610	If you are using a simplex core or survivable remote template. If you are using a duplex core template. For physical installation information, refer to *Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager*.	
S8300D server	If you are using an embedded main or embedded survivable remote template. For physical installation information, refer to the appropriate media gateway quick start book.	
A laptop with an Ethernet crossover cable or, optionally, a USB keyboard, USB mouse, and VGA monitor	To be used to connect to the servers for installing System Platform and Communication Manager applications. You cannot use the keyboard, mouse, and monitor with the Avaya S8300 Server.	

Requirement	Note	✔
	Note: Depending on the capabilities of the network interface card in your laptop, you might be able to use a straight-through cable for this connection. See the documentation for your laptop. The supported keyboard types are sg-latin1, sk-qwerty, slovene, sv-latin1, trq, uautf, uk, and us.	
DVD writer application	To write the software ISO images to the blank DVDs. You download the ISO images from the Product Licensing and Delivery System (PLDS) Web site, http://plds.avaya.com.	
Blank DVDs	The media for the ISO images.	
Bootable DVD, if available	Contains the release 6.0 versions of System Platform and Communication Manager installer files provided by Avaya.	
CAT5 Ethernet cable	To be used to connect the servers to the enterprise network.	
Crossover Ethernet cable	To be used to connect collocated duplicated servers.	
Uninterruptible Power Supply (UPS)	To provide power during a power outage. You can order a UPS from Avaya.	
VPN SAL Gateway	To access the application servers. This is optional.	
Correct firewall rules	To secure the customer network.	
Filled-out worksheets with the system and network information	To be used for configuringSystem Platform and Communication Manager as part of the installation process.	
Access to the customer network		
EPW file	The Electronic Pre-Installation Worksheet can be filled out ahead of time, speeding up the installation time. This is optional.	

Server and template matrix

The following table provides the list of templates and the servers on which the individual templates can be installed.

Template type	S8800/HP ProLiant DL360 G7/ Dell™ PowerEdge™ R610	S8300D
Main/Survivable Core—duplex version	✔	
Main/Survivable Core—simplex version	✔	
Survivable Remote—simplex version	✔	
Survivable Remote—embedded version		✔
Main—embedded version		✔

What Avaya provides

Avaya provides the following items

- For standalone servers: One Avaya S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Servers for a Communication Manager simplex configuration, and two Avaya S8800, HP ProLiant DL360 G7,or Dell™ PowerEdge™ R610 Servers for a Communication Manager duplex configuration.

  For embedded servers: One Avaya S8300D Server with a choice of media gateways, such as the Avaya G430 Media Gateway or Avaya G450 Media Gateway.
- Slide rails to mount the servers in a rack.
- Other hardware as ordered, such as an uninterruptible power supply (UPS). UPS is a required component.
- System Platform installation software.
- Communication Manager installation software.
- Product registration form. The form is available on http://support.avaya.com. Click **More Resources** > **Equipment Registration (Partners only)**. Click **Universal Install/SAL Product Registration Request Form** under **Non-Regional (Product) Specific Documentation**. For more information, see Registering the system.

Checklist for Communication Manager installation

Use this checklist to ensure that you have carried out the installation of Communication Manager per Avaya recommendation. If you are installing a duplex template, follow this checklist to install Communication Manager on the second server.

#	Task	Note	✔
1	Complete and submit the Universal Install/SAL Product Registration Request form. When opening the Excel based form, click **Enable Macros**; otherwise, the form automation will not work. Submit the completed form using the built in e-mail button. See Registering the system. **Note:** Allow 48 business hours for a reply.	**Important:** Make sure that you submit the registration form at least two business days before the planned installation date.	
2	Gather the required information relating to installation, such as IP configuration information, DNS addresses, and NTP server addresses. See Installation worksheet for System Platform on page 115.		
3	Download the following files from PLDS • System Platform installer ISO image file • appropriate solution templates and license files • Electronic Pre-installation Worksheet file . See Downloading software in PLDS on page 21.		
4	Verify that the downloaded ISO images match the images on the PLDS Web site. See Verifying the ISO image on a Linux-based computer on page 21 and Verifying the ISO image on a Windows-based computer on page 22.		
5	Write the ISO images to separate DVDs. See Writing the ISO image to DVD on page 23.		
6	Install the Electronic Pre-installation Worksheet file and fill out the fields See Creating an EPW file on page 24		
7	If you are installing System Platform from a laptop, perform the following tasks: • 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. • Configure the IP settings of the laptop for direct connection to the server. See Configuring the laptop for direct connection to the server on page 27. • Disable use of proxy servers in the Web browser on the laptop.		

#	Task	Note	✔
	See Disabling proxy servers in Microsoft Internet Explorer on page 28 or Disabling proxy servers in Mozilla Firefox on page 28 .		
8	If you are installing System Platform from a laptop, connect the laptop to the server. See Connecting to the server through the services port on page 42. **Note:** If you are using an S8300D server, ensure that the media gateway is on the latest firmware.		
9	Turn on the server.		
10	Place the DVD in the DVD drive on the server. See Starting the installation from your laptop on page 30 or Starting the installation from the server console on page 31 depending on your selection of installation method.		
11	If using the server console to install System Platform, enter the **`vspmediacheck`** command and press **Enter**. The **`vspmediacheck`** command verifies that the image on the System Platform DVD is not corrupt. See Starting the installation from your laptop on page 30 or Starting the installation from the server console on page 31 depending on your selection of installation method.		
12	If using your laptop to install System Platform, establish a Telnet connection to the server. See Starting the installation from your laptop on page 30.		
13	Select the required keyboard type. See Selecting the type of keyboard on page 32.		
14	Verify that the image on the System Platform DVD is not corrupt. See #unique_23.		
15	Configure the network settings for the System Domain (Domain-0). See Configuring network settings for System Domain on page 33.		
16	Configure the network settings for the Console Domain.		

#	Task	Note	✔
	See Configuring network settings for Console Domain on page 36.		
17	Configure the time zone for the System Platform server. See Configuring the time zone for the System Platform server on page 37.		
18	Configure the date and time and specify an NTP server if using for the System Platform server. See Configuring the date and time for the System Platform server on page 37.		
19	Configure the System Platform passwords. See Configuring System Platform passwords on page 38.		
20	Verify that System Platform installed correctly. See Verifying installation of System Platform on page 41.		
21	Configure the SAL gateway. See Configuring the SAL Gateway.		
22	Select the required Communication Manager template. See Installing a solution template on page 58.		
23	Confirm template network configuration. See Confirming template network configuration on page 69.	Complete this step only if using an EPW file.	
If installing the template using the Installation Wizard rather than the EPW file, complete these additional tasks.			
24	Specify IP address and hostname for the Communication Manager virtual machine. See Configuring Network Settings.		
25	Specify user ID and password for the privileged administrator. See Configuring Customer Login on page 65. **Note:** You may not need to add a privileged administrator for Communication Manager, but you may need it for BranchSession Manager.		
25	If the template includes Utility Services, configure DHCP. See Configuring DHCP on page 65.		
26	If the template includes Branch Session Manager, configure Branch Session Manager. See Installing		

#	Task	Note	✔
	and configuring Branch Session Manager on page 66.		
27	Review summary information and note if any setting needs to be done. See Reviewing summary information on page 67.		
28	Proceed with the Communication Manager installation. See Confirming installation on page 67.		

Registering for PLDS

1. Go to the Avaya Product Licensing and Delivery System (PLDS) Web site (https://plds.avaya.com).
   You will be redirected to the Single sign-on (SSO) Web site.
2. Log in to SSO using SSO ID and Password.
   You will be redirected to the PLDS registration page.
3. If you are registering:
   - as an Avaya Partner, enter the Partner Link ID. If you do not know your Link ID, send an e-mail 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 in PLDS

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

    When the install is complete, PLDS displays the downloads again with a checkmark next to the downloads that have been completed successfully.

Verifying the downloaded ISO image

Verifying the ISO image on a Linux-based computer

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.

1. Enter `md5sum filename`, where *filename* is the name of the ISO image. Include the .iso file extension in the filename.
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

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.

1. Download a tool to compute md5 checksums from one of the following Web sites:
   - http://www.md5summer.org/
   - http://zero-sys.net/portal/index.php?kat=70
   - http://code.kliu.org/hashcheck/

   Note:

   Avaya has no control over the content published on these external sites. Please 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 recommendations

Avaya recommends use of high quality, write-once, blank DVDs. Multiple rewrite DVDs are prone to error and should not be used.

When writing the data to the DVD, Avaya recommends a slower write speed of 4X or at 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 want to write on media are less than 680 Mb in size, you can use a CD instead of a DVD.

Writing the ISO image to DVD

Prerequisites

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.

This procedure requires a computer or server that has a DVD writer and software that is capable of writing ISO images to DVD.

Important:

When the ISO image is being written 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.

Write the ISO image of the installer to a DVD.

Creating an EPW file

Prerequisites

You must have the zip file for the stand-alone installation wizard downloaded from PLDS and installed on your computer.

To create the EPW file, you use a stand-alone installation wizard. The stand-alone installation wizard is the same as the installation wizard that launches as part of the template installation. By downloading, installing, and filling out the fields in the stand-alone installation wizard file ahead of time, you save time during the template installation. The stand-alone installation wizard installs only on a Windows PC.

1. Unzip the stand-alone installation wizard file and extract the file to a location on your computer.
2. Locate the setup_wizard.exe file and click it to start the setup.
3. Click through the Setup screens to complete the installation.

   The installation creates a shortcut link within the **Start** > **Programs** menu.
4. To launch the stand-alone installation wizard, select **Start** > **Programs** > ***PreinstallWizardname*** > `Run`***PreinstallWizardname***, where *PreinstallWizardname* is the name of the stand-alone installation wizard for the template, for example, SP Pre-installation Wizard.

   The stand-alone installation wizard opens in your default browser.
5. On the Load Files page, select the appropriate template, and then click **Next Step**.
6. On the CM Template Type page, select the template you plan to install, and then click **Next Step**.
7. Complete the fields on the rest of the screens. Click **Next Step** to move from screen to screen.
8. On the Save page, read the warning text, and then click **Accept**.
9. Click **Save EPW file**, and save the file to a location on your computer.

   Give the file a unique name that identifies the template.

Related topics:

Installing Communication Manager using the Installation Wizard on page 64

Chapter 2: Installing System Platform

System Platform installation overview

System Platform servers

System Platform is installed on an Avaya S8300D, Avaya S8800, HP ProLiant DL360 G7,or Dell™ PowerEdge™ R610 server. The servers arrive at the customer's site with all appropriate components and memory, and nothing needs to be added to the servers on site. Servers are installed in customer-provided racks and connected to the customer's network.

Installation process

Installation of System Platform consists of the following tasks:

1. Install the server hardware.
2. Connect the server to the customer network. If installing duplicated servers, connect both servers to the customer network.
3. If collocated duplicated servers, connect the two servers together.

   Important:

   For HP ProLiant DL360 G7 and Dell™ PowerEdge™ R610 servers, you need to install System Platform Service Pack 2 version. This Service Pack allows System Platform and the Communication Manager templates to be installed on these servers.

Software installation

To install System Platform, you must first download the ISO image from the Avaya PLDS Web site (http://plds.avaya.com) and then burn the ISO image to a DVD.

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. This option does not apply to the S8300D. To install to the S8300D, you must use a laptop connected to the services port.

Note:

On S8800 and S8510 servers, the services port is located on the back of the servers, while it is located on the faceplate of the S8300D server.

During the installation, you will need to boot the servers. The S8800 and the S8300D server takes in excess of 7 minutes to boot. The server is ready to boot when the power-on LED changes from a fast flashing state to a slow flashing state.

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 a PuTTY SSH client and Telnet application 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 27.

Use the provided worksheets and checklists during installation.

Related topics:

Connecting to the server through the services port on page 42

Preinstallation tasks for System Platform

Server installation

Depending on your server type, refer to one of the following hardware installation guides:

- For S8300D server with G250 Media Gateway: *Quick Start for Hardware Installation: Avaya G250 Media Gateway*
- For S8300D server with G350 Media Gateway: *Quick Start for Hardware Installation: Avaya G350 Media Gateway*
- For S8300D server with G430 Media Gateway: *Quick Start for Hardware Installation: Avaya G430 Media Gateway*
- For S8300D server with G450 Media Gateway: *Quick Start for Hardware Installation: Avaya G450 Media Gateway*

- For S8300D server with G700 Media Gateway: *Quick Start for Hardware Installation: Avaya G700 Media Gateway*
- For S8800 server: *Installing the Avaya S8800 Server for Avaya Aura^{TM} Communication Manager*

Connecting your laptop to the server

Configuring the laptop for direct connection to the server

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. The procedure may differ slightly for other versions of Windows.

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, type `192.11.13.5`.
8. In the **Subnet mask** field, type `255.255.255.252`.
9. In the **Default gateway** field, type `192.11.13.6`.
10. Click **OK**.

Disabling proxy servers in Microsoft Internet Explorer

To connect directly to the services port, you must disable the proxy servers in Internet Explorer.

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

   Tip:

   When you need to reenable 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

To connect directly to the services port, you must disable the proxy servers in Firefox.

Note:

This procedure is for Firefox on a Windows-based laptop. The procedure may differ slightly if your laptop is running Linux or another operating system.

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

   Tip:

   When you need to reenable the proxy server, select the appropriate option again.
7. Click **OK** to close each dialog box.

Installing System Platform software

Starting the installation

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. This option does not apply to the S8300D. To install to the S8300D, you must use a laptop connected to the services port.

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 a PuTTY SSH client and Telnet application 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 27.

Powering on a server

1. If using an S8800 server, perform the following steps:
    a. Wait for the fast flashing of the power-on LED (about 3 flashes per second) to cease to about 1 flash per second.
    b. Turn on the server by pressing the power-on button.
    The LED will change to solid indicating that the server is booting up. The LED will remain solid indicating that the server is booted.
2. If using an S8300D server, perform the following steps:
    a. Seat the circuit pack for the first time or re-seat the circuit pack if it was already seated.
    b. Power on the gateway in which the S8300D server resides.
    c. Connect the CD/DVD drive to the server.

Note:

The attached CD/DVD drive that the S8300D server uses for software installation runs on a battery. Make sure that the battery is fully charged and its on/off switch is set in the on position during the installation.

Starting the installation from your laptop

Prerequisites

- 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.

Note:

On S8800 server, eth1 is the services port labeled 2 on the server itself. On S8300D server, eth0 is the services port, which is on the front of the server face plate and is marked as 'SERVICES'.

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

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

   Note:

   Depending on the capabilities of the network interface card (NIC) in your laptop, you might be able to use a straight-through cable for this connection. See the documentation for your laptop.
2. Turn on the server.
3. Insert the System Platform DVD in the server DVD drive.
   The server boots from the DVD.
4. Verify that the laptop can ping the service port by performing the following steps:
   a. Click **Start** > **Run**.
   b. Type `ping -t 192.11.13.6`

      Note:

      Allow sufficient time for the `ping` command to return continuous responses before proceeding to the next step.
5. Open a PuTTY session by performing the following steps:

   Important:

   If you use a Telnet client other than PuTTY, or if you forget to set the proper terminal emulation for the PuTTY client, the system might not display the

Keyboard Type screen correctly. This screen problem does not affect the installation.

a. Open the PuTTY application.

b. In the **Host Name** field, enter `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.

Related topics:

Configuring the laptop for direct connection to the server on page 27
Powering on a server on page 29

Starting the installation from the server console

Note:
This procedure does not apply to embedded servers such as S8300D.

Prerequisites

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

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, so you can connect to the

server through Telnet. At this point, if you want to install through the server console, 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.

Related topics:

Powering on a server on page 29

Selecting the type of keyboard

On the Keyboard Type screen, select the type of keyboard that you have.

Note:

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

- 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 33.
- The System Domain Network Configuration screen is displayed if you are installing System Platform from the server console and did not enter the **`vspmediacheck`** command at the boot prompt. See Configuring network settings for System Domain on page 33.

Next steps

- Verify that the System Platform image was copied correctly to the DVD. See Verifying the System Platform image on the DVD on page 33.

  OR
- Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain on page 33.

Verifying the System Platform image on the DVD

Use this procedure to verify that the System Platform image was 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.

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 is corrupt, you must write a new DVD with the System Platform image. Before using the new DVD, make sure that you restart the server.

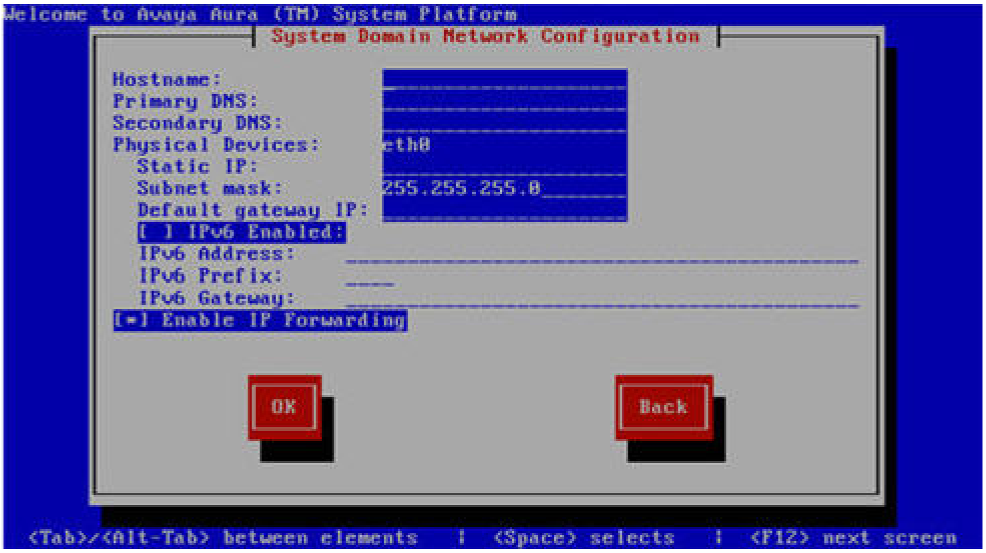
The system displays the System Domain Network Configuration screen.

Next steps

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

Configuring network settings for System Domain

1. On the System Domain Network Configuration screen, complete the following fields:
   - **Hostname**. Enter a fully qualified domain name (FQDN), for example, SPDom0.mydomainname.com.
   - **Primary DNS**
   - (Optional) **Secondary DNS**



```
Welcome to Avaya Aura (TM) System Platform
            ┤ System Domain Network Configuration ├

    Hostname:
    Primary DNS:
    Secondary DNS:
    Physical Devices:          eth0
      Static IP:
      Subnet mask:             255.255.255.0
      Default gateway IP:
      [ ] IPv6 Enabled:
      IPv6 Address:
      IPv6 Prefix:
      IPv6 Gateway:
    [*] Enable IP Forwarding

              OK                          Back

  <Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

Note:

In the case of S8300D server, the above screen will have an additional field of **VLAN ID**.

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. If using an S8300D server, use the Tab key to highlight the **VLAN ID** field. Enter a valid VLAN ID.
5. Use the `Tab` key to highlight the **IPv6 Enabled** field. Press the `Spacebar` to either enable or disable entering IP addresses in IPv6 format.
6. If you have enabled IPv6, fill in the following fields:
    - **IPv6 Address**
    - **IPv6 Prefix**
    - **IPv6 Gateway**
7. 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).

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

Next steps

Configure network settings for Console Domain. See Configuring network settings for Console Domain on page 36.

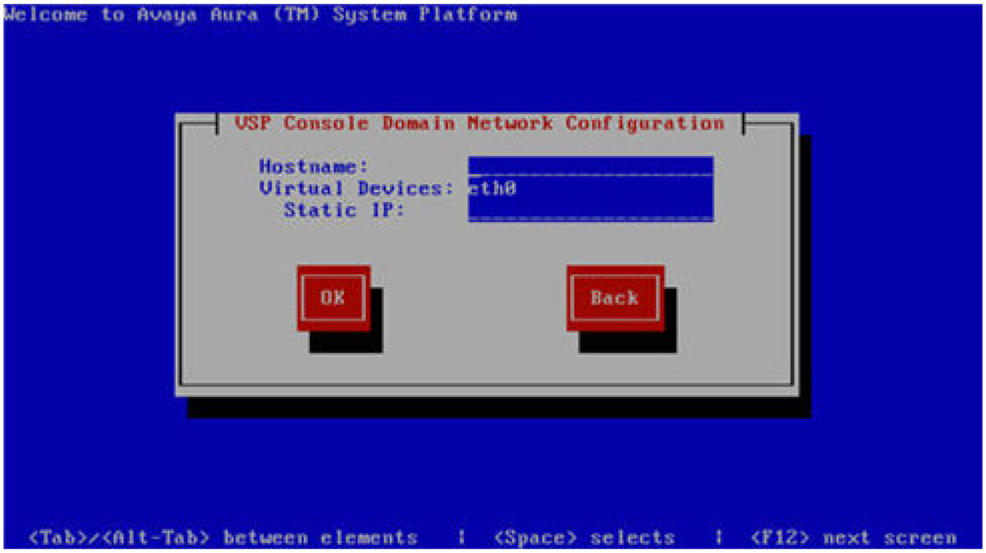
System Domain Network Configuration field descriptions

Name	Description
Hostname	The host name for System Domain (Domain-0). This must be a fully qualified domain name (FQDN), for example, SPDom0.mydomainname.com.
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. 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. This default gateway IP address will be used for all the virtual machines if you do not specify gateway IP addresses for them.
VLAN ID	The virtual LAN ID, which is displayed if using an S8300D server. Enter a value between 1 and 4092 to match the ICC-VLAN configured on the media gateway. **Note:** To get the ICC-VLAN configured on the media gateway, login to the media gateway command line interface and run the `show run` command.
IPv6 Enabled	The indicator to show whether the IP addresses required by System Platform need to be IPv6-compliant.
IPv6 Address	The IPv6-compliant IP address of System Domain.
IPv6 Prefix	The IPv6 prefix for **IPv6 Address**.

Name	Description
IPv6 Gateway	The IP address of the default gateway for IPv6 traffic.
Enable IP Forwarding	The indicator to show whether IP forwarding is enabled. An asterisk on the left of the field denotes that IP forwarding is enabled. 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

1. On the VSP Console Domain Network Configuration screen, complete the following fields to set up the Console Domain network:
   - **Hostname**. Enter an FQDN, for example, SPCdom.mydomainname.com.
   - **Static IP**



```
Welcome to Avaya Aura (TM) System Platform

VSP Console Domain Network Configuration

        Hostname:
 Virtual Devices: eth0
       Static IP:

<Tab>/<Alt-Tab> between elements   |   <Space> selects   |   <F12> next screen
```

2. Select **OK** and press **Enter** to accept the configuration and display the Time Zone Selection screen.

Next steps

Configure the time zone for the System Platform server. See Configuring the time zone for the System Platform server on page 37.

System Platform Console Domain Network Configuration field descriptions

Name	Description
Hostname	The host name for the Console Domain. This must be an FQDN, for example, SPCdom.mydomainname.com.
Static IP	The IP address for the Console Domain. **Note:** 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).

Configuring the time zone for the System Platform server

1. On the Time Zone Selection screen, select the time zone in which the server is located.

   Note:

   On the main server, you need to select the time zone relevant to the server location. In the case of ESS or LSP, you must set up the time zone, which is the same as that of the main server. In a failover situation, the ESS or the LSP provide the correct time information to display on the phones with the help of the time zone and the translation information.

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 System Platform server. See Configuring the date and time for the System Platform server on page 37.

Configuring the date and time for the System Platform server

Avaya recommends that you use an NTP server within your network to synchronize the time of the System Platform server.

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

   Note:
   Ensure that the time set here is correct. Changing the time in a virtual machine environment requires rebooting the virtual machines. Therefore, Avaya recommends setting the time correctly on this screen during the installation

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. See Configuring System Platform passwords.

Configuring System Platform passwords

Prerequisites

Configure the date and time for the System Platform server.

1. On the Passwords screen, enter new passwords for all logins. You must enter each password twice to ensure that you are not making any mistakes in typing.

   If you do not enter new passwords, the defaults are used. 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
manager (for ldap)	root01	Administrator for the System Platform local Lightweight Directory Access Protocol (LDAP) directory.

Login	Default password	Capability
		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.

Important:

Avaya highly recommends that you enter new passwords instead of using the default passwords. Make a careful note of the passwords that you set for all logins. Customers are responsible for managing their passwords.

Passwords must be at least six characters long. Avaya recommends using uppercase and lowercase alphabetic characters and at least one numeral or special character.

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. Select **OK** and press **Enter** to accept the passwords and continue the installation.

Result

The installation takes approximately 6 minutes. During this time, you can see the Package Installation page with progress bars, followed by the Running page, as the system completes the post-install scripts. After the installation is completed, the system ejects the DVD and reboots the server. If you used a laptop for installation, the telnet session supporting the System Platform installation is dropped.

After the reboot, the system displays the Linux login page for System Domain (Domain-0).

Passwords field descriptions

Note:

Passwords must be at least six characters long. Avaya recommends using uppercase and lowercase alphabetic characters and at least one numeral or special character.

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.
ldap Password	The password for the ldap login. System Platform uses a local LDAP directory to store login and password details. Use this login and password to log in to the local LDAP directory. This login does not have permissions to access the System Platform Web Console.

Checking network configuration

1. Log in to the System Platform Web Console.
2. Click **Server Management** > **Network Configuration**.
3. In the Network Configuration page, ensure that the following fields have the same values that you setup during System Platform installation:
    - **Dom0 Hostname**
    - **Primary DNS**
    - **Secondary DNS**
    - **Physical Network Interface**
    - **Gateway address**
    - **Network mask**
    - **DNS**
4. Log out from the System Platform Web Console.

Verifying installation of System Platform

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 43.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

After completing installation of System Platform, perform this procedure to check for problems with the installation.

1. Access the System Platform Web Console. See Accessing the System Platform Web Console on page 43.
2. 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.
3. Perform the following steps to log in to Console Domain as `cust`:
   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 `cust`, and type the password that you entered for the cust login during System Platform installation.
   e. Type `exit` to exit Console Domain.

Important:

If you cannot log in to Console Domain as `admin` or `cust` or access the System Platform Web Console, contact Tier 3 Engineering.

Accessing System Platform

Connecting to the server through the services port

Prerequisites

- 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.

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

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

   Note:

   Depending on the capabilities of the network interface card (NIC) in your laptop, you might be able to use a straight-through cable for this connection. See the documentation for your laptop.
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

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 43.

Important:
You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access 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.

1. Open a compatible Internet browser on your computer.

Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

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:

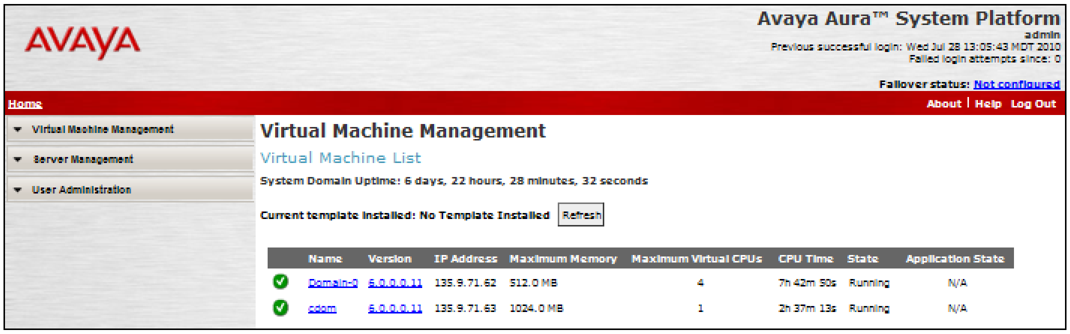
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

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.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Related topics:

Enabling IP forwarding to access System Platform through the services port on page 43

Accessing the command line for System Domain

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. Alternatively, 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.

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 obtain the IP address of System Domain (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 access Console Domain from System Domain, type **`xm list`**, note the ID for *udom*, and then type **`xm console`** *`udom-id`*. When prompted, login 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

> **Important:**
> You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

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

> **Tip:**
> You can obtain the IP address of Console Domain (cdom) 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.

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

Chapter 3: Installing the license file and authentication file

Installing the license file

Obtaining and installing the license file

Use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Communication Manager 6.0 and later. PLDS is an online, Web-based tool for managing license entitlements and electronic delivery of software and related license files.

Earlier versions of Communication Manager, except Communication Manager 5.2.1 that is part of Avaya Aura® Midsize Business Template, continue to use the Remote Feature Activation (RFA) online tool for license files. Communication Manager 5.2.1 that is part of Avaya Aura®Midsize Business Template uses PLDS to manage licenses. After you obtain the license file, use WebLM to install it. WebLM is a Web-based application for managing licenses and is installed as part of System Platform in the Console Domain.

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

For Communication Manager 6.0 and later, license files are installed only on the Communication Manager main server. License files are not installed on survivable servers. Survivable servers receive licensing information from the main server.

If you are licensing a duplicated pair configuration, you must install the license file on both servers. The license file is not synchronized from the active server to the standby server.

A 30-day grace period applies to new installations or upgrades to Communication Manager 6.0. You have 30 days from the day of installation to install a license file.

PLDS

The Avaya Product Licensing and Delivery System (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 Communication Manager, the license entitlements on the order are automatically created in PLDS. Once these license entitlements are created, you receive an e-mail notification from PLDS. This e-mail notification includes 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 is obtained from the WebLM Web interface.

Related topics:

Obtaining the WebLM host ID on page 49

Activating license entitlements in PLDS on page 49

Duplicated server licensing

If you are licensing a duplicated pair configuration, you must install the license file on both servers. The license file is not synchronized from the active server to the standby server.

When you activate a Communication Manager license file for a duplicated pair in PLDS, you must provide the WebLM host ID for both servers. Both host IDs are included in the license file that is generated, and that license file must be installed on both servers in the duplicated pair.

Accessing WebLM from the System Platform Web Console

1. Start the System Platform Web Console and log in.
2. In the navigation pane, click **Server Management** > **License Management**.
3. On the License Management page, click **Launch WebLM License Manager** .
4. When WebLM displays its Logon page, enter the user name and password for WebLM. For initial login to WebLM, the user name is `admin`, and the password is `weblmadmin`. However, you must change the password the first time that you log in to WebLM.

Related topics:

Accessing the System Platform Web Console on page 43

Obtaining the WebLM host ID

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 is obtained from the WebLM Web interface.

Important:

If you are licensing a duplicated pair configuration, you must obtain the WebLM host ID for both servers. Perform this procedure on both servers.

1. Start the WebLM Web interface and log in.
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.

Related topics:

Accessing WebLM from the System Platform Web Console on page 48

Activating license entitlements in PLDS

Prerequisites

Host ID of the License Host if you are activating license entitlements on a new License Host.

Use the License Activation Code (LAC) to activate one or more license entitlements. You may choose to activate all of the licenses or specify the number of licenses that you want to activate from the quantity available. Upon successful activation of the license entitlements, PLDS creates an Activation Record and sends an Activation Notification e-mail message to the customer that is registered with the entitlements. The Activation Record and Activation Notification provide details on the number of activated licenses and the License Host. The license file can be accessed on the License/Keys tab of the Activation Record in PLDS and is also an attachment to the Activation Notification e-mail message. You need to install the license file on WebLM to use the licenses.

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

1. Type `http://plds.avaya.com` in your Web browser to access the Avaya PLDS Web site.
2. Enter your Login ID and password to log on to the PLDS Web site.

3. In the **LAC(s)** field of the Quick Activation section, enter the LAC that you received in an e-mail message.

   Note:

   If you do not have an e-mail message with your LAC, you can search for your entitlements and locate the LAC. See "Searching for entitlements" in *Getting Started with Avaya PLDS*.

   Note:

   The Quick Activation automatically assumes that you want to activate all license entitlements on LAC and gives the option to remove line items and enter the amount of each license to activate (full or partial amount).

4. Enter the License Host information.

   You can either create a new license host or use an existing license host.

   Note:

   Communication Manager servers in a duplicated pair share the same license host. Separate (non-duplicated pair) Communication Manager servers cannot share a single 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. The Host ID is obtained from the Server Properties page of the WebLM server where the license file will be installed.

7. Enter the number of licenses you want to activate.
8. Review the Avaya License Agreement and accept the agreement if you agree.
9. Perform the following steps to send an activation notification e-mail message:
   a. In the **E-mail to** field, enter e-mail addresses for any additional activation notification recipients.
   b. Enter any comments or special instructions in the **Comments** field.
   c. Click **Finish**.
10. Click **View Activation Record**.
    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application. From **License/Key** tab, you can view and download the license file. Each license file must installed on the WebLM server associated with the License Host.
    - The **License/Key** tab displays the license files resulting from the license activation. Communication Manager and Call Center are licensed together in

a single license file. Communication Manager Messaging is licensed its own separate license file. From **License/Key** tab, you can view and download the license files. Each license file must be installed on the WebLM server that is associated with the License Host.

Installing a license file in WebLM

Prerequisites

You must have a license file obtained from the Avaya PLDS Web site.

Important:

If you are licensing a duplicated pair configuration, you must install the license file on both servers. The license file is not synchronized from the active server to the standby server.

1. Start the WebLM Web interface and log in.
2. Click **Install License** in the left navigation pane.
3. On the Install License page, enter the license file path. You can also click **Browse** to select the license file.
4. Click **Install** to install the license file.
   WebLM displays a message on the successful installation of the license file.

Related topics:

Accessing WebLM from the System Platform Web Console on page 48

Installing the authentication file

Authentication files for Communication Manager

The authentication file contains Access Security Gateway (ASG) keys and the server certificate for Communication Manager. ASG keys make it possible for Avaya Services to securely access the customer's system.

System Platform and Communication Manager share the same authentication file. A default authentication file is installed with System Platform. However the default file must be replaced with a unique file. Unique authentication files are created by the Authentication File System (AFS), an online application at http://rfa.avaya.com. After you create and download the authentication file, you install it from the System Platform Web Console of the Communication Manager server. When you install the authentication file in System Platform, the file is automatically installed on Communication Manager, Utility Server, and any other virtual machines on the server.

Every time that you upgrade Communication Manager to a new major release, you need to create and install a new authentication file.

Authentication files for duplicated servers and survivable servers

For duplicated pair configurations, you must install the same authentication file on both the active server and standby server. The authentication file is not synchronized from the active server to the standby server.

Each survivable server must have its own unique authentication file. A unique file must be installed from the System Platform Web Console of each server.

About the authentication file

AFS authentication files have a plain text XML header with encrypted authentication data and an encrypted server certificate.

Each authentication file contains an authentication file ID (AFID) that identifies it. You need this AFID to create a new authentication file for an upgrade or to replace the current authentication file on the server.

Starting the AFS application

Prerequisites

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.

You must have a login ID and password to start the AFS application. You can sign up for a login at http://rfa.avaya.com.

1. Type `http://rfa.avaya.com` in your Web browser.
2. Enter your login information and click **Submit**.
3. Click **Start the AFS Application**.
   A security message is displayed.
4. Click **I agree**.
   The AFS application starts.

Creating an authentication file for a new system

You can choose to download the authentication file directly from AFS to your computer, or you can have the authentication file sent in an e-mail message.

1. Start and log in to AFS.
2. In the **Product** field, select **SP System Platform**.
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. Enter the fully qualified domain name (FQDN) of the host system where Communication Manager is installed. For duplicated Communication Manager servers, enter the alias FQDN.
6. Enter the FQDN of the Utility Server.
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 have the authentication file sent in an e-mail message:
    a. Enter the e-mail address in the **Email Address** field.
    b. Click **Download file via email**.
    AFS sends the e-mail message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.
    c. Save the authentication file to a location on the e-mail recipient's computer.

    After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
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.

Related topics:

Starting the AFS application on page 52

Obtaining the AFID from System Platform Web console

1. Start the System Platform Web Console and log in.
2. In the navigation pane, click **User Administration** > **Authentication File**.
   The AFID is displayed in the **AFID** field. An AFID of 7100000000 is the default authentication that is installed with System Platform. The default file must be replaced with a unique file.

Related topics:

Accessing the System Platform Web Console on page 43

Installing an authentication file

Prerequisites

You must create and download the authentication file from AFS.

System Platform and Communication Manager share the same authentication file. When you install the authentication file in System Platform, the file is automatically installed on Communication Manager, Utility Server, and any other virtual machines on the server. However, the suser account must be created on Communication Manager for the authentication file to be installed on Communication Manager. Once the suser account is created, the authentication file that is installed on System Platform (default or unique), is automatically installed on Communication Manager. The authentication file must be installed on Communication Manager for you to log in to Communication Manager.

1. Start the System Platform Web Console and log in.
2. Click **User Administration** > **Authentication File**.
3. Click **Upload**.
4. In the Choose File to Upload dialog box, find and select the authentication file, and then click **Open**.

Note:

To override validation of the AFID and date and time, select **Force load of new file** on the Authentication File page. Select this option if you:

- need to install an authentication file that has a different unique AFID than the file that is currently installed, or
- have already installed a new authentication file but need to reinstall the original file

You do not need to select this option if you are replacing the default authentication file with a unique authentication file.

Caution:

Use caution when selecting the **Force load of new file** option. If you install the wrong authentication file, certificate errors and login issues may occur.

5. Click **Install**.
   The system uploads the selected authentication file and validates the file. The system installs the authentication file if it is valid.
6. To confirm that the authentication file is installed on Communication Manager, check the Authentication File page of the SMI.

Related topics:

Accessing the System Platform Web Console on page 43

Obtaining the AFID from System Platform Web console on page 54

Chapter 4: Installing Communication Manager templates

This section provides procedures for installing Communication Manager as a template. The following templates are the ones you select as part of the installation wizard:

- Duplex CM Main/Survivable Template: This template offers Communication Manager only and is installed on a pair of S8800, HP ProLiant DL360 G7,or Dell™ PowerEdge™ R610 Servers, which offer server redundancy. The server pair can be designated the role of main server or a survivable core server. The filename is called CM_Duplex.ovf.
- Simplex CM Main/Survivable Template: This template offers Communication Manager, Communication Manager Messaging, and Utility Services on a single S8800, HP ProLiant DL360 G7, Dell™ PowerEdge™ R610, or an S8510 Server. The S8510 Server is available in an upgrade scenario only. The server can be designated the role of main server or a survivable core server.Communication Manager Messaging is enabled only if the server role is a main server. The filename is called CM_Simplex.ovf.
- Embedded CM Main Template: This template offers Communication Manager, Communication Manager Messaging, and Utility Services on an embedded S8300D Server. The server can be designated the role of main server only. The filename is called CM_onlyEmbed.ovf.
- Simplex Survivable Remote Template: This template offers Communication Manager, Session Manager , and Utility Services on a single S8800, HP ProLiant DL360 G7, Dell™ PowerEdge™ R610, or an S8510 Server. The S8510 Server is available in an upgrade scenario only. The server can be designated the role of survivable core server only. Session Manager can be installed and administered at installation or activated at a later time. The filename is called CM_SurvRemote.ovf.
- Embedded Survivable Remote Template: This template offers Communication Manager, Session Manager, and Utility Services on an embedded S8300D Server. The server can be designated the role of survivable remote server only. Session Manager can be installed and administered at installation or activated at a later time. The filename is called CM_SurvRemoteEmbed.ovf.

Solution template

Configuring system settings for System Platform

1. Click **Server Management** > **System Configuration**.
2. On the System Configuration page, modify the fields as appropriate. If the default settings are satisfactory, no changes are necessary.
3. Click **Save**.

System configuration field descriptions

Use the System Configuration page to configure proxy settings, change the current keyboard layout, or enable or disable statistics collection.

Name	Description
Proxy Status	Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform.
Proxy Address	The address for the proxy server.
Proxy Port	The port address for the proxy server.
Keyboard Layout	Determines the specified keyboard layout for the keyboard attached to the System Platform server.
Statistics Collection	If you disable this option, the system stops collecting the statistics data. **Note:** If you stop collecting statistics, the system-generated alarms will be disabled automatically.

Installing a solution template

Approximate installation times for the Communication Manager templates are as follows:

- CM_Duplex: 15 minutes
- CM_Simplex: 25 minutes
- CM_onlyEmbed: 50 minutes
- CM_SurvRemote: 30 minutes. If installing Branch Session Manager, add another 30 minutes to the installation time.
- CM_SurvRemoteEmbed: 65 minutes. If installing Branch Session Manager, add another 30 minutes to the installation time.

1. Log in to the System Platform Web Console as admin.
2. Click **Virtual Machine Management** > **Solution template**.

   The system displays the Search Local and Remote Template page. Use this page to select the template that you want to install on System Platform.
3. Select a location from the list in the **Install Templates From** box.

   Note:

   If the template installation files are located on a different server (for example, Avaya PLDS or HTTP), you may be required to configure a proxy depending on your network. See Configuring a proxy.
4. Click **Search** to display a list of template descriptor files (each available template has one template descriptor file).
5. On the Select Template page, click the required template, and then click **Select** to continue.
   The system displays the Template Details page with information on the selected template and its Virtual Appliances.
6. Click **Install** to start the template installation.

   If the template you selected supports an Electronic Pre-installation Worksheet (EPW), the system prompts you to continue without an EPW or to provide an EPW file. The system also prompts you with pages that require your input such as IP addresses for the applications that are included in the template. These pages vary depending on the template that you are installing. If you provided an EPW file, some of these pages may be pre-populated with data from the EPW.

   If you are installing a Communication Manager template from a DVD, make sure that you remove the CD/DVD from the CD-ROM/DVD tray after the template installation completes.

Next steps

If you are following this document as part of upgrading your Communication Manager template, refer to *Upgrading to Avaya Aura^{TM} Communication Manager* for further instructions.

Related topics:
Configuring system settings for System Platform on page 58

Search Local and Remote Template field descriptions

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

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

Search Local and Remote Template button descriptions

Name	Description
Install	Installs the solution template. This button is displayed only if no template is currently installed on System Platform.
Configure Proxy	Active only when you select the HTTP option to search for a solution template. Lets you configure a proxy for the HTTP address.

Name	Description
	A proxy may also be required for Secure Access Link (SAL) and alarming to access the internet.
Upgrade	Upgrades the installed solution template from the selected template location option. This button is displayed only if a template is installed on System Platform.
Delete Installed Template	Deletes the currently installed template. This button is displayed only if a template is installed on System Platform.

Beginning installation of template

In the Template Details page, click **Install**.
The Template Installation page shows the installation progress. The template installation time varies, depending on which template is being installed.

Template Details button descriptions

Name	Description
Install	Begins the template installation.

Template Installation button descriptions

Name	Description
Cancel Installation	Cancels the template installation that is currently in progress.

EPW file

An EPW file

An Electronic Pre-installation Worksheet (EPW) file plays an important role in installing a template. It helps you to set up and save those parameters required during the template installation ahead of time. When installing the template, you upload the EPW file and let the installation happen with minimal intervention.

Using an EPW file provides the following benefits:

- If you are installing the Duplex Main/Survivable Core template, you can copy and modify an EPW to provide an EPW for each server.
- If you need to install a template on multiple survivable core or remote servers, you can copy and modify an EPW to generate EPWs for multiple survivable servers. This is especially useful if you have as many as 250 survivable servers.
- If you need to reinstall a template, you can reuse the original EPW with all the correct specifications.

EPW file creation

The EPW file shows the same configuration pages that appear in the Installation Wizard if you install the template without using the EPW file. The configuration pages that the EPW file shows depend on which template you select. The following table summarizes the configuration pages applicable for different Communication Manager templates:

Template	Network Settings page	Customer Login page	DHCP page	Branch Session Manager page	Summary page
Duplex Main/ Survivable Core	✔	✔			✔
Simplex Main/ Survivable Core	✔	✔	✔		✔
Embedded Survivable Remote	✔	✔	✔	✔	✔
Simplex Survivable Remote	✔	✔	✔	✔	✔

Template	Network Settings page	Customer Login page	DHCP page	Branch Session Manager page	Summary page
Embedded Main	✔	✔	✔		✔

You will find the tasks corresponding to the pages listed in the above table later in this document that explain how to setup the installation parameters in those pages.

Selecting a template installation method

Prerequisites

If using an Electronic Pre-installation Worksheet (EPW) file, you must have it filled out and in an accessible location. If not using an EPW file, make sure you have the filled-out worksheet available.

When installing a template, you can either upload a filled-out EPW file or continue with the installation process. Using an existing EPW file ensures that Communication Manager is installed across the enterprise in a standard manner.

1. To upload an EPW file:
    a. Click **Browse EPW file** to locate the EPW file on the computer or enterprise network.
    b. Click **Upload EPW file** to upload the file.
2. To continue installation without an EPW file, click **Continue without EPW file**.

   Refer to the installation and configuration worksheet when filling in the fields.

Select Template button descriptions

Name	Description
Select	Confirms the template selection and shows the next page.
Browse EPW File	Opens a Browse window that allows you to locate the EPW file.
Upload EPW file	Uploads the EPW file for installing the template.
Continue without EPW file	Proceeds to installing the template without using an EPW file.

Name	Description
Cancel	Cancels the action.

Installing Communication Manager using the Installation Wizard

The topics in this section are applicable if installing Communication Manager templates using the Installation Wizard rather than the filled-out EPW file. Use the worksheets in the appendix to fill in the fields.

Virtual machine details

Entering virtual machine IP address and hostname

1. In the Template Details page, the top portion shows the fields that are setup during System Platform installation. In the bottom portion, fill in the following fields for the Communication Manager virtual machine:
    a. IP address
    b. Hostname
2. Click **Next Step**.

Network Settings field descriptions

Virtual Machine

Name	Description
IP Address	Is the IP address of the application virtual machine.
Hostname	Is the host name of the application virtual machine. For Branch Session Manager, the Hostname must be a fully qualified domain name; it is not a requirement for the other applications. The Branch Session Manager application shows only if installing the Simplex Survivable Remote or Embedded Survivable Remote template.

New customer login

Configuring Customer Login

The login created here is for the privileged administrator.

1. Fill in all the fields.
2. Click **Next Step**.

Customer Login field descriptions

Field descriptions

Name	Description
Login name	Is the user ID of the privileged administrator.
Password	Is the password of the privileged administrator.
Re-type password	Is the same password as entered for the **Password** field.

DHCP

Configuring DHCP

If you are installing a template that provides Utility Services, you have the option of enabling DHCP.

Enable and configure DHCP if you want Communication Manager to act as an internal Dynamic Host Configuration Protocol server for telephones. If you plan to use an external DHCP server, then do not enable the internal DHCP. You can access additional, more advanced DHCP configuration options through the web console of the Utility Services after completing the installation.

1. Select **Enable DHCP** to enable the internal DHCP server.

2. Fill in all the fields.
3. Click **Next Step**.

DHCP field descriptions

Name	Description
Enable DHCP	When selected, enables the internal DHCP server. If you are using an external DHCP server, then do not select.
DHCP Network Address	The network IP address for the DHCP subnet.
DHCP Subnet Mask	The subnet mask associated with the network.
DHCP Router address	The IP address of the router on the DHCP subnet.
DHCP Pool IP address range	The range of IP addresses to be used within the DHCP pool.
DHCP DNS Server IP address	(Optional) The IP address of a DNS server if used.
DHCP WINS Server IP address	(Optional) The IP address of a WINS server if used.

Branch Session Manager

Installing and configuring Branch Session Manager

If you are installing either the Simplex Survivable Remote or the Embedded Survivable Remote template, you have the option of installing Branch Session Manager.

1. On the Configure Branch Session Manager page, select **Install Session Manager**.
2. Fill in all the fields.
3. Click **Next Step**.

Branch Session Manager field descriptions

Name	Description
Install Session Manager	When selected, installs Branch Session Manager.
DNS Search	Is the DNS domain name for the search list in the form of, for example, domain.com. If more than one search list name, separate them with commas.
System Manager IP	Is the IP address of the System Manager server.
System Manager FQDN	Is the fully qualified domain name of the System Manager server.
Trust Management Password	Is the Enrollment Password used to access the System Manager server.
Re-type Password	Is the same password as entered for the **Trust Management Password** field.

Reviewing summary information

1. Review the summary information that may show incomplete settings. If you want to go to previous installation step for completing those settings, click the **Previous Step** link.
2. Click **Next Step**.

Continuing the template installation

Confirming installation

The Confirm Installation page shows you which required and optional fields were not set. You may go back and complete those fields or continue with the installation without completing those fields. You may complete the installation with incomplete fields.

When used as an EPW, this page's title is Save.

1. To correct or complete any fields

- Select the appropriate page from the navigation pane.
- Click **Previous Step** to return to the appropriate page.

2. To continue, click **Install** to start the template installation.

Result

At this time, the installation progress screen resumes.

Approximate installation times for the Communication Manager templates are as follows:

- CM_Duplex: 15 minutes
- CM_Simplex: 25 minutes
- CM_onlyEmbed: 50 minutes
- CM_SurvRemote: 30 minutes. If installing Branch Session Manager, add another 30 minutes to the installation time.
- CM_SurvRemoteEmbed: 65 minutes. If installing Branch Session Manager, add another 30 minutes to the installation time.

The template installation is complete when the message `Template Installation Completed Successfully` appears in the top section of the page.

Confirm Installation button descriptions

Name	Description
Install	Starts the template installation. Shows only when part of the actual template installation.
Download installation package	Allows you to save the EPW file to a location of your choice. Shows only when used as an EPW.

Verifying virtual machine installation

Prerequisites

You must wait about 5 minutes after the template installs before you try to access the Web console.

Some applications within the template may take longer to install than others. You may want to verify that they are running before proceeding. This is an optional task.

1. Log in to the System Platform Web console.
2. Under the **Virtual Machine List**, check the **State** column to determine that all virtual machines are running.
3. If some of the virtual machines are not running, you may click the **Version** link to open the Detailed Version Information for domain page.

   You can view the installation progress within this page.
4. When done, click **Close** to close the detail page.

Confirming template network configuration

Prerequisites

You must be logged into the System Platform Web Console to perform this task.

Once the installation is complete, verify that the appropriate fields were populated within the Network Configuration screen. If you installed a template with Branch Session Manager and installed it, you need to complete some fields.

1. Select **Server Management** > **Network Configuration**.
2. Verify the settings shown in the various sections.
3. Within the bsm section, fill in the following fields:
   - Enrollment Password—This is the enrollment password from System Manager.
   - SIP Entity IP Address—This is the IP address of the Branch Session Manager's Security Module that is used for signaling. The IP address must match the one used for BSM as a SIP Entity specified in System Manager.
4. Click **Save**.

Next steps

If you used this document to install a Communication Manager template as part of an upgrade, return to the upgrade documentation after finishing this task.

Managing patches

Patch management

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

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

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Configuring a proxy

If the patches are located in a different server (for example, Avaya PLDS or HTTP), you may need to configure a proxy depending on your network.

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

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Removing patches

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch that you want to remove.
4. On the Patch Detail page, click **Deactivate**, if you are removing a template patch.
5. Click **Remove**.

   Tip:
   You can clean up the hard disk of your system by removing a patch installation file that is not installed. To do so, in the last step, click **Remove Patch File**.

Search Local and Remote Patch field descriptions

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

Name	Description
Supported Patch File Extensions	The patch that you are installing should match the extensions in this list. For example, *.tar.gz,*.tar.bz,*.gz,*.bz,*.zip,*.tar,*.jar,*.rpm,*.patch.
Choose Media	Displays the available location options for searching a patch. Options are: • **Avaya Downloads (PLDS)**: The template files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password. The list will contain all the templates to which your company is entitled. Each line in the list begins with the “sold-to” number to allow you to select the appropriate template for the site where you are installing. You may hold the mouse pointer over the selection to view more information about the “sold-to” number. • **HTTP**: Files are located in a different server. You must specify the Patch URL for the server. • **SP Server**: Files are located in the vsp-template file system in the System Platform server. You must specify the Patch URL for the server. **Tip:** When you want to move files from your laptop to the System Platform Server, you may encounter some errors, as System Domain (Dom–0)

Name	Description
	and Console Domain support only SCP, but most laptops do not come with SCP support. You can download the following two programs to enable SCP (Search on the Internet for detailed procedures to download them): - Pscp.exe - WinSCP • **SP CD/DVD**: Files are located in a System Platform CD or DVD. • **SP USB Disk**: Files are located in a USB flash drive. • **Local File System**: Files are located in a local computer.
Patch URL	Active only when you select **HTTP** or **SP Server** as the media location. URL of the server where the patch files are located.

Button descriptions

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

Patch List field descriptions

The Patch List page displays the patches on the System Platform server for installing or removing. Use this page to view the details of patch file by clicking on the file name.

Name	Description
System Platform	Lists the patches available for System Platform under this heading.
Solution Template	Lists the patches available for the respective solution templates under respective solution template headings.
Patch ID	File name of a patch.

Name	Description
Description	Information of a patch, for example, if the patch is available for System Platform the description is shown as SP patch.
Status	Shows the status of a patch. Possible values of **Status** are **Installed**, **Not Installed**, **Active**, and **Not Activated**.
Service Effecting	Shows if installing the patch causes the respective virtual machine to reboot.

Button descriptions

Button	Description
Refresh	Refreshes the patch list.

Patch Detail field descriptions

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

Name	Description
ID	File name of the patch file.
Version	Version of the patch file.
Product ID	Name of the virtual machine.
Description	Virtual machine name for which the patch is applicable.
Detail	Virtual machine name for which the patch is applicable. For example, Console Domain (cdom patch).
Dependency	Shows if the patch file has any dependency on any other file.
Applicable for	Shows the software load for which the patch is applicable.
Service effecting when	Shows the action (if any) that causes the selected patch to restart the System Platform Web Console.
Disable sanity when	Shows at what stage the sanity is set to disable.
Status	Shows if the patch is available for installing or already installed.
Patch File	Shows the URL for the patch file.

Button descriptions

Button	Description
Refresh	Refreshes the Patch Details page.

Button	Description
Patch List	Opens the Patch List page, that displays the list of patches.
Install	Installs the respective patch.
Activate	Activates the installed patch of a solution template.
Deactivate	Deactivates the installed patch of a solution template.
Remove	Removes the respective patch.
Remove Patch File	Removes the respective patch file. The button appears only if the patch file is still present in the system. On removing the patch file, the button does not appear.

Chapter 5: Administering SAL on System Platform

SAL Gateway

Secure Access Link (SAL) Gateway provides Avaya remote support engineers and Avaya Partners with remote access and alarming for serviceability of applications on System Platform. The Secure Access Link (SAL) Gateway application is automatically installed with System Platform. SAL Gateway software is also available separately for stand-alone deployments. See **Secure Access Link** on http://support.avaya.com. The SAL Gateway application 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 do so. The SAL gateway application 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, eliminating the need for a service technician to visit the customer's site. System Platform uses the customer’s existing Internet connectivity to facilitate 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:

Business Partners and customers must ensure that SAL is always configured and registered with Avaya 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.

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 included in the solution template that is installed. For example, virtual machines might include Communication

Manager, Communication Manager Messaging, SIP Enablement Services, and other applications that are included in the template.

To configure SAL, perform these high-level steps:

1. Register the system.

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

   Avaya assigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway and managed device that is registered. In the context of System Platform, managed devices are the applications that are included 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 included 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.

Related topics:

Registering the system

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 *Universal Install/SAL Registration Request* form and submit the form to Avaya. The form includes complete instructions. Open the Microsoft Excel form with macros enabled.

This form is available at http://support.avaya.com. In the navigation pane, click **More Resources** > **Equipment Registration**. Under Non-Regional (Product) Specific Documentation, click **Universal Install/SAL Product Registration Request Form**, or search *Universal Install/SAL Product Registration Request Form*.

Note:

Avaya must receive the registration form at least two business days before the planned installation date.

Related topics:

Registering the system

System and browser requirements

Browser requirements for SAL Gateway:

- Internet Explorer 6.x and 7.x
- Firefox 3.5

System requirements:

A computer with access to the System Platform network.

Starting the SAL Gateway user interface

1. Log in to the System Platform Web Console.
2. Click **Server Management** > **SAL Gateway Management**.
3. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.
4. When the SAL Gateway displays its 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.

   When you are successfully logged in, the Managed Element page of the SAL Gateway user interface is displayed. If the SAL Gateway is up and 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

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:
    - **Gateway IP Address**
    - **Solution Element ID**
    - **Gateway Alarm ID**
    - **Alarm Enabled**

    For field descriptions, see Gateway Configuration field descriptions on page 81.
4. (Optional) Complete the following fields if desired:
    - **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. If you want to cancel your changes, click **Undo Edit**.

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

    See the *Secure Access Link Gateway 1.8 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, Avaya recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Gateway Configuration field descriptions on page 81

Applying configuration changes on page 88

Gateway Configuration field descriptions

Name	Description
Gateway Hostname	A host name for the SAL Gateway. ⚠ **Warning:** 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.
Gateway IP Address	The IP address of the SAL Gateway. This IP address is the same as that of cdom (also called VSPU).
Solution Element ID	The Solution Element ID that uniquely identifies the SAL Gateway. If you have not obtained your System Platform Solution Element IDs, start the registration process as described in Registering the system. The system uses the SAL Gateway Solution Element ID to authenticate the SAL Gateway and its devices with the Secure Access Concentrator Remote Server.
Gateway Alarm ID	The Alarm ID of the SAL Gateway. The system uses the value in the **Gateway Alarm ID** 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. 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 who are working on tickets and want to 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 you want inventory collected.

Configuring a proxy server

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.

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. If using an authenticating HTTP proxy server, complete the following fields:
   - **Login**
   - **Password**
4. Click **Apply**.
5. (Optional) Once 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 1.8 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, Avaya recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Proxy server field descriptions on page 83

Applying configuration changes on page 88

Proxy server field descriptions

Name	Description
Use Proxy	Check box to enable use of a proxy server.
Proxy Type	Type of proxy server that is used. Options are: • **SOCKS 5** • **HTTP**
Host	The IP address or the host name of the proxy server.
Port	The port number of the Proxy server.
Login	Login if authentication is required.
Password	Password for login if authentication is required.

Configuring SAL Gateway communication with a Secure Access Concentrator Core Server

Use the SAL Enterprise page to review settings for communication between SAL Gateway and a Secure Access Concentrator Core Server (SACCS). The SACCS handles alarming and inventory. Do not change the default settings unless you are explicitly instructed to do so.

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **SAL Enterprise**.
   The SAL Enterprise page is displayed.
2. Do not change the default settings on this page.

   See the *Secure Access Link Gateway 1.8 Implementation Guide* for more information. This document is available at http://support.avaya.com.
3. (Optional) Once 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 1.8 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, Avaya recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

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

Related topics:

SAL Enterprise field descriptions on page 84
Applying configuration changes on page 88

SAL Enterprise 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 Enterprise	IP Address or the host name of the primary Secure Access Concentrator Core Server. The default value is `secure.alarming.avaya.com`.
Port	Port number of the primary Secure Access Concentrator Core Server. The default value is `443`.
Secondary Enterprise	This value must match the value in the **Primary Enterprise** field.
Port	This value must match the value in the **Port** field for the primary server.

Configuring SAL Gateway communication with a Secure Access Concentrator Remote Server

Use the Remote Access page to review settings for communication between SAL Gateway and a Secure Access Concentrator Remote Server (SACRS). The SACRS handles remote access, and updates models and configuration. Do not change the default settings unless you are explicitly instructed to do so.

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

The Remote Access page is displayed.

2. Do not change the default settings on this page unless you are explicitly instructed to do so.
3. (Optional) Once 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 1.8 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, Avaya recommends that you 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 terminates all active connections.

Related topics:

Remote Access field descriptions on page 85
Applying configuration changes on page 88

Remote Access field descriptions

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

Configuring NMS

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.

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 1.8 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, Avaya recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Network Management Systems field descriptions on page 86

Applying configuration changes on page 88

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.

Name	Description
Community	The community string of the NMS server. Use `public` as the **Community**, as SAL agents support only public as community at present.

Managing service control

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

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Service Control**.
   The system displays the Gateway Service Control page. The page lists the following services:
   - **Inventory**
   - **Alarming**
   - **Remote Access**
   - **Health Monitor**

   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 stopping the Remote Access service. Doing so will block you from accessing SAL Gateway remotely.

Applying configuration changes

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Apply Configuration**.
   The system displays the Apply Configuration Changes page.
2. Click the **Apply** next to **Configuration Changes**.

   See the *Secure Access Link Gateway 1.8 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.

Configuring a managed element

Prerequisites

Complete the Managed Element Worksheet for SAL Gateway. See Managed element worksheet for SAL Gateway.

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

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, Avaya recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Managed element worksheet for SAL Gateway
Applying configuration changes on page 88
Managed Element field descriptions on page 89

Managed Element field descriptions

Name	Description
Host Name	Host name for the managed device or any meaningful name that describes the device to your or your provider (for example, CM_Bldg5_Production).
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. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely.
Product ID	The Product ID or the Alarm ID. The Product ID is included 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. 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 who are working on tickets and want to 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

Name	Description
Inventory collection schedule	Interval in hours at which you want inventory collected from 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. 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 for which you want health monitoring suspended for the managed device. SAL Gateway resumes monitoring the device after the configured time elapses.

Chapter 6: Configuration tasks for Communication Manager

Communication Manager configuration

To complete the installation, you must use the Communication Manager System Management Interface (SMI) to complete the configuration tasks. You must also have IP forwarding enabled. If you disabled it as part of the System Platform installation, see Enabling IP forwarding to access System Platform through the services port on page 43.

The primary areas are

- Server role—Use to indicate whether the server is a main, survivable core, or survivable remote server.
- Network configuration—Use to configure the IP-related settings for the server. Many of the fields are prepopulated with data generated as part of the System Platform and template installation.
- Duplication parameters—Use to configure the duplication settings if you installed the Duplex Main/Survivable Core template.

Server role

Server role configuration

A telephony system may be made up of several servers, each fulfilling a certain role, such as main or primary server, a second redundant server, Survivable Remote server, or Survivable Core server. You configure the individual server roles using the System Management Interface. Depending on the server role, configure at least two of the following data:

- Server settings
- Survivable data
- Memory

Template type and server role

The Communication Manager template installed on the server determines which roles are available. The following table summarizes the roles for which you can configure the individual servers:

Template type	Main or primary server	Survivable Remote server	Survivable Core server	Second server
Simplex Main/ Survivable Core	✔		✔	
Duplex Main/ Survivable Core	✔		✔	✔
Embedded Main	✔			
Simplex Survivable Remote		✔		
Embedded Survivable Remote		✔		

Configuring server role

Prerequisites

You must be logged into the Communication Manager System Management Interface.

1. In the menu bar, click **Administration** > **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role**.
3. In the Server Role page, fill-in the fields from the following sets:
    a. **Server Settings**
    b. **Configure Survivable Data**

    Note:
    If you are configuring server role for the main server, this set will not be displayed.

    c. **Configure Memory**
4. Click **Change** to apply the server role configuration.

Server Role field descriptions

Server Settings Field descriptions

Name	Description
This Server is	Specifies the role of the server. The possible server roles are: • **a main server:** Select this role if a primary server. • **an enterprise survivable server (ESS):** Select this role if a survivable core server. • **a local survivable server (LSP):** Select this role if a survivable remote server.
SID	Is the system ID. This ID must be the same for the main server and each survivable server. Avaya provides the system ID when you submit the Universal Install/SAL Product Registration Request form.
MID	Is the module ID. The main server module ID must be 1 and that of other servers must be unique and 2 or above. If a survivable remote server, the MID must match the Cluster ID/MID for that server.

Configure Survivable Data Field descriptions

Name	Description
Registration address at the main server (C-LAN or PE address)	Are the IP addresses of the Control LAN (C-LAN) or the Processor Ethernet (PE). These addresses are registered with the main server.
File Synchronization address at the main cluster (PE address)	Are the IP addresses of the NICs of the main server and the second redundant server connected to a LAN to which the Survivable Remote or the Survivable Core server is also connected. **Note:** If a second server is not used, do not fill in this field. The Survivable Remote or the Survivable Core server must be able to ping these addresses. Avaya recommends use of the enterprise LAN for file synchronization.
File Synchronization address at the alternate main cluster (PE address)	Is the IP address of the interface to be used as alternate file synchronization interface. Refer to the **File Synchronization address at the main cluster (PE Address)** field description for information on how to fill in this field.

Configure Memory Field descriptions

Name	Description
This Server's Memory Setting	Is this server's template-specific memory settings. Each template has a memory size value associated with it: Large Survivable, Medium Survivable, or Small Survivable. The choices vary depending on the template installed. The choice must be equal to or less than the memory setting for the main server.
Main Server's Memory Setting	Is the main server's template-specific memory settings. The choices are Large, Medium, or Small and vary depending on the template installed.

Button descriptions

Name	Description
Change	Updates the current values on the page with the corresponding values in the system database.
Restart CM	Updates the current values on the page with the corresponding values in the system database and restarts the Communication Manager virtual machine. **Note:** Click Restart CM only after configuring the complete settings of the server. Too many restarts may escalate to a full Communication Manager reboot.

Communication Manager network configuration

Network configuration

Use the Network Configuration page to configure the IP-related settings for the server.

Note:

Some of the changes made on the Network Configuration page may affect the settings on other pages under **Server Configuration**. Make sure that all the pages under **Server Configuration** have the appropriate configuration information.

The Network Configuration page enables you to configure or view the settings for the hostname, alias host name, DNS domain name, DNS search list, DNS IP addresses, server ID, and default gateway.

- If the configuration setting for a field is blank, you can configure that setting from the Network Configuration page.
- If the configuration setting for a field is already obtained from an external source, such as System Platform or Console Domain, that field is view-only.
- If you want to change the configuration setting obtained from an external source, you must navigate to the external source used to configure the setting.

You can also configure the IP-related settings for each Ethernet port to determine how each Ethernet port is to be used (functional assignment). Typically, an Ethernet port can be configured without a functional assignment. However, any Ethernet port intended for use with Communication Manager must be assigned the correct functional assignment. Make sure that the Ethernet port settings in the Network Configuration page match the physical connections to the Ethernet ports. However, the labels on the physical ports may be shifted by 1. For example, eth0 may be labeled as 1 and eth1 may be labeled 2 and so on. Ethernet ports may be used for multiple purposes, except for the services port. Currently, there is no services port within Communication Manager.

The Network Configuration page displays the network interfaces that will be used by Communication Manager. This will be eth0 for all Communication Manager templates except CM_Duplex. For CM_Duplex, the network interfaces will be eth0 and eth1.

To activate the new settings in the server, you must restart Communication Manager. Make sure that you restart Communication Manager only after configuring the complete settings of the server. Too many restarts may escalate to a full Communication Manager reboot.

Configuring the Communication Manager network

Prerequisites

Log in to Communication Manager System Management Interface on the server on which you want to configure the network.

For the Duplex Survivable Core template, additional fields appear for configuring Communication Manager for duplication. This enables Communication Manager to duplicate data on the second server.

1. In the menu bar, click **Administration** > **Server (Maintenance)**.
2. Click **Server Configuration** > **Network Configuration**.
3. Fill in all the fields.

4. Click **Change** to save the network configuration.
5. Click **Restart CM**.

   ✱ **Note:**

   If configuring for duplication, do not restart Communication Manager yet. Wait until after you configure the duplication parameters.

   It takes about 2 minutes to start and stabilize the Communication Manager processes. Additional time is required to start the port networks, the media gateway, and the phones, depending on your enterprise configuration.

Network Configuration field descriptions

Field descriptions

Name	Description
Host Name	Is the host name of the server and is aligned with the DNS name of the server. The name must be a fully qualified domain name (FQDN).
Alias Host Name	Is the alias host name for duplicated servers only. If the server is running in the survivable mode, make sure that you fill in this field.
DNS Domain	Is the domain name server (DNS) domain of the server.
Search Domain List	Is the DNS domain in the form of domain.com, for example. If more than one list, separate them with commas. Is the DNS domain name for the search list in the form of, for example, domain.com. If more than one search list name, separate them with commas.
Primary DNS	Is the primary DNS IP address.
Secondary DNS	Is the secondary DNS IP address. This field is optional.
Tertiary DNS	Is the tertiary DNS IP address. This field is optional.
Server ID	Is the unique server ID, which is a number between 1 and 256. If a duplicated server or survivable server, the number cannot be 1.
Default Gateway	Is the default gateway IP address.
IP Configuration	Is the set of parameters for configuring an Ethernet port. The parameters are: • IP Address • Subnet Mask • Alias IP Address (for duplicated servers only) • Functional Assignment. Choices are

Name	Description
	- Corporate LAN/Processor Ethernet/Control Network - Corporate LAN/Control Network - Duplication Link **Note:** You may configure as many Ethernet ports as available on the NICs of your server.

Button descriptions

Name	Description
Change	Updates the current values on the page with the corresponding values in the system database.
Restart CM	Updates the current values on the page with the corresponding values in the system database and restarts the Communication Manager virtual machine. **Note:** Click **Restart CM** only after configuring the complete settings of the server. Too many restarts may escalate to a full Communication Manager reboot.

Duplication parameters configuration

Duplication parameters

The Duplication Parameters page is available only when the Duplex Main/Survivable Core template is installed. Configuring duplication parameters ensures that your telephony applications run without interruption even as the primary server faces operational problem.

Duplicated Communication Manager servers are not the same thing as the System Platform High Availability Failover feature.

The duplication type setting must be the same for both servers. If you are changing the already configured duplication parameters, make sure that you do it in the following order:

1. Busy-out the standby server and change the settings.
2. Change the settings on the active server. This causes a service outage.
3. Release the standby server.

> **Important:**
> Changing the duplication parameters on the active server results in the standby server becoming the active server. Moreover, the new active server will not be available for call processing.

In the Duplication Parameters page, configure the following settings for the server:

- Duplication type for the servers: Communication Manager supports two server duplication types—software-based duplication and encrypted software-based duplication.
- Duplication parameters of the other server: Configure the hostname, server ID, Corporate LAN IP address and the duplication link IP address for the other server.
- Processor Ethernet parameters: Configure the Processor Ethernet interchange priority level for the server and the IP address that enables the server to determine whether its Processor Ethernet interface is working or not.

Configuring duplication parameters

Prerequisites

You must be logged into the Communication Manager System Management Interface.

1. In the menu bar, click **Administration** > **Server (Maintenance)**.
2. Click **Server Configuration** > **Duplication Parameters**.
3. Fill in all the fields for the server.
4. Click **Change**.
5. Click **Restart CM**.
   In the pop-up confirmation page, click **Restart Now** if you want to restart the server immediately. Click **Restart Later**, if you want to restart the server later.

Duplication Parameters field descriptions

Field descriptions

Name	Description
Select Server Duplication	Specifies the duplication method. The choices are: **This is a duplicated server using software-based duplication:** Software-based duplication provides memory synchronization between an active and a standby server by using a TCP/IP link.

Name	Description
	This is a duplicated server using encrypted software-based duplication: Encrypted software-based duplication provides memory synchronization between an active and a standby server by using AES 128 encryption.
Hostname	Is the host name of the other server.
Server ID	Is the unique server ID of the other server, which must be an integer between 1 and 256.
Corporate LAN/ PE IP	Is the IP address for the Corporate LAN/Processor Ethernet interface for the other server.
Duplication IP	Is the IP address of the duplication interface of the other server. This is typically 192.11.13.13 for the first server and 192.11.13.14 for the second server.
PE Interchange Priority	Is a simple relative priority as compared to IPSIs in configurations that use both Processor Ethernet and IPSIs. Select one of the following priority levels: • **HIGH:** Favors the server with the best PE state of health (SOH) when PE SOH is different between servers. • **EQUAL:** Counts the Processor Ethernet interface as an IPSI and favors the server with the best connectivity count. • **LOW:** Favors the server with the best IPSI connectivity when IPSI SOH is different between servers. • **IGNORE:** Does not consider the Processor Ethernet in server interchange decisions.
IP address for PE Health Check	Is the IP address that enables the server to determine whether its PE interface is working or not. **Note:** The network gateway router is the default address. However, the IP address of any other device on the network that will respond can be used.

Button descriptions

Name	Description
Change	Updates the current values on the page with the corresponding values in the system database. A dialog box appears with three buttons: **Restart Now**, **Restart Later**, and **Cancel**. **Note:** Click **Restart Now** only after configuring the complete settings of the server. Too many restarts may escalate to a full Communication Manager reboot.

Name	Description
Restart CM	Updates the current values on the page with the corresponding values in the system database and restarts the Communication Manager virtual machine. **Note:** Click **Restart CM** only after configuring the complete settings of the server. Too many restarts may escalate to a full Communication Manager reboot.

Chapter 7: Postinstallation administration, verification, and testing

Installation tests

You need to perform a number of postinstallation administration, verification, and testing tasks to ensure that the various system components are installed and configured as desired as part of Communication Manager installation.

This section provides a list of tasks for testing the template, server, and system component installation and configuration. Some tests cannot be performed until the complete solution is installed and configured, including port networks. See the *Installing and Configuring the Avaya Aura™ Communication Manager Solution*, 03–603559, book for the installation and configuration tasks.

Perform the following postinstallation administration and verification tasks:

- Reviewing the template state on the System Platform Web Console.
- Verifying the translations
- Clearing and resolving alarms
- Backing up the files.

The following tests can be done only after the port networks and UPS are installed and configured.

- Testing the IPSI circuit pack
- Testing the IPSI LEDs
- Testing the UPS LEDs.

Refer to the relevant server installation document for your server-specific postinstallation administration and verification tasks. Also refer to *LED Descriptions for Avaya Aura™ Communication Manager Hardware Components* for understanding the states that LEDs on different components of your system denote.

Reviewing the template state on System Platform Web Console

Avaya recommends performing this task to ensure the successful installation of your Communication Manager template.

1. Log in to the System Platform Web Console.
2. On the Virtual Machine List page, check that the **State** column shows **Running** for the Communication Manager template.
3. Log out from the System Platform Web Console.

Checking date and time settings

By checking date and time settings on System Platform Web Console, you will ensure that correct time zone has been setup on System Platform server. Also, if a network time processor has been setup, you will ensure that System Platform is able to ping the network time processor.

1. Log in to the System Platform Web Console.
2. Click **Server Management** > **Date / Time Configuration**.
3. Check that the **Local Time** and **UTC Time** fields show the correct time settings.
4. If network time processor IP address is present in the **Time Server** field, click **Ping** and check that the network time processor is pinged successfully.
5. Log out from the System Platform Web Console.

Verifying the license status

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address of the S8xxx Server in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.
3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon 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.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Viewing the license status

Prerequisites

You must be logged in to the System Management Interface (SMI).

Use this procedure to view the status of the license for Communication Manager and Communication Manager Messaging. The license can be installed and valid, unlicensed and within the 30-day grace period, or unlicensed and the 30-day grace period has expired. The License Status page also displays the System ID and Module ID.

1. In the menu bar, click **Administration** > **Licensing**.
2. In the navigation pane, click **License Status**.
   The License Status page displays the license mode and error information.

Related topics:

Accessing the System Management Interface on page 103
License Status field descriptions on page 105

License Status field descriptions

Name	Description
CommunicaMgr License Mode	Status of the license. Possible statuses are: • Normal: The Communication Manager license mode is normal and there are no license errors. • Error: The Communication Manager license has an error and the 30-day grace period is active. • No License: The Communication Manager license has an error and the 30-day grace period has expired. The Communication Manager software is running, but blocks normal call processing. The switch administration software remains active so you can correct license errors (for example, reducing the number of stations).
checking application CommunicaMgr version	Version of Avaya Aura® Communication Manager. For example, R016x.00.0.340.0.
WebLM server used for License	Displays the WebLM server URL used for the license. For example, `https://10.18.2.8:52233/WebLM/LicenseServer`.
Module ID	The Communication Manager main server has a default module ID of 1. You can configure the Module ID on the Server Role page. Each survivable server has a unique module ID of 2 or greater. The module ID must be unique for the main server and all survivable servers.
System ID	Communication Manager has a default system ID of 1. You can configure the System ID on the Server Role page. The system ID is common across the main server and all survivable servers. Avaya provides the system ID when you submit the Universal Install/SAL Product Registration Request form.

Related topics:

Viewing the license status on page 104

Verifying the software version

Prerequisites

You must be logged into the Communication Manager System Management Interface.

Since the system is running on a new software release, you must log in with the `craft` user ID. You cannot use the `dadmin` user ID.

1. In the menu bar, click **Administration** > **Server (Maintenance)**.
2. Click **Server** > **Software Version**.
3. Verify that the **CM Reports as:** field shows the correct software load.
4. In the menu bar, click **Log Off**.

Verifying survivable server registration

Prerequisites

You must be logged into a Communication Manager SAT session.

If you installed a Survivable Core or Survivable Remote template on the server, you want to verify that it has registered with the main server. This task could take several minutes to complete.

1. Enter **`list survivable-processor`** to open the Survivable Processor screen.
2. Verify that the **Reg** field is set to **y**, indicating that the survivable server has registered with the main server.
3. Verify that the **Translations Updated** field shows the current time and date, indicating that the translations have been pushed down to the survivable server.

Verifying the mode of the server

1. Under **Server (Maintenance)**, click **Server** > **Status Summary**.
2. Verify the **Mode** field:
   - `Active` on an active server.
   - `StandBy` on a standby server.
   - `BUSY OUT` on a server that is busied out.
3. To verify the process status, click **Server** > **Process Status**.
4. Under **Frequency**, click **Display Once**.
5. Click **View**.
6. Verify all operations are:
   - `Down` for dupmanager
   - `UP` all other operations

Chapter 8: Troubleshooting installation

Troubleshooting System Platform installation

Template DVD does not mount

The template DVD does not mount automatically.

Troubleshooting steps

1. Log in to the Console Domain as admin.
2. Type `su -`
3. Enter the root password.
4. Run the following commands:

   ```
   > ssh dom0.vsp /opt/avaya/vsp/template/scripts/udomAttachCd
   > mount /dev/xvde /cdrom/
   ```

System Platform installation problems

Troubleshooting steps

After completing installation of System Platform, you can perform this procedure to check for problems with the installation. For example, you might set an IP address for the System Domain or Console Domain that is already being used by another host.

Note:

The checking requires that both System Domain and Console Domain are installed as a part of System Platform installation. Console Domain is installed after System Domain and the availability of the login prompt for System Domain does not necessarily mean that Console Domain is installed. If the **`check_install`** command indicates a problem accessing Console Domain, wait for a couple minutes and type the command again.

If you are unable to access System Domain through an IP connection, try connecting to the System Platform server through the console or the services port.

1. Log in to System Domain (Domain-0) as root.
2. Type the command `check_install`.
   If the command finds no issues, it will display the following message: `cursory checks passed`. This message indicates that the System Platform installation checking has passed successfully.

Cannot ping Console Domain or access the Web Console

Troubleshooting steps

1. Log in to the System Domain (Domain-0) as `admin`.
2. Enter **`su -`** to log in as root.
3. At the prompt, type **`xm list`**.

   The **`xm list`** command shows information about the running virtual machines in a Linux screen.

   You should see two virtual machines running at this time: System Domain (shown as `Domain-0`) and Console Domain (shown as `udom` in **`xm list`**).

   A state of `r` indicates that the virtual machine is running. A state of `b` indicates that the virtual machine blocked.

   Note:
   The blocked state does not mean that there is a problem with the virtual machine. It only means that the virtual machine is currently not using any CPU time.

   Other possible virtual machine states are:

   - p: paused
   - s: shutdown
   - c: crashed

For more information on the information displayed, see the Linux manual page for the **`xm`** command.

4. On the Linux screen, type **`exit`** to log off as root. Type `exit` again to log off from System Domain (Domain-0).

Example

`xm list` output:

```
Name                                        ID   Mem VCPUs      State   Time(s)
Domain-0                                     0   512     2     r-----   60227.8
cm                                          17  1024     1     -b----   14898.2
utility_server                              18   512     1     -b----    1909.0
```

Troubleshooting Communication Manager installation

DVD does not read

Troubleshooting steps

The DVD may be corrupted or the DVD player may be failing.

Burn another DVD.

Service port not working

Troubleshooting steps

1. Recheck the connection process.
2. Ensure that web browser proxy is turned off.

System time drifts over a period of weeks

Troubleshooting steps

Use an NTP clock source through system platform to time sync.

Survivable server fails to sync with main server

Troubleshooting steps

1. Within the survivable remote server:
    a. Access the Communication Manager System Management Interface.
    b. In the navigation pane, click **Server Configuration** > **Server Role**.
    c. Verify that the **This Server is** field is set to a local survivable processor (LSP) and the other fields are filled out correctly.
2. Within the main server:
    a. Start a SAT session.
    b. Enter **`list survivable-processor`**.
    c. Verify that the following fields are set correctly:
        - Reg: **y**. If set to **n**, then the survivable remote server has not registered with the main server. You must reregister the survivable server.

- Act: **n**
- Translation Updated: Shows a timestamp.

Session Manager fails to completely install

When Session Manager is installed within the Survivable Remote template and after the initialization has been given 20 additional minutes to run, the Virtual Machine Manage page on the System Platform Web console should list the Session Manager state as Running. If not, follow these troubleshooting steps.

Troubleshooting steps

1. Log into the System Manager Web interface.
2. Under the **Services** column, select **Replication**.
3. Select the appropriate **Replica Group** for the Session Manager server.
4. Click on **View Replica Nodes**.
5. If the state of the Session Manager server is either stuck in **Starting** or is **Queued for Repair**, then
   a. Log into the CLI of the System Manager.
   b. Verify that the **/etc/hosts** file has the IP address and hostnames of itself, all the standalone Session Managers, and all the Session Managers on survivable remote servers.
   c. Log into the CLI of the Session Manager on the survivable remote server.
   d. Verify that the **/etc/hosts** file has the IP address and hostnames of itself and the System Manager
   e. Enter **`initDRS`**. The command should complete within 5 minutes. If it does not complete within that time, continue with the next step.
   f. Enter **`initTM`**. The command should complete within 5 minutes. If it does not complete within that time, continue with the next step.
   g. Enter **`SMnetSetup`**. Verify all the information and retype the Enrollment password.
6. On System Manager, check to see if the survivable remote Session Manager is now synchronized.

Appendix A: Installation worksheet for System Platform

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

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

System Domain Network Configuration

Field	Value	Notes
Hostname		This is the hostname for System Domain (Dom 0)
Primary DNS		
Secondary DNS		Optional
Static IP		The static IP address for the Ethernet interface that connects to the customer network.
Subnet mask	255.255.255.0 (default)	
Default gateway IP		This will be the default gateway for all the virtual machines, if you do not configure gateways for them.
VLAN		Is required only if an S8300D server is used for installing System Platform.

VSP Console Domain Network Configuration

Field	Value/requirement	Notes
Hostname		This is the hostname for Console Domain.
Static IP		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

Field	Value/requirement	Notes
		enter here must be a valid IP address. Further, the Console Domain must be on the same network as System Domain (Domain-0).

Date/Time and NTP setup

Field	Value/requirement	Notes
NTP Server 1		Use of NTP server is optional. However, Avaya recommends its use.
NTP Server 2		Optional
NTP Server 3		Optional

Passwords

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

Field	Value/requirement	Notes
root		
admin		
cust		
ldap		

Appendix B: Installation and configuration worksheets for Communication Manager

Communication Manager configuration worksheets

Installation Wizard screens

Use the following worksheets to gather information needed to fill in the fields when using the Installation Wizard as part of the template installation. The Installation Wizard is also used to create the Electronic Pre-installation Worksheet file. Fill out worksheets for each server being installed.

Network Settings fields

Field	Value	Note
Communication Manager virtual machine IP address		
Communication Manager virtual machine hostname		
Utility Server virtual machine IP address		If template includes Utility Services.
Utility Server virtual machine hostname		If template includes Utility Services.
Branch Session Manager virtual machine IP address		If template includes Branch Session Manager.
Branch Session Manager virtual machine hostname		If template includes Branch Session Manager. Must be a fully qualified domain name.

Customer Login fields

Field	Value	Note
Login name		For privileged administrator

Field	Value	Note
Password		For privileged administrator

DHCP fields

Gather data only if planning to use the internal DHCP server, which is only available if the template contains Utility Services.

Field	Value	Note
DHCP Network Address		
DHCP Subnet Mask		
DHCP Router IP address		
DHCP Pool IP address range		
DHCP DNS Server IP address		Optional
DHCP WINS Server IP address		Optional

Branch Session Manager fields

Field	Value	Note
DNS Search		Domain name
System Manager IP		
System Manager FQDN		
Trust Management Password		

Communication Manager System Management Interface screens

Use the following worksheets to gather information needed to fill in the fields when accessing various System Management Interface (SMI) screens. Fill out worksheets for each server being installed.

Server Role fields

Field	Value	Note
This server is		Specifies whether server will be a main, survivable core, or survivable remote server.
System ID		
Module ID		

If the server is a survivable server, additional data is needed

Field	Value	Note
Registration address at the main server (C-LAN or PE address)		
File Synchronization address at the main cluster (PE address)		
File Synchronization address at the alternate main cluster (PE address)		

Network Configuration fields

Field	Value	Note
Hostname		
Alias hostname		Required only for duplication.
DNS domain		
Search domain list		Domain name
Primary DNS		
Secondary DNS (Optional)		
Tertiary DNS (Optional)		
Server ID (between 1 and 256)		The main server is always 1
Default gateway		
IP address for IP configuration of eth0		
Subnet mask for IP configuration of eth0		
Alias IP address for eth0		Required only for duplication.
IP address for IP configuration of eth1		
Subnet mask for IP configuration of eth1		
Alias IP address for eth1		Required only for duplication.

Duplication Parameters fields

These parameters are needed only with duplicated servers and are for the second server.

Field	Value	Note
Hostname		
Server ID		Must be between 2 and 256. The main server is always 1; a duplicated server is generally 2.

Field	Value	Note
Corporate LAN/PE IP address		
Duplication IP		
IP address for PE health check		

Index