Implementing Avaya Aura® Communication Manager

Release 6.2
03-603558
Issue 3
December 2012

© 2012 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

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

Warranty

Avaya provides a limited warranty on 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 website: 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. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

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 you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "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.

License types

- Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, 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.
- Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.
- CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage

Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, 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

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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 and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya and Avaya Aura® are trademarks of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux is the registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 9
- Purpose 9
- Intended audience 9
- Technical Assistance 9
- Related resources 10
  - Documentation 10
  - Training 11
  - Avaya Mentor videos 11
- Support 11
- Warranty 12

Chapter 2: Communication Manager overview 13
- Communication Manager installation overview 13
- System Platform overview 14
- Communication Manager templates overview 17
- Checklist of hardware and software requirements 19
- What Avaya provides 22
- Checklist for Communication Manager installation 22
- Registering the system 26
- Registering for PLDS 27
- Downloading software from PLDS 28
- Verifying the downloaded ISO image 29
  - Verifying the ISO image on a Linux-based computer 29
  - Verifying the ISO image on a Windows-based computer 29
- Writing the downloaded software to DVD 30
  - DVD requirements 30
  - Writing the ISO image to DVD or CD 30
- Service Pack and Dot Release Guardian overview 31
  - Communication Manager license features 32
  - Viewing Support End Date 33
  - Viewing software Publication Date 34
  - Guardian Enforcement for Service Packs and Dot Releases 34
- Creating an EPW file 36

Chapter 3: Installing System Platform 39
- System Platform installation overview 39
  - System Platform servers 39
  - Installation process 39
  - Software installation 39
- Preinstallation tasks for System Platform 40
  - Server installation 40
  - Connecting your laptop to the server 41
- Installing System Platform software 43
  - Verifying the System Platform image on the DVD 43
  - Configuring network settings for System Domain (Domain-0) 44
  - Starting the installation 45

Selecting the type of keyboard.... 48
Verifying the System Platform server hardware.... 49
Configuring network settings for System Domain.... 50
System Domain Network Configuration field descriptions.... 52
Configuring network settings for Console Domain.... 53
System Platform Console Domain Network Configuration field descriptions.... 54
Installing the Services Virtual Machine.... 55
Configuring the time zone for the System Platform server.... 58
Configuring the date and time for the System Platform server.... 59
Configuring System Platform passwords.... 60
Passwords field descriptions.... 61
Checking network configuration.... 62
Verifying installation of System Platform.... 63
Accessing System Platform.... 64
Feature Pack installation.... 69
Managing pathces.... 69
Chapter 4: Installing the license file and authentication file.... 71
Installing the license file.... 71
License file for Communication Manager.... 71
PLDS.... 71
Duplicated server licensing.... 72
Accessing WebLM from the System Platform Web Console.... 72
Obtaining the WebLM host ID.... 73
Activating license entitlements in PLDS.... 73
Installing a license file using WebLM.... 75
Installing the authentication file.... 76
Authentication files for Communication Manager.... 76
Starting the AFS application.... 76
Creating an authentication file for a new system.... 77
Obtaining the AFID from System Platform Web console.... 78
Installing an authentication file.... 78
Chapter 5: Installing Communication Manager templates.... 81
Solution template.... 82
Configuring system settings for System Platform.... 82
System configuration field descriptions.... 82
Installing a solution template.... 84
Search Local and Remote Template field descriptions.... 87
Beginning installation of template.... 88
Template Details button descriptions.... 89
Template Installation button descriptions.... 89
EPW file.... 89
An EPW file.... 89
Selecting a template installation method.... 90
Select Template button descriptions.... 91
Installing Communication Manager using the Installation Wizard.... 91
Virtual machine details.... 91
New customer login.... 92

DHCP ... 93
Branch Session Manager ... 94
Reviewing summary information ... 95
Continuing the template installation ... 95
Verifying virtual machine installation ... 96
Confirming template network configuration ... 97
Managing patches ... 98
Patches ... 98
Downloading patches ... 99
Configuring a proxy ... 99
Patch installation ... 100
Removing patches ... 107
Search Local and Remote Patch field descriptions ... 114
Patch List field descriptions ... 116
Patch Detail field descriptions ... 117
Chapter 6: Configuring SAL Gateway on System Platform ... 119
SAL Gateway ... 119
Configuration prerequisites ... 120
Changing the Product ID for System Platform ... 121
System and browser requirements for accessing the Gateway user interface ... 122
Starting the SAL Gateway user interface ... 122
Configuring the SAL Gateway ... 123
Gateway Configuration field descriptions ... 124
Configuring a proxy server ... 125
Proxy server field and button descriptions ... 126
Configuring SAL Gateway communication with a Secure Access Concentrator Core Server ... 127
Core Server field descriptions ... 128
Configuring SAL Gateway communication with a Secure Access Concentrator Remote Server ... 129
Remote Server field descriptions ... 130
Configuring NMS ... 130
Network Management Systems field descriptions ... 131
Managing service control and status ... 131
Applying configuration changes ... 132
Adding a managed element ... 133
Managed Element field descriptions ... 133
Using a stand-alone SAL Gateway ... 135
Adding an SNMP trap receiver ... 135
Disabling SAL Gateway ... 136
Chapter 7: Configuration tasks for Communication Manager ... 137
Communication Manager configuration ... 137
Server role ... 137
Server role configuration ... 137
Configuring server role ... 138
Server Role field descriptions ... 139
Communication Manager network configuration ... 141
Network configuration ... 141
Configuring the Communication Manager network ... 142

Network Configuration field descriptions..... 142
Duplication parameters configuration..... 144
Duplication parameters..... 144
Configuring duplication parameters..... 145
Duplication Parameters field descriptions..... 145
Chapter 8: Postinstallation administration, verification, and testing..... 149
Installation tests..... 149
Reviewing the template state on System Platform Web Console..... 150
Checking date and time settings..... 150
Verifying the license status..... 151
Accessing the System Management Interface..... 151
Viewing the license status..... 152
License Status field descriptions..... 153
Verifying the software version..... 154
Verifying survivable server registration..... 154
Verifying the mode of the server..... 155
Chapter 9: Troubleshooting installation..... 157
Troubleshooting System Platform installation..... 157
Template DVD does not mount..... 157
System Platform installation problems..... 157
Cannot ping Console Domain or access the Web Console..... 158
Troubleshooting Communication Manager installation..... 159
DVD does not read..... 159
Service port not working..... 160
System time drifts over a period of weeks..... 160
Survivable server fails to sync with main server..... 160
Branch Session Manager fails to completely install..... 161
Appendix A: Installation worksheet for System Platform..... 163
Appendix B: Installation and configuration worksheets for Communication Manager 175
Communication Manager configuration worksheets..... 175
Appendix C: Managed element worksheet for SAL Gateway..... 179
Appendix D: PCN and PSN notifications..... 181
PCN and PSN notifications..... 181
Viewing PCNs and PSNs..... 181
Signing up for PCNs and PSNs..... 182
Index..... 183

Chapter 1: Introduction

Purpose

This document provides procedures to install Avaya Aura® System Platform, license and authentication files, and Avaya Aura® Communication Manager.

Intended audience

This document is intended for anyone who wants to install, configure, and verify Avaya Aura® Communication Manager. The audience includes and is not limited to implementation engineers, field technicians, business partners, and customers.

Technical Assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with feature administration and system applications, call the Avaya Technical Consulting and System Support (TC-SS) at 1-800-225-7585.

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Related resources

Documentation

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

Title	Description	Audience
Design		
Avaya Aura®Communication Manager System Capacities Table	Describes the system capacities for Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Implementation		
Installing and Configuring Avaya Aura® System Platform Release 6.2	Describes the installation instructions for Avaya Aura® System Platform.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Upgrading to Avaya Aura® Communication Manager Release 6.2, 03-603560.	Describes the Communication Managerupgrade instructions.	
Installing and Configuring Avaya WebLM Server	Describes the installation instructions for Avaya WebLM Server.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Secure Access Link 2.1 SAL Gateway Implementation	Describes the implementation instructions for SAL gateway.	Sales Engineers, Solution Architects, Implementation Engineers,

Title	Description	Audience
		Support Personnel
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation, 555-245-205	Describes the features that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Getting Started with Avaya PLDS	Describes Avaya PLDS.	Sales Engineers, Support Personnel

Training

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

Course code	Course title
ATI02348IEN, ATI02348VEN	Avaya Aura® Communication Manager Implementation
5U0041I	Avaya Aura® Communication Manager Administration

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit http://www.youtube.com/AvayaMentor and do one of the following:

- Enter a key word or key words in the Search channel to search for a specific product or topic.
- Click the name of a playlist to scroll through the posted videos.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release

notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

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

Chapter 2: Communication Manager overview

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

Communication Manager is the key component of Avaya Aura®. Communication Manager delivers rich voice and video capabilities and provides a resilient, distributed network for 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. Communication Manager includes advanced mobility features, built-in conference calling and contact center applications, and E911 capabilities.

Communication Manager aims to solve business challenges by powering voice communications and integrating with value-added applications. Communication Manager 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 provides 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
- 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 Avaya Aura® System Platform on the server
- Installing the appropriate Communication Manager template on the server
- Configuring the applications on the template, including Communication Manager, Communication Manager Messaging, and Branch Session Manager
- Completing the post installation verification tasks

If Communication Manager is not running as an application in your enterprise, perform the installation. You must also install Communication Manager if one or more of your current Communication Manager executable files are corrupted.

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

Note:

Communication Manager is installed on System Platform as a template.

You must upgrade Communication Manager when a new release is available. To start using the new release, shut down Communication Manager, replace the executable files with the new files, and restart Communication Manager.

For information about the upgrade process, see *Upgrading Servers to Avaya Aura® Communication Manager Templates*.

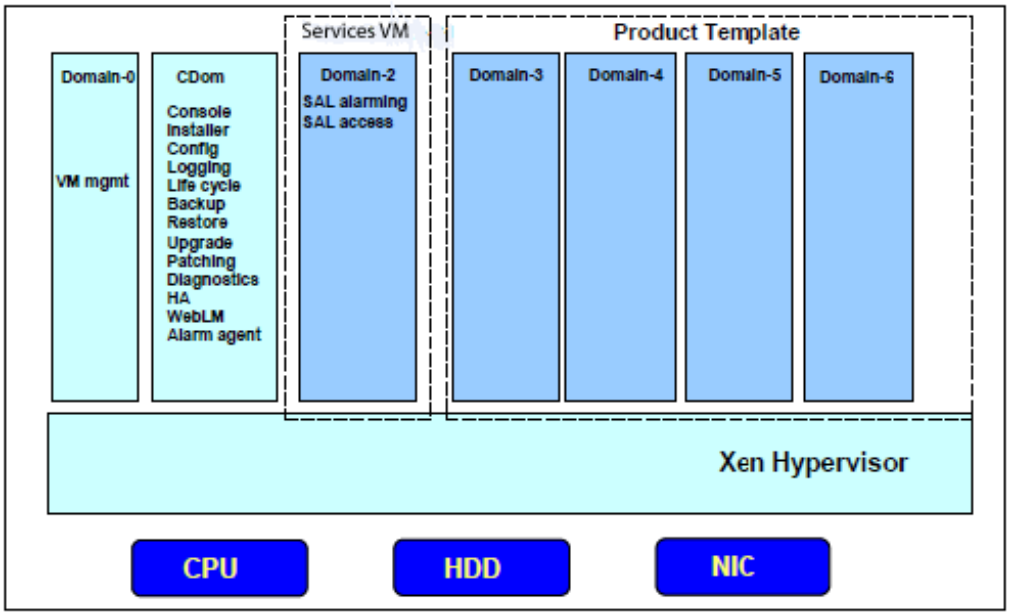
System Platform overview

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.

System Platform:

- is a software platform running CentOS plus Xen open source hypervisor for virtual machine monitoring and management
- hosts one or more Avaya products, each running on its own virtual server (virtual machine), all running on a single physical server platform
- provides a set of utilities commonly required for Avaya products, including installation, upgrade, backup/restore, licensing server, hardware monitoring and alarming, and remote access

The following figure shows an abstraction of the System Platform virtualized environment:



Avaya deploys System Platform through a *virtual appliance* model. The model includes:

- An Avaya-defined common server platform
- An Operating System (O/S) for allocating and managing server hardware resources (CPU, memory, disk storage, and network interfaces) among virtual machine instances running on the server platform
- System Platform
- An Avaya solution template containing a bundled suite of pre-integrated Avaya software applications
- A Secure Access Gateway, supporting a Secure Access Link (SAL) for remote diagnosis by Avaya or an Avaya Partner.

The advantages of System Platform include:

- Consolidation of servers
- Simpler maintenance
- Faster disaster recovery
- Easy installation of any Avaya Aura® solution template (bundled applications suite) on a single server platform
- Simpler and faster deployment of applications and solutions
- Efficient licensing of applications and solutions
- Security
- Portability of applications
- Reduction of operating costs

- Avaya common look-and-feel Web Console (Web Graphical User Interface) for server, virtual machine, application, and overall solution management.
- Remote access and automated alarm reporting for Network Management Systems monitored by Avaya Services and Avaya Partners personnel
- Coordinated backup and restore
- Coordinated software upgrades

Installation

Avaya provides an installation wizard program for System Platform software on Avaya-defined common server platforms.

Following System Platform installation, you install Avaya Aura® solution templates on the same server. Template installation significantly streamlines solution deployment across your organization. Installation wizard software installs a solution template in less time than if you installed multiple applications individually. The installation process is simple and requires only personnel with basic software installation skills. System Platform also supports remote installation of Avaya Aura® solution templates.

Solution templates

A solution template is a set of one or more Avaya applications pre-integrated for easy installation on System Platform. Installation personnel 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 enables 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 solution template software on a single server. Some solutions offer a server with System Platform and an Avaya Aura solution template pre-installed.

Networking

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 connects to a physical interface and serves as the default connection to your LAN. Most virtual machines have a virtual interface on the avpublic bridge to connect to your network. You can reach avpublic IP addresses by using PING over your network.

The avprivate bridge does not connect to any physical interface, but instead provides internal communication among the virtual machine instances running on a single server hardware platform. You cannot reach avprivate IP addresses by using PING over your network.

Some templates require additional connections to your network. In some cases, System Platform creates another software bridge for this purpose. This bridge contains the name

specified by the template, and the name is visible 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 that the virtual machine is assigned another physical NIC on the system and does not use avpublic. For example, in the Solution for Midsize Enterprise, Application Enablement Services uses eth3. See related solution template documentation for more information.

If a virtual machine in the installed template requires a dedicated NIC, it must have a separate cable connection to your network. Both the avpublic interface and the dedicated NIC must be connected to the network for those machines to communicate in the same way as if they were separate physical machines. For example, in the Solution for Midsize Enterprise, the Console Domain is on the avpublic bridge and Application Enablement Services has a dedicated NIC (eth 3). In this case you must connect eth0 and eth3 to the network before attempting to ping the Application Enablement Services virtual machine from the Console Domain.

Remote serviceability

Avaya or Avaya Partner support personnel can access and service System Platform from a remote location so that a site service call becomes unnecessary.

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

SAL uses your existing Internet connectivity to facilitate remote support. All communication outbound from your environment uses encapsulated Hypertext Transfer Protocol Secure (HTTPS). This is just one of many security features used by SAL to support secure remote access.

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

Important:

The SAL Gateway in the Services Virtual Machine or on a stand-alone server supports System Platform and Avaya Aura® solution templates. Avaya Partners and customers must register SAL, the solution template, and System Platform with Avaya during installation, and must configure SAL for remote support. Avaya support will be delayed or circumvented if SAL is improperly implemented or inoperative. System Platform and SAL do not support modem connections.

Communication Manager templates overview

Communication Manager as a template is a virtualized version that runs on System Platform. The Communication Manager template image has all the features that Communication Manager supports whether the image 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 Server. The templates support Communication Manager which configures as Main, Survivable Core Server, or Survivable Remote Server. In addition, you can use the network infrastructure of the templates 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
- Efficient licensing of applications and solutions
- Common look-and-feel Web Console (Web Graphical User Interface) for server, virtual machine, application, and overall solution management.
- Remote access and automated alarm reporting for Network Management Systems monitored by Avaya Services and Avaya Partners personnel
- Coordinated backup and restore
- Coordinated software upgrades

The Communication Manager templates come in two categories: The templates in each category are as follows:

- Communication Manager for Main/Survivable Core. This category contains the following templates:
  - Simplex CM Main/Survivable Core
  - Duplex CM Main/Survivable Core
  - Embedded CM Main
- Communication Manager for Survivable Remote. This 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:

You can gain access to Communication Manager Messaging only if you configure Communication Manager as the main server. You cannot gain access to

Communication Manager Messaging and Utility Services on Duplex Main/Survivable Core.

- Utility Services

You can install Simplex Main/Survivable Core and Duplex Main/Survivable Core templates on an S8510, S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server.

Note:

Avaya no longer sells the S8800 and S8510 Servers. You can only reuse the S8800 and S8510 Servers as an upgrade.

You can install the Simplex Main/Survivable Core template on an S8510 Server with a total 8-Gb memory as an upgrade only. You can install the Embedded Main template on an S8300D Server in a G250, G350, G430, G450, or G700 Branch 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

You can install the Simplex Survivable Remote on an S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server. You can install Simplex Survivable Remote on an S8510 Server with 8-Gb memory as an upgrade only. You can install Embedded Survivable Remote on S8300D Server in a G250, G350, G430, G450, or G700 Branch Gateway. You can use both the templates in the following two scenarios:

- Communication Manager Evolution Server
- Communication Manager Feature Server

Note:

For information on template capacities, see *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 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	

Requirement	Note	✔
	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	Needed if you are using a simplex core or survivable remote template. Needed 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	Needed if you are using an embedded main or embedded survivable remote template. For physical installation information, refer to the appropriate gateway quick start book.	
A laptop with an Ethernet crossover cable or, optionally, a USB keyboard, USB mouse, and VGA monitor	These are connected to the servers for installing System Platform and Communication Manager applications. You cannot use the keyboard, mouse, and monitor with the Avaya S8300 Server. **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	The application writes the software ISO images to the blank DVDs. Download the ISO images from the Product Licensing and Delivery System (PLDS) website, http://plds.avaya.com.	
Blank DVDs	The media for the ISO images.	
Bootable DVD, if available	Contains the System Platform and Communication Manager installer files.	
CAT5 Ethernet cable	Connects the servers to the enterprise network.	
Crossover Ethernet cable	Connects collocated duplicated servers.	

Requirement	Note	✔
Uninterruptible Power Supply (UPS)	Provides power during a power outage. You can order a UPS from Avaya.	
VPN SAL Gateway	Accesses the application servers. This is optional.	
Correct firewall rules to secure the customer network.		
Filled-out worksheets with the system and network information.	This information is 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 gateways, such as the Avaya G430 Branch Gateway or Avaya G450 Branch Gateway.
- Slide rails to mount the servers in a standard 19-inch, 4-post rack that have square holes.
- 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 the Avaya Support website at http://support.avaya.com. Click **More Resources** > **Avaya Equipment Registration**. Under **Non-Regional (Product) Specific Documentation**, click **Universal Install/SAL Product Registration Request Form**.

Checklist for Communication Manager installation

Use this checklist to ensure that you installed Communication Manager according to 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 submitthe 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.	**Important:** Submit the registration form three weeks before the planned installation date.	
2	Gather the required information relating to installation, such as IP configuration information, DNS addresses, and address information for Network Time Protocol (NTP) servers.		

#	Task	Note	✔
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 from PLDS on page 28.		
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 29 and Verifying the ISO image on a Windows-based computer on page 29.		
5	Write the ISO images to separate DVDs. See Writing the ISO image to DVD or CD on page 30.		
6	Install the Electronic Pre-installation Worksheet file and fill out the fields See Creating an EPW file on page 36		
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 41. • Disable use of proxy servers in the Web browser on the laptop. See Disabling proxy servers in Microsoft Internet Explorer on page 42 or Disabling proxy servers in Mozilla Firefox on page 42 .		
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 64. **Note:** If you are using an S8300D server, ensure that the gateway is on the latest firmware.		
9	Turn on the server.		

#	Task	Note	✔
10	Place the DVD in the DVD drive on the server. See Starting the installation from your laptop on page 46 or Starting the installation from the server console on page 48 depending on your selection of the 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 46 or Starting the installation from the server console on page 48 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 46.		
13	Select the required keyboard type. For detailed information, see the Selecting the type of keyboard section.		
14	Verify that the image on the System Platform DVD is not corrupt. See Verifying the System Platform image on the DVD on page 43.		
15	Configure the network settings for the System Domain (Domain-0). See Configuring network settings for System Domain on page 50.		
16	Configure the network settings for the Console Domain. See Configuring network settings for Console Domain on page 53.		
17	Configure System Platform to synchronize with an NTP server. See Configuring System Platform time to synchronize with an NTP server.		
18	Configure the System Platform passwords. See Configuring System Platform passwords on page 60.		
19	Verify that System Platform installed correctly. See Verifying installation of on page 63.		

#	Task	Note	✔
20	Configure the SAL gateway.		
21	If applicable, install Feature Pack 1 (FP1) for System Platform 6.2.1. See Feature Pack installation on page 69.		
22	Select the required Communication Manager template. See Installing a solution template on page 84.		
23	Confirm the template network configuration. See Confirming template network configuration on page 97.	Complete this step only if using an EPW file.	
If installing the template using the Installation Wizard instead of the EPW file, complete these additional tasks.			
24	Specify IP address and hostname for the Communication Manager virtual machine.		
25	Specify user ID and password for the privileged administrator. For more information, see Configuring Customer Login on page 92. **Note:** You may not need to add a privileged administrator for Communication Manager, but you may need it for BranchSession Manager.		
26	If the template includes Utility Services, configure DHCP. See Configuring DHCP on page 93.		
27	If the template includes Branch Session Manager, configure Branch Session Manager. See Installing Branch Session Manager on page 94.		
28	Review the summary information and check if you need to change any setting. See Reviewing summary information on page 95.		
29	Proceed with the Communication Manager installation. See Confirming installation on page 95.		

Registering the system

About this task

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

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

Note:

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

Registrations are performed in two stages: before installation of System Platform, the solution template, and SAL Gateway and after installation. The first stage of registration provides you with the SE IDs and Product Identifications required to install the products. For solution templates that include Communication Manager, the first stage of registration also provides you with the system ID (SID) and module ID (MID). The second stage of the registration makes alarming and remote access possible.

Procedure

1. Access the registration form and follow the instructions. This form is available at http://support.avaya.com. In the navigation pane, click **More Resources** > **Avaya 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*.
2. Complete the Universal Install Product Registration page and submit it at least three weeks before the planned installation date.

   Provide the following:

   - Customer name
   - Avaya Sold-to Number (customer number) where the products will be installed

- Contact information for the person to whom the registration information should be sent and whom Avaya can contact if any questions arise
- Products that are included in the solution template and supporting information as prompted by the form

Avaya uses this information to register your system. When processing of the registration request is complete, Avaya sends you an e-mail with an ART install script attached. This script includes instructions for installation and the SE IDs and Product IDs that you must enter in SAL Gateway to add managed devices. For solution templates that include Communication Manager, the ART install script also includes the SID and MID.

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

Related topics:

SAL Gateway on page 119
Configuration prerequisites on page 120
Gateway Configuration field descriptions on page 124

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) Web site at https://plds.avaya.com.
   The PLDS Web site redirects you to the Avaya single sign-on (SSO) Web page.
2. Log in to SSO with your SSO ID and password.
   The PLDS registration page is displayed.
3. If you are registering:
   - as an Avaya Partner, enter the Partner Link ID. If you do not know your Partner Link ID, send an 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 from PLDS

About this task

Note:

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

Procedure

1. Type `http://plds.avaya.com` in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads 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**
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click on the message, install Active X, and continue with the download.
9. When the system displays the security warning, click **Install**.

   When the installation is complete, PLDS displays the downloads again with a checkmark next to the downloads that are completed successfully.

Verifying the downloaded ISO image

Verifying the ISO image on a Linux-based computer

About this task

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

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

Procedure

1. Enter `md5sum 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

About this task

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

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

Procedure

1. Download a tool to compute md5 checksums from one of the following Web sites:
   - http://www.md5summer.org/
   - http://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. Use the content only as reference.

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

Writing the downloaded software to DVD

DVD requirements

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

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

Note:

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

Writing the ISO image to DVD or CD

Before you begin

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

About this task

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

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

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.

Procedure

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

Service Pack and Dot Release Guardian overview

Avaya Service Pack and Dot Release Guardian is patent pending technology that protects and controls the authorized use of Communication Manager Service packs and dot releases by inserting the Support End Date (SED) in the license file and comparing it to the Publication Date of the service pack or dot release. The application of service packs and dot release upgrades require Avaya support entitlements.

Using Avaya Service Pack and Dot Release Guardian technology, you can use a service pack or dot release if the Publication Date of the service pack or dot release is on or before the SED in the Communication Manager license file. Consider the following examples where the SED in the license file is 01 March 2013:

- Service Pack Guardian:
  - If the service pack Publication date is 01 March 2013 (or any earlier date), you can apply the service pack.
  - If the service pack Publication date is 02 March 2013 (or any later date), Communication Manager blocks the service pack installation.
- Dot Release Guardian:
  - If the Communication Manager software Publication Date is 01 March 2013 (or any earlier date), the Communication Manager software is allowed, and no license error displays.
  - If the Communication Manager software Publication Date is 02 March 2013 (or any later date), Communication Manager enters in license error mode with a 30-day grace period.

The SED is the expiration date for the support entitlements based on your Software Support (SSI), Software Support Plus Upgrades (SSU), Support Advantage (SA) or co-delivery support contract (for example, Joint Services Delivery (JSD) or Partner Support Services (PSS)). If you

have not purchased Avaya support coverage, the SED in the license file reflects a 90-day warranty period that starts when the license entitlements are first activated.

For more information about obtaining and installing the Communication Manager licenses, see Communication Manager license section in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555–245–205.

Communication Manager license features

A specific feature in the Communication Manager license file may enable or map to multiple features on the Customer Options form. For example, ASAI Features (FEAT_CM_ASAI_PCKG) in the license file enables multiple ASAI-related features on the Customer Options form, including ASAI Link Core Capabilities and ASAI Link Plus Capabilities. Unlicensed features are available to all customers and are excluded from the license file.

The following table summarizes the mapping of features in the Communication Manager license file to Customer Option features.

License feature	Communication Manager Customer Option features
Edition (VALUE_CM_EDITION)	`Standard` enables all unlicensed Customer Option features. `Enterprise` maps to the Multinational Locations Customer Option feature. Also enables all unlicensed Customer Option features.
Maximum Stations (VALUE_CM_STA)	Maps to multiple Customer Option features, notably Maximum Stations.
Maximum Analog Stations (VALUE_CM_ANALOG)	Specifies the number of analog stations to which the customer is entitled.
Maximum Survivable Processors (VALUE_CM_SP)	Maps directly to the Maximum Survivable Processors Customer Option feature.
Maximum ESS Stations (VALUE_CM_ESS_STA)	Specifies the number of Survivable Core station licenses to which the customer is entitled.
Maximum LSP Stations (VALUE_CM_LSP_STA)	Specifies the number of Survivable Remote station licenses to which the customer is entitled.
Maximum Mobility Enabled Stations (VALUE_CM_MOBILITY)	Maps to multiple Off-PBX Telephones Customer Option features.
Maximum Video Capable IP Softphones (VALUE_CM_VC_IPSP)	Maps to the Maximum Video Capable IP Softphones Customer Option feature.
ASAI Features (FEAT_CM_ASAI_PCKG)	Maps to ASAI-related Customer Option features including ASAI Link Core

License feature	Communication Manager Customer Option features
	Capabilities and ASAI Link Plus Capabilities.
Maximum Expanded Meet-Me Conference Ports (VALUE_CM_EMMC_PORTS)	Maps to the Maximum Number of Expanded Meet-Me Conference Ports Customer Option feature.
Access Security Gateway (FEAT_CM_ASG)	Maps to the Access Security Gateway Customer Option feature.
IP Endpoint Registration Features (for example, IP_Soft)	Map directly to Customer Option features of the same name, for example, IP_Soft.
Support End Date (VALUE_CM_SED)	Specifies the Support End Date (SED) used for Avaya Service Pack and Dot Release Guardian. If the Support End Date feature is available in the Communication Manager license file, the value is in DD-Month-YYYY format (for example, 01 June 2012). If the Support End Date feature is not available in the license file, Communication Manager does not perform the Support End Date validations. For more information, see the Service Pack and Dot Release Guardian overview section.

Viewing Support End Date

- You can view the SED for a Communication Manager server by accessing the associated WebLM server and viewing the Support End Date (VALUE_CM_SED) feature setting in the Communication Manager license file.
- You can view the SED in PLDS.
  - Select **Activation** > **View Activation Record**.
  - Search for the required record.
  - Click on the **License/Key** tab. Look for VALUE_CM_SED in the License/Key box for Communication Manager.
  - The SED is contained in the VALUE_CM_SED feature.

If there is no SED value in the license file then Communication Manager does not perform the SED or Publication Date check. However, you can install the Communication Manager software or apply the service pack.

Every 9 minutes, Communication Manager sends a request to WebLM to renew its license information. Because of this time interval, you may have to wait up to 9 minutes for a newly installed license file to take effect on Communication Manager.

Viewing software Publication Date

- You can view the software publication date on the PLDS download screen on top of the download description text.
- You can view the publication date of the installed Communication Manager software on the Software Version page of Server Management Interface (SMI).
- You can use the **`swversion`** command to view the publication date of the Communication Manager software in the **Publication Date** field.
- You can view the publication date of a service pack on the System Platform Console Domain. Select the **Server Management** > **Patch Management** menu.
  - If you have not downloaded the service pack, select the Download/Upload sub-menu option, and select the appropriate media to download the patch. When the service pack is successfully loaded, the details page displays the publication date.
  - If you have downloaded the service pack, select the Manage sub-menu option. Select the required service pack. The service pack details are displayed with the publication date. If the service pack **Publication Date** field is null on the patch details page, then Avaya Service Pack and Dot Release Guardian technology does not protect the service pack.

Note:

If the Communication Manager software or service pack does not contain a publication date then Avaya Service Pack and Dot Release Guardian technology does not protect the Communication Manager software and service packs.

Guardian Enforcement for Service Packs and Dot Releases

Guardian enforcement for Service Packs

Most services packs require support entitlements. Security patches do not require support entitlements. The services packs that require the support entitlement are licensed service packs. If the **License Required** field is set to yes in the ReadMe file then the service pack is the licensed service pack. You can view the **License Required** field on the System Platform Console Domain. When you apply a licensed service pack, the service pack publication date is checked against the SED in the Communication Manager license file.

If the service pack publication date is after the SED, Communication Manager blocks the service pack installation and System Platform Console Domain displays the following error message:

```
Command Failed: Service Pack publication date is after the Support
End Date in the license file.
```

If the service pack publication date is on or before the SED, the service pack is allowed and is installed on Communication Manager.

If the **License Required** field is set to yes in the ReadMe file but there is no SED value in the license file then Communication Manager does not perform the SED or Publication Date check. However, you can apply the service pack. Later, if you want to install the license file with a SED value and the SED is before the publication date, you cannot apply the service pack. Communication Manager blocks the service pack installation. Any previously installed service pack with a publication date after the SED in the newly installed license file will not cause license errors.

If the **License Required** field is set to no in the ReadMe file, the service pack is not a licensed service pack. A service pack that does not require a license does not have a publication date and no Guardian check of the SED is performed when service pack is applied.

For more information about managing and installing service packs on the System Platform Console Domain, see Managing patches section in *Implementing Avaya Aura® Communication Manager*.

Guardian enforcement for Dot Releases

If you are installing a dot release with a publication date that is not allowed by the SED in the license file, Communication Manager displays a license error, enters license error mode, and starts the 30-day license grace period. The system displays the following error message in the **Administration** > **Licensing** > **License Status** screen on the System Management Interface (SMI):

```
CommunicaMgr License Mode: License Error.
System Administration Will Be Blocked in Approximately 30 days.
Contact Your Service Representative Immediately.
Software Publication Date is After the Support End Date in License File.
```

To correct the license error:

- If you have an Avaya support contract, contact Avaya or business partner to regenerate and reinstall the license file to update the SED in the license file.
- If you do not have an Avaya support contract, you can purchase support coverage.
- If you do not want to purchase an Avaya support contract to allow the dot release, you need to go back to an earlier release of Communication Manager that is consistent with your support entitlements.

If the software publication date is on or before the SED, the software is allowed and is installed on Communication Manager without a license error.

If there is no SED value in the license file then Communication Manager does not perform the SED or Publication Date check. However, you can install the Communication Manager software. Later, if you install a license file with a SED value and the SED is before the publication date, Communication Manager enters in license error mode with a 30-day grace period.

License error mode

If Communication Manager detects an error with the licensing, for example, license file is not installed, feature usage exceeds license capacity, or software publication date is after the SED in the license file, the Communication Manager server enters in license error mode, raises a major alarm, and starts a 30-day license grace period. During the 30-day license grace period, Communication Manager provides full normal operations.

- If the license grace period expires before the license error is resolved, Communication Manager enters no license mode. In no license mode, Communication Manager continues to provide call processing. However, you cannot administer the system.
- If the license error is resolved either before or after expiration of the 30-day grace period, Communication Manager returns to license normal mode.

Creating an EPW file

Before you begin

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

About this task

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-based computer.

Procedure

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 91

Chapter 3: Installing System Platform

System Platform installation overview

System Platform servers

System Platform is installed on an Avaya S8300D, Avaya S8510, Avaya S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 server. The servers arrive at the customers 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 customers network.

Installation process

About this task

Installation of System Platform consists of the following tasks:

Procedure

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

   For more information about the System Platform installation, see *Installing and Configuring Avaya Aura® System Platform* Release 6.2.

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 an SSH and Telnet client application such as PuTTY installed on the laptop and Telnet must be enabled to install System Platform. Make sure that you change the network settings on the laptop before connecting to the server. See Configuring the laptop for direct connection to the server on page 41.

Use the provided worksheets and checklists during installation.

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

- For S8300D server with G700 Branch Gateway: *Quick Start for Hardware Installation: Avaya G700 Branch Gateway*
- For S8800 server: *Installing the Avaya S8800 Server for Avaya Aura® Communication Manager*

Connecting your laptop to the server

Configuring the laptop for direct connection to the server

About this task

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

Note:

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

Procedure

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

   Caution:

   Do not click the **Alternate Configuration** tab.
7. In the **IP address** field, enter a valid IP address.
   For example: `192.11.13.5`
8. In the **Subnet mask** field, enter a valid IP subnet mask.
   For example: 255.255.255.252
9. In the **Default gateway** field, enter the IP address that is assigned to the default gateway.
   For example: `192.11.13.6`

10. Click **OK**.

Disabling proxy servers in Microsoft Internet Explorer

About this task

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

Procedure

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

   Tip:

   To 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

About this task

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

Note:

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

Procedure

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

Tip:

To reenable the proxy server, select the appropriate option again.

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

Installing System Platform software

Verifying the System Platform image on the DVD

About this task

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.

Procedure

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

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

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

Note:

If the DVD you are using 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) on page 44.

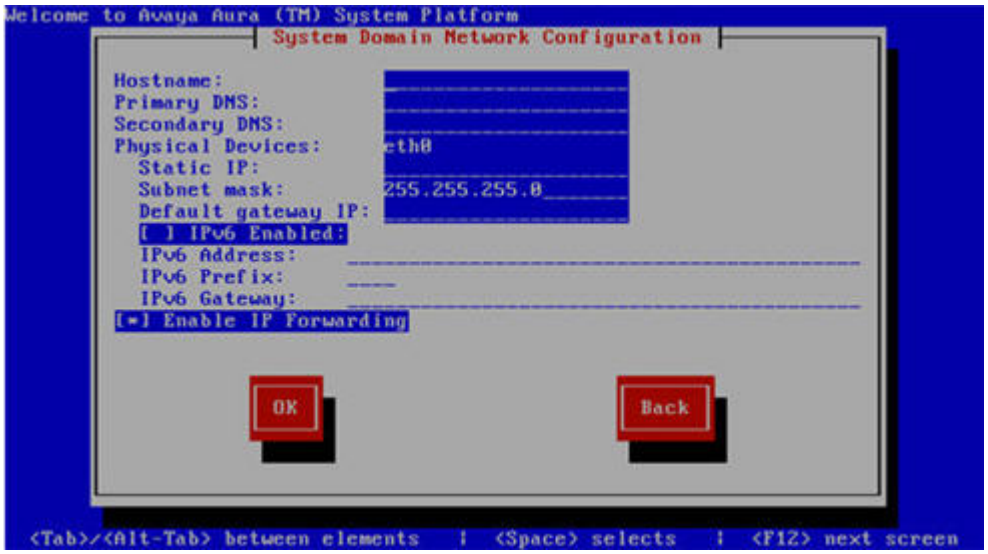
Configuring network settings for System Domain (Domain-0)

Procedure

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

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

   For descriptions of the fields on this page, see System Domain Network Configuration field descriptions.



2. Perform the following steps to configure the interface that is connected to the customer network:
   a. Use the `Tab` key to highlight the **Physical Devices** field.
   b. Complete the **Static IP** field.
   c. Modify the subnet mask if necessary. The server displays a default value of 255.255.255.0.
3. Complete the **Default gateway IP** field.

4. Use the Tab key to highlight the **IPv6 Enabled** field. Press the Spacebar to either enable or disable entering IP addresses in IPv6 format.
5. If you have enabled IPv6, fill in the following fields:
   - **IPv6 Address**
   - **IPv6 Prefix**
   - **IPv6 Gateway**
6. Use the Tab key to highlight the **Enable IP Forwarding** field. Press the Space bar to either enable or disable the IP forwarding as desired.

   Note:

   IP forwarding is enabled by default and is denoted by an asterisk (* character).
7. Use the Tab key to highlight **OK** and press **Enter** to accept the configuration.
8. If IP forwarding is enabled, a confirmation message is displayed. Use the Tab key to highlight **OK** and press **Enter**.
   The system displays the System Platform Console Domain Network Configuration screen.

Next steps

Configure network settings for Console Domain. See Configuring network settings for Console Domain on page 53.

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 an SSH and Telnet client application such as PuTTY installed on the laptop and Telnet must be enabled to install System Platform. Make sure that you change the network settings on the laptop before connecting to the server. See Configuring the laptop for direct connection to the server on page 41.

Powering on a server

Procedure

1. If using an S8800 Server or HP DL360 G7 Server or Dell R610 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.
   c. Insert the CD/DVD to the server.
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

Before you begin

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

Note:

On S8800 Server, HP DL360 G7 Server, and Dell R610 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'.

Procedure

1. Connect your laptop to the services port with an Ethernet crossover cable.
   If you do not have a crossover cable, use an IP hub.

Note:

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

2. Turn on the server.
3. Insert the System Platform DVD in the server DVD drive.
   The server boots from the DVD.
4. Verify that the laptop can ping the service port by performing the following steps:
   a. Click **Start** > **Run**.
   b. Enter **`ping`** `-t` *`IP_Address`*.

      Note:

      Wait for the `ping` command to return several continuous responses before proceeding to the next step.
5. Open a Telnet session by performing the following steps:

   Important:

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

   a. Open the PuTTY application.
   b. In the **Host Name** field, enter *Host_Name*.
   c. Under **Connection type**, select **Telnet**.
   d. Under **Window** in the left navigation pane, select **Translation**.
   e. Under **Received data assumed to be in which character set** , select **UTF-8** from the list.
   f. Click **Open** to open a PuTTY session.
      The system displays the Keyboard Type screen.

Next steps

Select the required keyboard type. See Selecting the type of keyboard on page 48.

Related topics:

Configuring the laptop for direct connection to the server on page 41
Powering on a server on page 46

Starting the installation from the server console

Note:

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

Before you begin

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

Procedure

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

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

   Important:

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

   The system displays the Keyboard Type screen.

Next steps

Select the required keyboard type. See Selecting the type of keyboard on page 48.

Related topics:

Powering on a server on page 46

Selecting the type of keyboard

Procedure

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

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

2. Use the `Tab` key to highlight **OK** and press **Enter**.
   The system displays one of the following screens:

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

     See Verifying the System Platform image on the DVD on page 43.

   - The system displays the System Domain Network Configuration screen if you are installing System Platform from the server console and did not enter the **`vspmediacheck`** command at the boot prompt on the Avaya screen. See Configuring network settings for System Domain (Domain-0) on page 44.

Next steps

- Verify that the System Platform image was copied correctly to the DVD. See Verifying the System Platform image on the DVD on page 43.

  OR

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

Verifying the System Platform server hardware

Before you begin

- You are performing a new installation of the System Platform software.
- You have just completed the task, Selecting the type of keyboard on page 48

About this task

After Selecting the type of keyboard on page 48, the System Platform installer automatically performs a hardware check of the server platform. Since the servers supported by Avaya must meet all prerequisites for the System Platform , any platform options, and a specific solution template, the server hardware check normally passes. In this case, the System Platform installation proceeds transparently to the next phase, Verifying the System Platform image on the DVD on page 43. However, in the rare circumstance when the hardware check halts the System Platform installation, one or both of the following messages appear. (In the following examples, the first number represents what hardware resources the system nominally requires, and the second number represents what hardware resources the server actually has available for the system.)

```
The installation is going to abort due to the following reasons:
  • The expected minimum size of hard disk is 80 GB, but the actual
    number of hard disk is 40 GB.
  • The expected number of hard disk is 2, but the actual number of
    hard disk is 1.
```

Or:

```
The installer has detected the following problems:
• The expected number of CPU(s) is 2, but the actual number of CPU(s)
  is 1.
Do you still want to continue the installation?
```

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

Note:

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

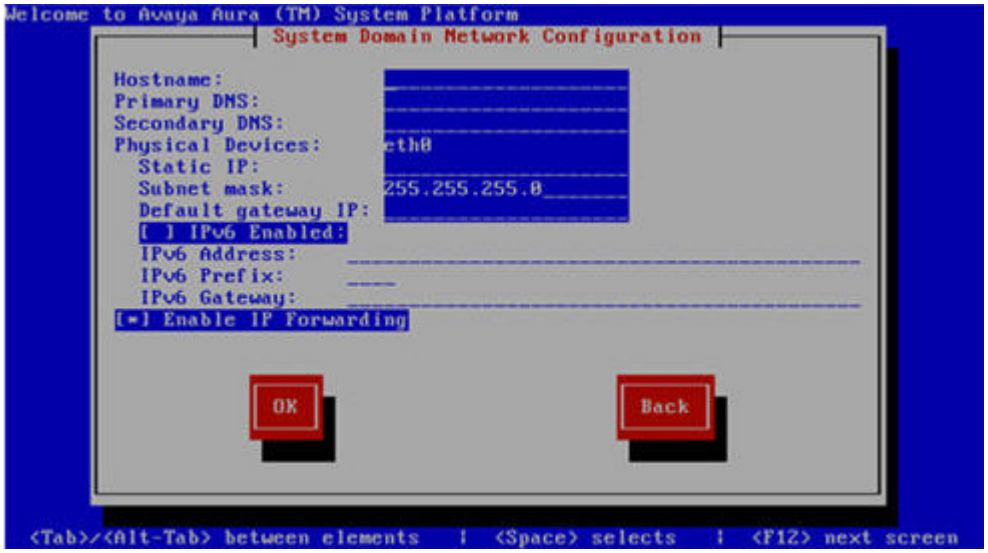
Next steps

If the server hardware check passed, continue with Verifying the System Platform image on the DVD on page 43

Configuring network settings for System Domain

Procedure

1. On the System Domain Network Configuration screen, complete the following fields:
   - **Hostname**
   - **Primary DNS**
   - (Optional) **Secondary DNS**



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 53.

System Domain Network Configuration field descriptions

Name	Description
Hostname	Depending on requirements of your solution template, you might need to enter the host name for System Domain as a fully qualified domain name (FQDN), for example, `SPDom0.mydomainname.com`. Otherwise, just enter the IP address for System Domain, or enter the hostname for System Domain in non-FQDN format. When using a Domain Name System (DNS) server in your network, the System Domain hostname must be FQDN format.
Primary DNS	The primary Domain Name System (DNS) server address.
Secondary DNS	(Optional) The secondary DNS server address.
Physical Devices	This field displays the physical Ethernet interface (NIC) that connects to the customer network. You must configure this interface for IP. 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.

Name	Description
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 gateway. **Note:** To get the ICC-VLAN configured on the gateway, login to the gateway command line interface and run the `show run` command.
IPv6 Enabled	The indicator to show whether the IP addresses required by System Platform must be IPv6-compliant.
IPv6 Address	The IPv6-compliant IP address of System Domain.
IPv6 Prefix	The IPv6 prefix for **IPv6 Address**.
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

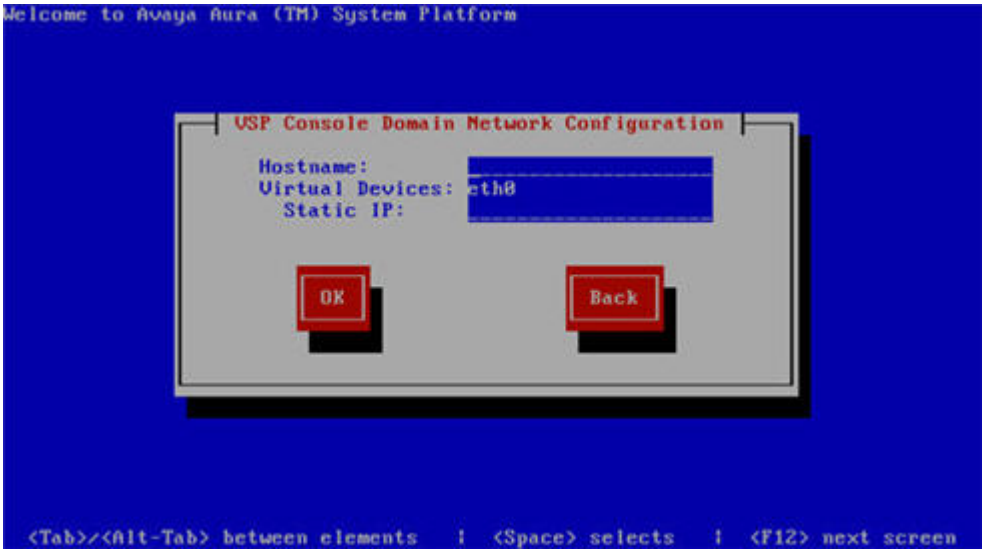
Procedure

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

   - **Hostname**.

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

- **Static IP**



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

Next steps

Install and configure the Services Virtual Machine. See Installing the Services Virtual Machine on page 55.

System Platform Console Domain Network Configuration field descriptions

Name	Description
Hostname	Depending on requirements of your solution template, you may need to enter the host name for Console Domain as a fully qualified domain name (FQDN), for example, `SPCdom.mydomainname.com`. Otherwise, just enter the IP address for Console Domain or enter the hostname for Console Domain in non-FQDN format.
Static IP	The IP address for the Console Domain. **Note:** The Console Domain does not have a physical interface. It has a virtual interface that uses the physical interface in System

Name	Description
	Domain (Domain-0). Because System Domain acts like a bridge, the IP address that you enter here must be a valid IP address. Further, the Console Domain must be on the same network as System Domain (Domain-0).
Virtual Devices	The virtual device (port) assigned to the Console Domain (Cdom) virtual machine. Default value (eth0) automatically assigned. No user input necessary.

Installing the Services Virtual Machine

Beginning with System Platform release 6.2, the Secure Access Link Gateway (SAL gateway) no longer runs on the System Platform Console Domain (cdom) virtual machine. Instead, SAL 2.1 runs on an independent Services Virtual Machine (services_vm domain) on your Avaya Aura® solution server. As with the prior implementation of the SAL gateway running on the cdom virtual machine, this new configuration supports secure remote access to local server resources, and forwards alarms (SNMP traps) from your local solution server to a remote Network Management System (NMS).

As of System Platform release 6.2, releases of the Services Virtual Machine are independent of System Platform releases, so your system may use the existing Services VM 1.0, or you can subsequently upgrade your system to use Services VM 1.1 (or later). When you upgrade the Services VM, the process preserves the prior Master Agent configuration. For information about how to upgrade the Services VM, see *Implementing and Administering Services-VM on Avaya Aura® System Platform*, which is available from Avaya Support (http://support.avaya.com). After the upgrade, you configure the Net-SNMP Master Agent in Services VM 1.1 (or later) to forward either SNMPv2c or SNMPv3 traps to your NMS.

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

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

For more information about SAL capabilities, see *Secure Access Link 2.1 SAL Gateway Implementation*, at http://support.avaya.com.

Before you begin

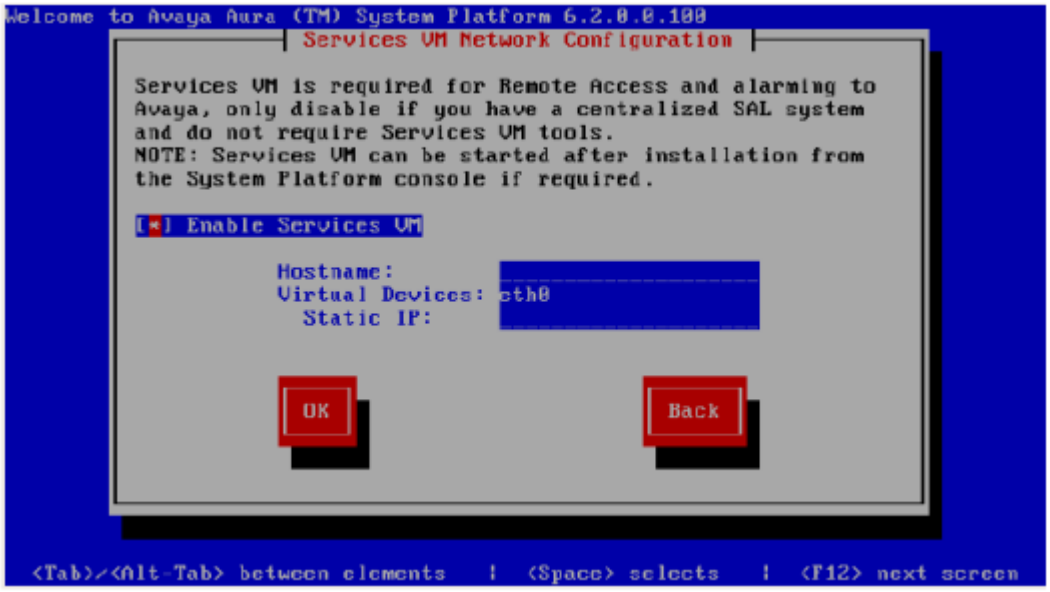
- You are performing a new installation of the System Platform.
- You have just completed the task, “Configuring network settings for Console Domain.”
- If you plan to deploy a stand-alone SAL gateway on a server elsewhere in your network, you must download, install, and configure the SAL 2.1 software on that server. For instructions, see the SAL gateway installation section of *Avaya Secure Access Link 2.1 Gateway Implementation*, available at the Avaya Support Web site at http://support.avaya.com.

About this task

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

Procedure

1. If you have a separate server dedicated for centralized SAL support, clear the **Enable Services VM** option in the Services VM Network Configuration window and click **OK**. Otherwise, leave the **Enable services VM** option enabled and begin with step 2 on page 56.
   If you disable the **Enable Services VM** option, System Platform installation automatically proceeds to “Configuring System Platform time to synchronize with an NTP server.”
2. In the Services VM Network Configuration window, enter a **Hostname** for the Services Virtual Machine.



3. Enter a **Static IP** address for the Services Virtual Machine.
   The IP address must be on the same subnet assigned to the Domain 0 (dom0) and Console Domain (cdom) virtual machines.

4. Click **OK**.
   System Platform installation proceeds to “Configuring System Platform to synchronize with an NTP server.”

Next steps

Configuring System Platform to synchronize with an NTP server.

Services VM Network Configuration field descriptions

Name	Description
Enable Services VM	Enables or disables remote access. Also supports local or centralized alarm reporting. Default value: **Enabled** Leave the **Enable services VM** option enabled (checkmark) for remote access and local SAL support, or disabled (no checkmark) if you have a separate server dedicated for independent/centralized remote access and SAL support.
Hostname	The name you assign to the Services Virtual Machine.
Static IP address	The IP address you assign to the Services Virtual Machine. The address must be on the same subnet assigned to the Domain 0 (dom0) and Console Domain (cdom) virtual machines.
Virtual devices	The virtual device (port) assigned to the Services Virtual Machine. Default value (eth0) automatically assigned. No user input necessary.

Select Services VM footprint size field descriptions

If you chose to leave Services VM support enabled while Installing the Services Virtual Machine on page 55, the Services VM installer opens the Selecting a Services VM footprint size window appears, prompting you to specify the size of Services VM required to support your Avaya Aura solution. Most Avaya Aura® solutions install a **Normal** size Services VM.

Note:

Do not specify the size of the Services VM footprint to be **Medium** or **Small** unless specified in your Avaya Aura® solution template requirements.

The Selecting a Services VM footprint size window also provides examples of resource consumption for each footprint size selection.

Name	Description
Services VM footprint size	The default value for **Services VM footprint size** is **Normal**. Specify only the exact footprint size required by the solution template you are deploying in your network. If you specify a footprint size larger than the template requires, the template may not install due to insufficient remaining server resources. This in turn may require you to reinstall the System Platform, this time specifying only the **Services VM footprint size** precisely required by the solution template. • **Normal**: Default Services VM footprint size for most templates. • **Medium**: Services VM footprint size required to support certain larger solution templates. • **Large**: Services VM footprint size required to support only the largest solution templates.

Configuring the time zone for the System Platform server

About this task

If you need to configure System Platform date and time settings manually instead of configuring the system to synchronize with a Network Time Protocol (NTP) server, you will first need to manually set the time zone in which the System Platform server resides.

Procedure

1. Click **Server Management** > **Date/Time Configuration**.
   The system displays the Date/Time Configuration page with default configuration settings.
2. Within the Select Time Zone panel, select a time zone and click **Save** at the bottom of the page.

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.

The system sets the selected time zone on the System Platform virtual machines (System Domain and Console Domain). The system also updates the time zone for other virtual machines running on the platform.

Note:

Clicking **Save** to make any change to the date or time configuration take effect will cause System Platform to reboot.

Next steps

Configure the date and time manually.

Configuring the date and time for the System Platform server

About this task

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

Procedure

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

   Note:

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

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

Before you begin

Configure the date and time for the System Platform server.

Procedure

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. 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:

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

For maximum password security, passwords for all users including `root` should conform to all of the following rules:

- Contain a minimum of 8 characters.

- Contain one or more lowercase characters.
- Contain one or more uppercase characters.
- Contain one or more digits.
- Contain one or more special characters.
- Must not be identical to any of the last 10 passwords.
- Must not be similar to the prior password. Passwords are similar when they share a sufficiently long common substring, where removal of that substring results in a weak new password.
- Must be changed within 90 days. At the end of this authorization interval, every user must change their password upon login to the Cdom (or Web Console) domain.

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 six 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:

For maximum password security, passwords for all users including `root` should conform to all of the following rules:

- Contain a minimum of 8 characters.
- Contain one or more lowercase characters.

- Contain one or more uppercase characters.
- Contain one or more digits.
- Contain one or more special characters.
- Must not be identical to any of the last 10 passwords.
- Must not be similar to the prior password. Passwords are similar when they share a sufficiently long common substring, where removal of that substring results in a weak new password.
- Must be changed within 90 days. At the end of this authorization interval, every user must change their password upon login to the Cdom (or Web Console) domain.

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

Procedure

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

Before you begin

To gain access to the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 65.

About this task

Important:

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

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

- The System Domain (Dom0) command line as `root`, and run the **`check_install`** command.
- The Console Domain (Cdom) Web Console as `admin`.
- The Console Domain as `cust`.

Note:

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

The actions in this procedure collectively help to verify successful installation of System Platform, and identify various issues associated with an unsuccessful installation, as well.

Procedure

1. Access the System Domain command line.
   See Accessing the command line for System Domain on page 67.
2. Enter the command, **`check_install`**.
   If **`check_install`** finds no issues, the following message appears in the command line interface:

   ```
   Cursory checks passed.
   ```

   If **`check_install`** command indicates a problem, wait a few minutes and run the command again. If the problem persists, contact Avaya using any of the technical support options at http://support.avaya.com.
3. Type **`exit`** to exit root login.
4. Type **`exit`** again to exit the System Domain.

5. Access the System Platform Web Console. See Accessing the Web Console on page 66.
6. Perform the following steps to log in to Console Domain as `admin`:
   a. Start PuTTY from your computer.
   b. In the **Host Name (or IP Address)** field, type the IP address of Console Domain.
   c. In the **Connection type** field, select **SSH**, and then click **Open**.
   d. When prompted, log in as `admin`, and type the password that you entered for the admin login during System Platform installation.
   e. Type `exit` to exit Console Domain.
7. 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 Avaya using any of the technical support options at http://support.avaya.com.

Accessing System Platform

Connecting to the server through the services port

Before you begin

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

Procedure

1. Connect your laptop to the services port with an Ethernet crossover cable.
   If you do not have a crossover cable, use an IP hub.

Note:

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

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

   The system assigns the IP address 192.11.13.6 to the services port.
4. For **Connection type**, select **SSH**.
5. In the **Port** field, type `22`.
6. Click **Open**.

   Note:

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

Enabling IP forwarding to access System Platform through the services port

About this task

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

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

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

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.

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 administrator.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 65.

About this task

Important:

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

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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

   Note:

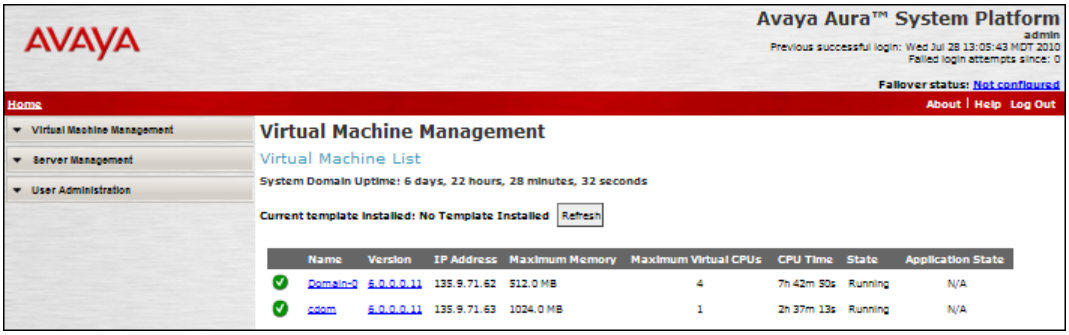
   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

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

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

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

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



Related topics:

Enabling IP forwarding to access System Platform through the services port on page 65

Accessing the command line for System Domain

About this task

If you have physical access to the system, you can log in to the system directly. When you connect to the services port, you are connected to System Domain. 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.

Note:

Administrators access the command line for System Domain to perform a very small number of tasks. Access to the command line for System Domain is normally reserved only for Avaya or Avaya Partners for troubleshooting purposes.

Procedure

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

   Tip:

   You can 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

About this task

Important:

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

Note:

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

Procedure

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

   Tip:

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

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

Feature Pack installation

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

RPM-based feature packs

For RPM-based feature packs (for example, FP1 for System Platform 6.2.1), proceed to Patch management on page 69.

ISO-based feature packs

For ISO-based feature packs (for example, FP2 for a future major or minor version of System Platform), perform a platform upgrade. (See relevant topics in your Avaya Aura® solution documentation.)

Managing pathces

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.

Feature packs

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

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

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

Guidelines for RPM-based feature packs

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

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

Guidelines for ISO-based feature packs

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

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

Feature Pack installation process

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

1. Upgrade System Platform from version 6.0 to version 6.2.1.
2. Install RPM-based Feature Pack 1 for System Platform 6.2.1. This step brings System Platform to version 6.2.2.
3. Upgrade Communication Manager from version 6.0 to version 6.2.
4. Install Service Pack 4 for Communication Manager 6.2.

Chapter 4: Installing the license file and authentication file

Installing the license file

License file for Communication Manager

Use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Communication Manager 6.0 and later, Collaboration Server, and Solution for Midsize Enterprise. 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 the license file. 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. The license file has the information regarding the product, major release, and license features and capacities.

For Communication Manager 6.0 and later, you must install license files on the Communication Manager main server and not on survivable servers. Survivable servers receive licensing information from the main server.

If you license a duplicated pair configuration, you must install the license file on both servers. The system does not synchronize the license file from active server to standby server.

A 30-day grace period applies to new installations or upgrades to Communication Manager 6.0, Collaboration Server, and Solution for Midsize Enterprise. 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 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, , and , 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 73
Activating license entitlements in PLDS on page 73

Duplicated server licensing

If you license a duplicated pair configuration, you must install the license file on both servers. The system does not synchronize the license file from active server to 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. The license file that the system generates includes both host IDs. You must install that license file on both servers in the duplicated pair.

Accessing WebLM from the System Platform Web Console

About this task

Procedure

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.

Obtaining the WebLM host ID

About this task

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.

Procedure

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 72

Activating license entitlements in PLDS

Before you begin

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

About this task

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

Procedure

1. Type `http://plds.avaya.com` in your Web browser to go to the Avaya PLDS website.

2. Enter your Login ID and password to log on to the PLDS 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 activates all license entitlements on the LAC. However, you can remove line items or specify a number of licenses to activate from the quantity available.
4. Enter the License Host information.

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

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

- 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 using WebLM

Before you begin

- Obtain the license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.
- If the currently installed license file is of greater capacity, you cannot install a new lower capacity license file using WebLM. You must first uninstall the higher capacity license file and then install the new lower capacity license file.

About this task

Important:

If you license a duplicated pair configuration, you must install the license file on both servers. The system does not synchronize the license file from active server to standby server.

Procedure

1. Start the WebLM Web interface and log in.
2. In the left navigation pane, click **Install license**.
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.

   For more information about installing and troubleshooting license file, see *Installing and Configuring Avaya WebLM Server*.

Related topics:

Accessing WebLM from the System Platform Web Console on page 72

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. With the ASG keys, Avaya Services can securely gain access to the customer system.

System Platform and Communication Manager share the same authentication file. The system installs a default authentication file with System Platform. However, you must replace the default file with a unique file. The Authentication File System (AFS) creates unique authentication files. AFS is an online application that you can download from 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 system automatically install the file on Communication Manager, Utility Server, and any other virtual machines on the server.

Every time you upgrade Communication Manager to a new major release, you must 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 system does not automatically synchronize the authentication file from active server to standby server.

Each survivable server must have its own unique authentication file. You must install a unique file 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 the file. 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

Before you begin

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.

About this task

Procedure

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

Creating an authentication file for a new system

About this task

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.

Procedure

1. Start and log in to AFS. See Starting the AFS application on page 76.
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 76

Obtaining the AFID from System Platform Web console

Procedure

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.

Installing an authentication file

Before you begin

You must create and download the authentication file from AFS.

About this task

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.

Procedure

1. Start the System Platform Web Console and log in.
2. Select **User Administration** > **Authentication File**.
3. Click **Upload**.
4. In the Choose File to Upload dialog box:
   a. Find and select the authentication file.
   b. 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:

   - must 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 must reinstall the original file

   Do *not* select this option if you are replacing the default authentication file with a unique authentication file.
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 from the System Management Interface (SMI) after the Communication Manager template has been installed.

Related topics:

Obtaining the AFID from System Platform Web console on page 78

Chapter 5: 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, Branch 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

Procedure

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 Internet proxy server settings, change the current keyboard language setting, configure WebLM server information, disable or reenable collection of System Platform statistics, disable or reenable autodiscovery of System Platform servers, and configure various elements of the installed solution template.

Note:

If an administrator modifies WebLM parameters in the System Configuration page, for example, to configure an alternate WebLM Server, then the Web console halts the local instance of WebLM. If the administrator clicks the License Manager menu option, the web console goes to the alternate instance of WebLM. If the administrator blanks out WebLM host and port values, the Web console recovers WebLM default values, resaves them, and then restarts the local instance of WebLM.

Refer to the Release Notes for more information about any known issues relating to WebLM behavior.

Proxy Configuration

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

Cdom Session Timeout

Name	Description
Session Timeout Status	Specifies whether Cdom session timeout is enabled or disabled.
Session Timeout (minutes)	The maximum amount of time in minutes that a Cdom session remains open since the last user transaction with the System Platform Web Console or the Cdom CLI.

WebLM Configuration

Name	Description
SSL	Specifies whether the Secure Sockets Layer (SSL) protocol will be used to invoke the WebLM server. Select **Yes** if the alternate WebLM application has an HTTPS web address. Otherwise, select **No** if the alternate WebLM application has an HTTP web address. Default value = **Yes**.
Host	The IP address or hostname extracted from the web address of the WebLM application. Default value = **<cdom_IP_address>**.
Port	The logical port number extracted from the web address of the WebLM application, for example, **4533**. Default value = **52233**

Other System Configuration

Name	Description
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.
SNMP Discovery	By default, this feature enables SNMPv2 management systems to automatically discover any System Platform server in the network, including retrieval of server status and vital statistics. This is useful, for example, when using System Manager to view the entire inventory of System Platform servers across multiple enterprise solutions at a glance. This feature eliminates the tedious and error-prone task of manually adding a large number of System Platform servers to an SNMP management system, where that system typically requires three or more IP addresses for each System Platform server instance. SNMP management

Name	Description
	systems can also query any recognized System Platform server for its logical configuration. System Platform supports network discovery of values for the following MIB objects: • RFC 1213 (MIB-2, autodiscovery): sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, and sysServices • RFC 2737 (Entity MIB) get/getnext/getbulk: entPhysicalTable: One table entry for the Dom0 physical interface. entLogicalTable: One table entry for the Cdom virtual machine, and one table entry for each virtual machine associated with the installed solution template. Each entry contains the virtual machine name, type, software version, and IP address. If you disable this option, SNMP manager systems will be unable to automatically discover this System Platform server.
Syslog IP Address	IP address of the Syslog server, which collects log messages generated by the System Platform operating system.

Installing a solution template

Before you begin

- Determine if you will be using an Electronic Pre-installation Worksheet (EPW) file to configure the solution template while installing it. You must create the EPW file before installing the template.
- Ensure that your browser option to block pop-up windows is disabled.

About this task

Important:

Some Avaya Aura solutions do not support template installation using all four of the possible file source options (PLDS, CD/DVD, USB, SP_Server). Refer to template installation topics in your Avaya Aura solution documentation to determine the correct option for installation of your 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.

Procedure

1. Log in to the System Platform Web Console as admin.
2. If installing from a USB flash drive, connect the flash drive to the server.
3. If installing from a single CD or DVD, insert the CD or DVD in the server CD or DVD drive.
4. If installing from multiple DVDs, copy the DVDs to the server:
   a. Click **Server Management** > **File Manager** in the navigation pane.
   b. Insert the first DVD.
   c. Click **View DVD/CD**.
   d. After the system mounts and reads the DVD, click **Copy Files**.
      The files are copied to the /vsp-template/cdrom directory on the server.
   e. When the system finishes copying the files, insert the second DVD.
   f. Click **View DVD/CD**.
   g. After the system mounts and reads the DVD, click **Copy Files**.
      The files are copied to the /vsp-template/cdrom directory on the server.
   h. Repeat for remaining DVDs
   i. After the system finishes copying the files, select the template in the **/vsp-template/** field of the **Copy from Server DVD/CD** area.
   j. Click **Finalize copy**.
      The files are copied to the template-specific directory that you selected in the previous step, and the cdrom directory is deleted.

   Important:

   If the writable DVD does not mount, write the ISO images to high quality DVDs and use a slower write speed.
5. Click **Virtual Machine Management** > **Templates** in the navigation pane.

   The system displays the Search Local and Remote Template page. Use this page to select the template to install on System Platform.
6. Click **Upgrade** next to the virtual machine that you want to upgrade, and then, in the **Install Template From** field, select the location of the software to be installed.

   If you copied multiple DVDs to the server, select **SP Server**.

Note:

If the software is located on a different server (for example, Avaya PLDS or HTTP), and depending on your specific network environment, configure a proxy if necessary to access the software. See Configuring a proxy on page 99.

7. If you selected **HTTP** or **SP Server** in the **Install Template From** field, enter the complete URL or path of the template files.
8. Click **Search** to display a list of template descriptor files (each available template has one template descriptor file).
9. On the Select Template page, click the 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.
10. Click **Install** to start the template installation.

Note:

System Platform automatically performs a hardware check of the server platform at this time. Servers supported by Avaya must meet all prerequisites for the System Platform, any platform options, and a specific solution template. If the server hardware check performed at this time passes, template installation proceeds normally. However, in a circumstance where the hardware check halts template installation, one or both of the following messages appear:

- Template Future Upgrade warning – `There is enough disk space to proceed with the current template installation/upgrade. However, there might not be enough disk space for a future template upgrade.`
- Insufficient disk space or memory resources message – `Insufficient resources to install this template (<template_name>).`

In either case, capture the exact details of the error message and go to the Avaya Support Web site at http://support.avaya.com/ for current documentation, product notices, knowledge articles related to the topic, or to open a service request.

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 according to the template you are installing. If you provided an EPW file, some of these pages typically contain 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.

Important:

If you are installing from a USB flash drive, remove the flash drive when the installation is complete. The presence of a flash drive connected to the server could prevent that server from rebooting.

Next steps

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

Related topics:

Configuring system settings for System Platform on page 82

Search Local and Remote Template field descriptions

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

Name	Description
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. 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**

Name	Description
	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. If necessary, configure a proxy for Secure Access Link (SAL) and alarming functions 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	Deletes the currently installed and active template. This button is displayed only if a template is installed on System Platform.

Beginning installation of template

Procedure

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 displays 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	✔	✔	✔	✔	✔
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

Before you begin

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.

About this task

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.

Procedure

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.
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

Procedure

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

About this task

The login created here is for the privileged administrator.

Procedure

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

About this task

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.

Procedure

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.

Name	Description
	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 Branch Session Manager

About this task

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

Procedure

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.

Name	Description
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

Procedure

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

About this task

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.

Procedure

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` displays 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

Before you begin

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

About this task

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.

Procedure

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

Before you begin

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

About 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.

Procedure

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

Patches

A patch provides critical security, performance, and stability fixes or updates. A service pack is a bundle of updates, fixes, enhancements, and previously released patches.

When a service pack is available on the Avaya support Web site, the supporting information clearly states the issues addressed in the service pack. You must implement the service packs even if you are not facing any problems. This will help keep the systems up to date and minimize the likelihood of any future impact from known issues.

Note:

Some patches might be service affecting and can require a Communication Manager reboot. Please see Product Correction Notice (PCN) or individual release notes to check for service affecting patches.

You can view the Product Correction Notice (PCN) and Release Notes for the latest patches, go to http://support.avaya.com and perform the Viewing the PCN and Release Notes from the Support site on page 98 procedure.

Viewing the PCN and Release Notes from the Support site

Procedure

1. Select **Downloads**.
2. Select “A” from the “A-Z” list.
3. SelectAvaya Aura® Communication Manager.
4. Select **Downloads**.
5. Select **Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates**.
6. Select the link for the Software Update, Service Pack, or Patch.
7. Select the link for the PCN or for the Release Notes specific to the patch.

Downloading patches

Procedure

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

Configuring a proxy

About this task

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

Procedure

1. Click **Virtual Machine Management** > **Templates**.
2. On the Search Local and Remote Template page, click **Configure Proxy**.
3. On the System Configuration page, select **Enabled** for the **Proxy Status** field.

4. Specify the proxy address.
5. Specify the proxy port.
6. Select the appropriate keyboard layout.
7. Enable or disable statistics collection.
8. Click **Save** to save the settings and configure the proxy.

Patch installation

You can install the following patches on Communication Manager:

- Security
- Kernel
- Regular

Important:

Perform a system backup before applying a patch. When you install the latest patch, the installation program automatically uninstalls the previous patch. So when you remove a patch, the system is not reverted to the state it was in before the patch was installed. You must re-install the previous patch to revert the system to the state it was in before the patch was installed.

You can download the patches to your local computer, or to System Platform from the Avaya Product Licensing and Delivery System (PLDS) Web site at http://plds.avaya.com.

Installing Kernel patch on simplex configuration

About this task

Note:

The Communication Manager server configuration can be observed on the System Platform Console Domain Web interface. To view the server configuration, see **Virtual Machine Management** > **Manage Web page**. If the **Current template installed** field is CM_Simplex, CM_onlyEmbed, CM_SurvRemote, or CM_SurvRemoteEmbed, the Communication Manager server configuration is considered to be simplex.

Procedure

1. To save the translations file, log on to Communication Manager and run the save translation SAT command.
2. Gain access to System Platform Console Domain (cdom).

3. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
4. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.
5. Download the patch.

   When the patch is successfully downloaded, the system displays the Patch Detail page.
6. Click **Install**.
7. Click **Commit**.

   The Kernel patch installation is complete.

Installing Regular patch on simplex configuration

About this task

Note:

The Communication Manager server configuration can be observed on the System Platform Console Domain Web interface. To view the server configuration, see **Virtual Machine Management** > **Manage Web page**. If the **Current template installed** field is CM_Simplex, CM_onlyEmbed, CM_SurvRemote, or CM_SurvRemoteEmbed, the Communication Manager server configuration is considered to be simplex.

Procedure

1. To save the translations file, log on to Communication Manager and run the save translation SAT command.
2. Gain access to System Platform Console Domain (cdom).
3. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
4. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.
5. Download the patch.

   When the patch is successfully downloaded, the system displays the Patch Detail page.
6. Click **Install**.

   The Regular patch installation is complete.

Installing Security patch on simplex configuration

About this task

Note:

The Communication Manager server configuration can be observed on the System Platform Console Domain Web interface. To view the server configuration, see **Virtual Machine Management** > **Manage Web page**. If the **Current template installed** field is CM_Simplex, CM_onlyEmbed, CM_SurvRemote, or CM_SurvRemoteEmbed, the Communication Manager server configuration is considered to be simplex.

Procedure

1. To save the translations file, log on to Communication Manager and run the save translation SAT command.
2. Gain access to System Platform Console Domain (cdom).
3. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
4. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.
5. Download the patch.

   When the patch is successfully downloaded, the system displays the Patch Detail page.
6. Click **Install**.

   The Security patch installation is complete.

Installing Kernel patch on duplex configuration

About this task

Note:

Communication Manager server configuration can be observed on the System Platform Console Domain Web interface. To view the server configuration, see **Virtual Machine Management** > **Manage Web** page. If the **Current template installed** field is CM_Duplex, the Communication Manager server configuration is considered to be duplex

Procedure

1. Log on to Communication Manager and determine which server is the active server.

2. To save the translations file, log on to the Communication Manager associated with the active server and run the save translation SAT command.
3. Log on to cdom of the standby server.
4. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
5. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.
6. Download the patch.

   When the patch is successfully downloaded, the system displays the Patch Detail page.
7. Click **Install**.
8. Click **Commit**.
9. Log on to Communication Manager and wait for the standby server to refresh.
10. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes`.
11. To switch the servers, run the `server –if` CLI command or use the Interchange Servers page of SMI.
12. Wait for the servers to interchange and the system to restart.
13. Log on to cdom of the new standby Communication Manager server.
14. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
15. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.
16. Download the patch.

    When the patch is successfully downloaded, the system displays the Patch Detail page.
17. Click **Install**.
18. Click **Commit**.
19. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes`.

    The Kernel patch installation is complete.

Installing Regular patch on duplex configuration

About this task

Note:

Communication Manager server configuration can be observed on the System Platform Console Domain Web interface. To view the server configuration, see **Virtual Machine Management** > **Manage Web** page. If the **Current template installed** field is CM_Duplex, the Communication Manager server configuration is considered to be duplex

Procedure

1. Log on to Communication Manager and determine which server is the active server.
2. Log on to SMI of the active server.
3. On the **Administration** tab, select **Server (Maintenance)**.
4. In the left navigation pane of the SMI page, click **Server Upgrades** > **Pre Update/ Upgrade Step**.
5. Click **Continue**.
6. Log on to cdom of the standby server.
7. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
8. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.
9. Download the patch.

   When the patch is successfully downloaded, the system displays the Patch Detail page.
10. Click **Install**.
11. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes (for Update/Upgrade)`.
12. To switch the servers, run the `server –if` CLI command or use the Interchange Servers page of SMI.
13. Wait for the servers to interchange and the system to restart.
14. Log on to cdom of the new standby Communication Manager server.
15. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
16. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.

17. Download the patch.

    When the patch is successfully downloaded, the system displays the Patch Detail page.

18. Click **Install**.

19. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes`.

    The Regular patch installation is complete.

Installing Security patch on duplex configuration

About this task

Note:

Communication Manager server configuration can be observed on the System Platform Console Domain Web interface. To view the server configuration, see **Virtual Machine Management** > **Manage Web** page. If the **Current template installed** field is CM_Duplex, the Communication Manager server configuration is considered to be duplex

Procedure

1. Log on to Communication Manager and determine which server is the active server.
2. To save the translations file, log on to the Communication Manager associated with the active server and run the save translation SAT command.
3. Log on to cdom of the standby server.
4. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
5. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.
6. Download the patch.

   When the patch is successfully downloaded, the system displays the Patch Detail page.

7. Click **Install**.
8. Log on to Communication Manager and wait for the standby server to refresh.
9. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes`.
10. To switch the servers, run the `server –if` CLI command or use the Interchange Servers page of SMI.

11. Wait for the servers to interchange and the system to restart.
12. Log on to cdom of the new standby Communication Manager server.
13. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
14. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.
15. Download the patch.

    When the patch is successfully downloaded, the system displays the Patch Detail page.
16. Click **Install**.
17. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes`.

    The Security patch installation is complete.

Installing Kernel patch on high availability configuration

Procedure

1. To save the translations file, log on to Communication Manager associated with the Primary/Active server and run the save translation SAT command.
2. Log on to cdom associated with the Primary/Active server.
3. In the left navigation pane of the Home page, click **Main** > **Server Management** > **High Availability**.
4. Click **Stop HA**.
5. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
6. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.
7. Download the patch.

   When the patch is successfully downloaded, the system displays the Patch Detail page.
8. Click **Install**.
9. Click **Commit**.
10. Click **Main** > **Server Management** > **High Availability**.
11. Click **Start HA**.

Installing Security patch on high availability configuration

Procedure

1. To save the translations file, log on to Communication Manager associated with the Primary/Active server and run the save translation SAT command.
2. Log on to cdom associated with the Primary/Active server.
3. In the left navigation pane of the Home page, click **Main** > **Server Management** > **High Availability**.
4. Click **Stop HA**.
5. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
6. In the left navigation pane of the Home page, click **Server Management** > **Patch Management** > **Download/Upload**.
7. Download the patch.

   When the patch is successfully downloaded, the system displays the Patch Detail page.
8. Click **Install**.
9. Click **Main** > **Server Management** > **High Availability**.
10. Click **Start HA**.

Removing patches

Removing Kernel patch when the status of the patch is installed

Procedure

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

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on the patch that you want to remove.
4. Click **Remove**.

Removing Regular patch when the status of the patch is installed

Procedure

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

Removing Security patch when the status of the patch is installed

Procedure

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

Removing Kernel patch when the status of the patch is active on simplex configuration

Procedure

1. To save the translations file, log on to Communication Manager and run the save translation SAT command.
2. Gain access to System Platform Console Domain (cdom).
3. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
4. In the left navigation pane of the Home page, click **Server Management** > **Patch Management**.
5. Click **Manage**.

6. On the Patch List page, click on the patch that you want to remove.
7. Click **Remove**.
8. Click **Commit**.

Removing Regular patch when the status of the patch is active on simplex configuration

Procedure

1. To save the translations file, log on to Communication Manager and run the save translation SAT command.
2. Gain access to System Platform Console Domain (cdom).
3. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
4. In the left navigation pane of the Home page, click **Server Management** > **Patch Management**.
5. Click **Manage**.
6. On the Patch List page, click on the patch that you want to remove.
7. Click **Remove**.

Removing Security patch when the status of the patch is active on simplex configuration

Procedure

1. To save the translations file, log on to Communication Manager and run the save translation SAT command.
2. Gain access to System Platform Console Domain (cdom).
3. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
4. In the left navigation pane of the Home page, click **Server Management** > **Patch Management**.
5. Click **Manage**.
6. On the Patch List page, click on the patch that you want to remove.

7. Click **Remove**.

Removing Kernel patch when the status of the patch is active on duplex configuration

Procedure

1. Log on to Communication Manager and determine which server is the active server.
2. To save the translations file, log on to the Communication Manager associated with the active server and run the save translation SAT command.
3. Log on to cdom of the standby server.
4. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
5. Click **Server Management** > **Patch Management**.
6. Click **Manage**.
7. On the Patch List page, click on the patch that you want to remove.
8. Click **Remove**.
9. Click **Commit**.
10. Log on to Communication Manager and wait for the standby server to refresh.
11. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes`.
12. To switch the servers, run the `server –if` CLI command or use the Interchange Servers page of SMI.
13. Wait for the servers to interchange and the system to restart.
14. Log on to cdom of the new standby Communication Manager server.
15. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
16. Click **Server Management** > **Patch Management**.
17. Click **Manage**.
18. On the Patch List page, click on the patch that you want to remove.
19. Click **Remove**.
20. Click **Commit**.

21. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes`.

Removing Regular patch when the status of the patch is active on duplex configuration

Procedure

1. Log on to Communication Manager and determine which server is the active server.
2. Go to Communication Manager SMI of the active server.
3. Click **Administration** > **Server Maintenance** > **Server Upgrades** > **Pre Update/ Upgrade**.
4. Click **Continue**.
5. Log on to cdom of the standby server.
6. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
7. Click **Server Management** > **Patch Management**.
8. Click **Manage**.
9. On the Patch List page, click on the patch that you want to remove.
10. Click **Remove**.
11. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes (for Update/Upgrade)`.
12. To switch the servers, run the `server –if` CLI command or use the Interchange Servers page of SMI.
13. Wait for the servers to interchange and the system to restart.
14. Log on to cdom of the new standby Communication Manager server.
15. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
16. Click **Server Management** > **Patch Management**.
17. Click **Manage**.
18. On the Patch List page, click on the patch that you want to remove.
19. Click **Remove**.

20. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes`.

Removing Security patch when the status of the patch is active on duplex configuration

Procedure

1. Log on to Communication Manager and determine which server is the active server.
2. To save the translations file, log on to the Communication Manager associated with the active server and run the save translation SAT command.
3. Log on to cdom of the standby server.
4. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
5. Click **Server Management** > **Patch Management**.
6. Click **Manage**.
7. On the Patch List page, click on the patch that you want to remove.
8. Click **Remove**.
9. Log on to Communication Manager and wait for the standby server to refresh.
10. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes`.
11. To switch the servers, run the `server –if` CLI command or use the Interchange Servers page of SMI.
12. Wait for the servers to interchange and the system to restart.
13. Log on to cdom of the new standby Communication Manager server.
14. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
15. Click **Server Management** > **Patch Management**.
16. Click **Manage**.
17. On the Patch List page, click on the patch that you want to remove.
18. Click **Remove**.
19. Run the `server` CLI command or check the Status Summary page of SMI to see if the **Standby Refreshed** field displays `yes`.

Removing Kernel patch when the status of the patch is active on high availability configuration

Procedure

1. To save the translations file, log on to Communication Manager associated with the Primary/Active server and run the save translation SAT command.
2. Log on to CDOM associated with the Primary/Active server.
3. In the left navigation pane of the Home page, click **Main** > **Server Management** > **High Availability**.
4. Click **Stop HA**.
5. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
6. Click **Server Management** > **Patch Management**.
7. Click **Manage**.
8. On the Patch List page, click on the patch that you want to remove.
9. Click **Remove**.
10. Click **Commit**.

Removing Security patch when the status of the patch is active on high availability configuration

Procedure

1. To save the translations file, log on to Communication Manager associated with the Primary/Active server and run the save translation SAT command.
2. Log on to cdom associated with the Primary/Active server.
3. In the left navigation pane of the Home page, click **Main** > **Server Management** > **High Availability**.
4. Click **Stop HA**.
5. In the left navigation pane of the Home page, click **Server Management** > **Backup/ Restore** > **Backup**.
6. Click **Server Management** > **Patch Management**.
7. Click **Manage**.
8. On the Patch List page, click on the patch that you want to remove.

9. Click **Remove**.

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. 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:** To move files from your laptop to the System Platform Server, some errors can occur because System Domain (Domain-0) and Console Domain support only SCP, but most laptops do not come with SCP support. You can download the following two programs to

Name	Description
	enable SCP (Search 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 Device**: Files are located in a USB flash drive. This option is: - supported for RPM patch upgrades not exceeding the storage capacity of the flash drive. - not supported for full-platform (ISO) upgrades to System Platform 6.2 or later. • **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, and depending on your network setup, configure a proxy address and port if necessary.
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.

Button	Description
Download	Downloads a patch file.

Patch List field descriptions

The Patch List page displays:

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

Components with patches

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

Fields per patch

Name	Description
Patch ID	File name of a patch. Click the name to view more details about the patch.
Description	Information about the patch, for example, if the patch is available for System Platform, the description is shown as `SP patch`.
Status	Status of a patch. Possible values of **Status** are **Installed**, **Not Installed**, **Active**, and **Not Activated**.
Service Affecting	Shows if installing the patch causes the associated 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, commit, roll back, 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 affecting when	Shows the action (if any) that causes the selected patch to restart the System Platform Web Console.
Restart this console when	Shows the conditions or circumstances when the System Platform Web Console must be restarted.
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.
Publication Date	Shows the publication date of the patch file.
License Required	Shows whether installation and use of the patch file requires the customer to obtain a software license from the Avaya corporation.
Rollbackable	Shows whether you can roll back the patch after installation.

Button descriptions

Button	Description
Refresh	Refreshes the Patch Details page.
Patch List	Opens the Patch List page, that displays the list of patches.
Install	Installs the respective patch.
Rollback	Rolls back the installed patch if the **Rollbackable** field value is Yes.
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 6: Configuring SAL Gateway on System Platform

SAL Gateway

Secure Access Link (SAL) Gateway provides Avaya support engineers and Avaya Partners with alarming and remote access to the applications on System Platform. System Platform includes an embedded SAL Gateway. SAL Gateway software is also available separately for stand-alone deployments. 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, possibly eliminating a service technician visit to the customer 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:

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

Stand-alone SAL Gateway

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

If you use a stand-alone SAL Gateway, you must add it as an SNMP trap receiver for System Platform. See Adding an SNMP trap receiver on page 135. You can also disable the SAL

Gateway that is embedded in System Platform so that it does not send duplicate heart beat messages to Avaya. See Disabling SAL Gateway on page 136.

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, Session Manager, 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 components of System Platform and of 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 on page 26
Configuration prerequisites on page 120

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** > **Avaya 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:

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

Related topics:

Registering the system on page 26
SAL Gateway on page 119

Changing the Product ID for System Platform

Before you begin

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

About this task

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

Procedure

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

   Note:

   VSPU is the model name for Console Domain.
3. Click **Save**.

System and browser requirements for accessing the Gateway user interface

Browser requirements for SAL Gateway:

- Internet Explorer 7 and 8
- Firefox 3.6 through 15.0.1

System requirements:

A computer with access to the System Platform network.

Starting the SAL Gateway user interface

Procedure

1. Log in to the System Platform Web Console.
2. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
3. On the **Server Management: SAL Gateway Management** page, click **Enable SAL Gateway**.
4. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.
5. When the SAL Gateway displays 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

About this task

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

Procedure

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

   For field descriptions, see Gateway Configuration field descriptions on page 124.
4. (Optional) Complete the following fields if the template supports inventory collection:
   - **Inventory Collection**
   - **Inventory collection schedule**
5. Click **Apply**.

   Note:

   The configuration changes do not take effect immediately. The changes take effect after you apply configuration changes on the Apply Configuration Changes page.
6. If necessary to cancel your changes, click **Undo Edit**.

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

   See the *Secure Access Link Gateway 2.1 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

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

Related topics:

Gateway Configuration field descriptions on page 124
Applying configuration changes on page 132

Gateway Configuration field descriptions

Name	Description
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.
IP Address	The IP address of the SAL Gateway. This IP address must be different from the unique IP addresses assigned to either the Cdom or Dom0 virtual machines.
Solution Element ID	The Solution Element ID that uniquely identifies the SAL Gateway. Format is `(000)123-4567`. If you have not obtained Solution Element IDs for the system, start the registration process. The system uses the SAL Gateway Solution Element ID to authenticate the SAL Gateway and its devices with the Secure Access Concentrator Remote Server.
Alarm ID	The Product ID (also called Alarm ID) for the SAL Gateway. This ID should start with a 5 and include ten digits. The system uses the value in the this field to uniquely identify the source of Gateway alarms in the Secure Access Concentrator Core Server.
Alarm Enabled	Enables the alarming component of the SAL Gateway. This check box must be selected for the SAL Gateway to send alarms.
Inventory Collection	Enables inventory collection for the SAL Gateway. When this check box is selected, SAL Gateway collects inventory information

Name	Description
	about the supported managed devices and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel working on tickets and must review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com
Inventory collection schedule	Interval in hours at which the SAL Gateway collects inventory data.

Related topics:

Registering the system on page 26

Configuring a proxy server

About this task

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

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Proxy**.
2. On the Proxy Server page, complete the following fields:
   - **Use Proxy**
   - **Proxy Type**
   - **Host**
   - **Port**
3. Click **Apply**.
4. (Optional) 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 2.1 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

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

Related topics:

Proxy server field and button descriptions on page 126
Applying configuration changes on page 132

Proxy server field and button descriptions

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

The page displays the following fields:

Name	Description
Use Proxy	Check box to enable the use of a proxy server.
Proxy Type	The type of proxy server that is used. Options are: • **SOCKS 5** • **HTTP**
Host	The IP address or the host name of the proxy server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
Port	The port number of the Proxy server.
Login	Login if authentication is required for the HTTP proxy server. **Important:** SAL Gateway in System Platform does not support authenticating proxy servers.
Password	Password for login if authentication is required for the HTTP proxy server. **Important:** SAL Gateway in System Platform does not support authenticating proxy servers.
Test URL	The HTTP URL used to test the SAL Gateway connectivity through the proxy

Name	Description
	server. The Gateway uses the proxy server to connect to the URL you provide.

The page displays the following buttons:

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

Configuring SAL Gateway communication with a Secure Access Concentrator Core Server

About this task

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

Procedure

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

   See the *Secure Access Link Gateway 2.1 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 2.1 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

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

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

Related topics:

Core Server field descriptions on page 128
Applying configuration changes on page 132

Core Server field descriptions

Name	Description
Passphrase	Default passphrase is `Enterprise-production`. Do not change the default unless you are explicitly instructed to do so. This passphrase is used to establish a channel for communication between the SAL Gateway and the Secure Access Concentrator Core Server.
Primary Core Server	IP Address or the host name of the primary Secure Access Concentrator Core Server. 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 Core Server	This value must match the value in the **Primary Core Server** field.
Port	This value must match the value in the **Port** field for the primary server.

Configuring SAL Gateway communication with a Secure Access Concentrator Remote Server

About this task

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

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Remote Server**.
   The Remote Server page appears.
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 2.1 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

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

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

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

Related topics:

Remote Server field descriptions on page 130
Applying configuration changes on page 132

Remote Server field descriptions

Name	Description
Primary Remote Server	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 Remote Server	This value must match the value in the **Primary Remote Server** field.
Port	This value must match the value in the **Port** field for the primary server.

Configuring NMS

About this task

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

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **NMS**.
2. On the Network Management Systems page, complete the following fields:
   - **NMS Host Name/ IP Address**
   - **Trap port**
   - **Community**
3. Click **Apply**.
4. (Optional) Use the **Add** button to add multiple NMSs.

   See the *Secure Access Link Gateway 2.1 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

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

Related topics:

Network Management Systems field descriptions on page 131
Applying configuration changes on page 132

Network Management Systems field descriptions

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

Managing service control and status

About this task

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

Procedure

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

- **Remote Access**
- **SAL Watchdog**
- **SAL SNMP Sub-agent**
- **Package Distribution**
- **SAL Agent Watchdog**

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

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Apply Configuration Changes**.
   The system displays the Apply Configuration Changes page.
2. Click the **Apply** next to **Configuration Changes**.
   See the *Secure Access Link Gateway 2.1 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.

Adding a managed element

Before you begin

Complete the Managed Element Worksheet for SAL Gateway.

About this task

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

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway** > **Managed Element**.
2. On the Managed Element page, click **Add new**.
3. Complete the fields on the page as appropriate.
4. Click **Add**.
5. Click **Apply** to apply the changes.

Next steps

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

Related topics:

Applying configuration changes on page 132
Managed Element field descriptions on page 133
Managed Element field descriptions on page 133
Managed element worksheet for SAL Gateway on page 179

Managed Element field descriptions

Name	Description
Host Name	Host name for the managed device. This must match the host name on the Network Configuration page of the System Platform Web Console (**Server Management** >

Name	Description
	Network Configuration in the navigation pane).
IP Address	IP address of the managed device.
NIU	Not applicable for applications that are installed on System Platform. Leave this field clear (not selected).
Model	The model that is applicable for the managed device.
Solution Element ID	The Solution Element ID (SE ID) of the device. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely.
Product ID	The Product ID (also called Alarm ID). 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 working on tickets and must review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com.
Inventory collection schedule	Interval in hours at which the SAL Gateway collects inventory information about the managed device.
Monitor health for this device	Check box to enable health monitoring of the managed device by SAL Gateway. SAL Gateway uses heartbeats to monitor health.

Name	Description
	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 to suspend health monitoring for the managed device. SAL Gateway resumes monitoring the device after the configured time elapses.

Related topics:

Managed element worksheet for SAL Gateway on page 179

Using a stand-alone SAL Gateway

Adding an SNMP trap receiver

About this task

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

Procedure

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

3. Click **Add SNMP Trap Receiver**.

Disabling SAL Gateway

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

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

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

About this task

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

Note:

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

Procedure

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

Chapter 7: 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 65.

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

Before you begin

Log into Communication Manager System Management Interface.

Procedure

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.

Name	Description
	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 system configuration files with the current values on the page and restarts the Communication Manager processes.
Restart CM	Updates the system configuration files with the current values on the page. **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

Before you begin

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

About this task

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

Procedure

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 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 often aligned with the DNS name of the server.
Alias Host Name	Is the alias host name for duplicated servers only. When the server is duplicated and is running in survivable mode, make sure that the alias host name field is populated.

Name	Description
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 - 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 system configuration files with the current values on the page and restarts the Communication Manager processes.
Restart CM	Updates the system configuration files with the current values on the page. **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 on the standby server.
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

Before you begin

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

Procedure

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. **This is a duplicated server using encrypted software-based duplication:** Encrypted software-based duplication provides memory synchronization between

Name	Description
	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 system configuration files with the current values on the page and restarts the Communication Manager processes. A dialog box is displayed 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.
Restart CM	Updates the system configuration files with the current values on the page. **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 8: Postinstallation administration, verification, and testing

Installation tests

You need to perform a number of post installation 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 *Implementing the Avaya Aura® Communication Manager Solution*, 03–603559, book for the installation and configuration tasks.

Perform the following post installation 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

About this task

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

Procedure

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

About this task

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.

Procedure

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

About this task

You can gain access to SMI 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.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.

2. In your browser, choose one of the following options depending on server configuration:

   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the 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 is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

   - Portable computer access by IP address

     To 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 the Logon page generates. 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 home page of the Communication Manager SMI.

Viewing the license status

Before you begin

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

About this task

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.

Procedure

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 151
License Status field descriptions on page 153

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 152

Verifying the software version

Before you begin

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

About this task

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.

Procedure

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

Before you begin

Log in to a Communication Manager SAT session.

About this task

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

Procedure

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

Procedure

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 9: Troubleshooting installation

Troubleshooting System Platform installation

Template DVD does not mount

The template DVD does not mount automatically.

Troubleshooting steps

Procedure

1. Log in to the Console Domain as admin.
2. Enter `su -`
3. Enter the root password.
4. Run the following commands:
   ```
   > ssh dom0.vsp /opt/avaya/vsp/template/scripts/udomAttachCd
   > mount /dev/xvde /cdrom/
   ```

System Platform installation problems

Troubleshooting steps

About this task

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.

Procedure

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

Use this procedure to determine if the state of the Console Domain virtual machine is the reason why you are unable to access the System Platform Web Console.

Troubleshooting steps

About this task

The Web Console runs on the Console Domain virtual machine, so if output of the **`xm list`** command described in this procedure shows that the Console Domain virtual machine is in either a normal or abnormal shutdown state, then the administrator is likely to lose access to the Web Console.

Important:

If you encounter these symptoms after completing the following procedure, go to the Avaya Support website at http://support.avaya.com. Take no further action to troubleshoot the issue locally.

Procedure

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

About this task

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

Procedure

Burn another DVD.

Service port not working

Troubleshooting steps

Procedure

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

System time drifts over a period of weeks

Troubleshooting steps

Procedure

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

Survivable server fails to sync with main server

Troubleshooting steps

Procedure

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.

Note:

If you change any of the configuration settings, click **Restart CM** to restart Communication Manager.

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

Branch Session Manager fails to completely install

CM_SurvRemote and CM_SurvRemoteEmbed templates include Branch Session Manager. After the template installation is finished, allow 20 additional minutes for the Branch Session Manager virtual machine to install and initialize. The Virtual Machine Management page on the System Platform Web console should list the Session Managers application state as *Running*. If not, follow these troubleshooting steps.

Troubleshooting steps

About this task

Perform the following troubleshooting steps if the replica group state is not **Synchronized**, **Queued for Repair**, or **Repairing**, or if the replica group is stuck in the **Starting** state.

Procedure

1. Log in to 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. Verify information in the `/etc/hosts` file of the System Manager:
   a. Log in to the CLI of the System Manager.
   b. Verify that the `/etc/hosts` file has the IP address, FQDN, and hostnames of itself and all of the associated Session Managers (applicable only if DNS is not used for host resolution of an IP address).

   c. Make corrections as needed.

6. Verify information in the `/etc/hosts` file of the Session Manager:
   a. Log in to the CLI of the Session Manager server.
   b. Verify that the `/etc/hosts` file has the IP address, FQDN, and hostnames of itself and the System Manager.
   c. Make corrections as needed.
7. If changes were made to any of the `/etc/hosts` files, reboot both the Session Manager and System Manager servers.

   Note:

   Before you reboot the System Manager server, take a backup of the configuration and installed templates files. If you need to manually edit the `/etc/hosts` files, investigate the other underlying reasons for the problem.
8. Enter **`initTM`**. The command should complete within 10 minutes. If it does not complete within that time, continue with the next step.
9. Verify that the system date and time on the Session Manager server is in sync with the system date and time on the System Manager virtual machine. Trust certificate initialization can fail if the clocks differ by more than a few seconds.
10. Enter **`SMnetSetup`**.
    a. Verify that all of the information is correct.
    b. Verify the Enrollment password is correct from the System Manager Security screen.
    c. Re-enter the Enrollment password.
11. On System Manager, check to see if the Session Manager is now synchronized.

Appendix A: Installation worksheet for System Platform

Use the System Platform preinstallation worksheet to help you gather in advance vital configuration values for successful installation, and for initial administration immediately following installation.

The System Platform installer application requires you to fill in various fields. Having the values required for these fields in advance helps the installation to progress more efficiently and accurately. It is likewise important and useful to gather information in advance about other key fields important for System Platform administration immediately following installation.

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

System Configuration

Name	Value	Description
Proxy Configuration:		
Status		Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform.
Address		The address for the proxy server.
Port		The port address for the proxy server.
Cdom Session Timeout		
Session Timeout Status		Specifies whether Cdom session timeout is enabled or disabled.
Session Timeout (minutes)		The maximum amount of time in minutes that a Cdom session remains open since the last user transaction with the System Platform Web Console or Cdom CLI.
WebLM Configuration:		
SSL		Specifies whether the Secure Sockets Layer (SSL) protocol

Name	Value	Description
		will be used to invoke the WebLM server. Select **Yes** if the alternate WebLM application has an HTTPS web address. Otherwise, select **No** if the alternate WebLM application has an HTTP web address. Default value = **Yes**.
Host		The IP address or hostname extracted from the web address of the WebLM application. Default value = *<cdom_IP_address>*.
Port		The logical port number extracted from the web address of the WebLM application, for example, `4533`. Default value = `52233`
Other System Configuration:		
Syslog IP Address		IP address of the Syslog server, which collects log messages generated by the System Platform operating system.
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.
SNMP Discovery		By default, this feature enables SNMPv2 management systems to automatically discover any System Platform server in an Avaya Aura-based network, including retrieval of server status and vital statistics. This is useful, for example, when using System Manager to view the

Name	Value	Description
		entire inventory of System Platform servers across multiple Avaya Aura enterprise solutions at a glance. This feature eliminates the tedious and error-prone task of manually adding a large number of System Platform servers to an SNMP management system, where that system often requires three or more IP addresses for each System Platform server. SNMP management systems can also query any recognized System Platform server for its logical configuration. System Platform supports network discovery of values for the following MIB objects: • RFC 1213 (MIB-2, autodiscovery): sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, and sysServices • RFC 2737 (Entity MIB) get/getnext/getbulk: entPhysicalTable – One table entry for the Dom0 physical interface. entLogicalTable – One table entry for the Cdom virtual machine, and one table entry for each virtual machine associated with the installed solution template. Each entry contains the virtual machine name, type, software version, and IP address. If you disable this option, SNMP manager systems will be unable to automatically discover this System Platform server.

Enable IPv6 Configuration

Name	Value	Description
Turn On IPv6		Enables IPv6.

General Network Settings Configuration

Name	Value	Description
Default Gateway		The default gateway IP address.
Primary DNS		The primary Domain Name System (DNS) server address.
Secondary DNS		(Optional) The secondary DNS server address.
Domain Search List		The search list, which is normally determined from the local domain name. By default, it contains only the local domain name. You can change this by listing the desired domain search path following the *search* keyword, with spaces or tabs separating the names.
Cdom Hostname		Depending on requirements of your solution template, you may need to enter the host name for Console Domain as a fully qualified domain name (FQDN), for example, `SPCdom.mydomainname.com`. Otherwise, just enter the IP address for Console Domain or enter the hostname for Console Domain in non-FQDN format.
Dom0 Hostname		Depending on requirements of your solution template, you might need to enter the host name for System Domain as a fully qualified domain name (FQDN), for example, `SPDom0.mydomainname.com`. Otherwise, just enter the IP address for System Domain, or enter the hostname for System Domain in non-FQDN format.

Name	Value	Description
		When using a Domain Name System (DNS) server in your network, the System Domain hostname must be FQDN format.
Physical Network Interface		The physical network interface details for eth0 and eth1 (and eth2 in case of High Availability Failover is enabled).
Domain Dedicated NIC		Applications with high network traffic or time-sensitive traffic often have a dedicated NIC. This means the virtual machine connects directly to a physical Ethernet port and typically requires a separate cable connection to the customer network. See template installation topics for more information.
Bridge		The bridge details for the following: • **avprivate**: This is called a private bridge because it does not use any Ethernet interface, so it is strictly internal to the server. The System Platform installer attempts to assign IP addresses that are not in use. • **avpublic**: This bridge uses the Ethernet interface associated with the default route, which is usually eth0, but can vary based on the type of the server. This bridge generally provides access to the LAN for System Platform elements (System Domain (Dom-0) and Console Domain) and for any guest domains that are created when installing a template. The IP addresses specified during System Platform installation are assigned to the interfaces that System Domain (Dom-0)

Name	Value	Description
		and Console Domain have on this bridge. • **template bridge**: These bridges are created during the template installation and are specific to the virtual machines installed.
Domain Network Interface		The domain network interface details for System Domain (Dom-0) or Console Domain that are grouped by domain based on your selection.
Global Template Network Configuration		The set of IP addresses and host names of the applications hosted on System Platform. Also includes the gateway address and network mask.
VLAN		Required only when installing System Platform on the S8300D server.

Services Virtual Machine Configuration

Name	Value	Description
Enable Services VM		Enables or disables remote access. Also supports local or centralized alarm reporting. Default value: **Enabled** Leave the **Enable services VM** option enabled (checkmark) for remote access and local SAL support, or disabled (no checkmark) if you have a separate server dedicated for independent/centralized remote access and SAL support.
Hostname		The name assigned to the Services Virtual Machine
Static IP address		The IP address assigned to the Services Virtual Machine. The address must be on the same subnet assigned to the Domain 0 (dom0) and Console Domain (cdom) virtual machines.

Name	Value	Description
Virtual devices		The virtual device (port) assigned to the Services Virtual Machine. Default value (eth0) automatically assigned. No user input necessary.

Ethernet Configuration

Name	Value	Description
Speed		Sets the speed in MB per second for the interface. Options are: • 10 Mb/s half duplex • 10 Mb/s full duplex • 100 Mb/s half duplex • 100 Mb/s full duplex • 1000 Mb/s full duplex Auto-Negotiation must be disabled to configure this field.
Port		Lists the available Ethernet ports. Auto-Negotiation must be disabled to configure this field.
Auto-Negotiation		Enables or disables auto-negotiation. By default it is enabled, but might cause some problems with some network devices. In such cases you can disable this option.

Bonding Interface Configuration

Name	Value	Description
Name		Is a valid bond name. It should match regular expression in the form of “bond[0-9]+”.
Mode		Is a list of available bonding modes that are supported by Linux.

Name	Value	Description
		The available modes are: • Round Robin • Active/Backup • XOR Policy • Broadcast • IEEE 802.3ad • Adaptive Transmit Load Balancing • Adaptive Load Balance For more information about bonding modes, refer to http://www.linuxhorizon.ro/bonding.html. **Note:** The default mode of new bonding interface is Active/Backup.
Slave 1/Primary		Is the first NIC to be enslaved by the bonding interface. If the mode is Active/Backup, this will be the primary NIC.
Slave 2/Secondary		Is the second NIC to be enslaved by the bonding interface. If the mode is Active/Backup, this will be the secondary NIC.

Static Route Configuration

Name	Value	Description
Interface		The bridge through which the route is enabled.
Network Address		The IP address of a destination network associated with an Avaya (or Avaya Partner) remote services host.
Network Mask		The subnetwork mask for the destination network.
Gateway		The address of a next-hop gateway that can route System Platform traffic to or from a

Name	Value	Description
		remote services host on the destination network.

SNMP Trap Receiver Configuration

Name	Value	Description
Product Id		Product ID for System Platform Console Domain. When you install System Platform, a default Product ID of 1001119999 is set. You must change this default ID to the unique Product ID that Avaya provides. **Note:** VSPU is the model name for Console Domain.
IP Address		IP address of the trap receiver.
Port		Port number on which traps are received.
Community		SNMP community to which the trap receiver belongs. Must be `public`.
Device Type		Default setting is **INADS**. Do not change this settings.
Notify Type		Default setting is **TRAP**. Do not change this setting.
Protocol Version		Default setting is **V2c**. Do not change this setting.

Password Configuration

Note:

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

Name	Value	Description
root Password		The password for the root login.
admin Password		The password for the admin login.

Name	Value	Description
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.

Network Time Protocol Configuration

Name	Value	Description
NTP server 1		The hostname or IP address of an NTP server, visible in the Web Console when you click **Query State** in the Date and Time Configuration page, under **Server Management**. When displayed, either of the following special characters precede each server hostname or IP address. Each character has a special meaning, as follows: • Asterisk character (*): The preferred server (currently referenced by the local system), chosen by System Platform. • Plus character (+): Indicates a high-quality candidate for the reference time that System Platform can use if its currently selected time source becomes unavailable. Avaya preconfigures several server names prior to system delivery. You can add more NTP reference servers by clicking **Add** in the Date and Time Configuration page under **Server Management**.
NTP server 2		

Name	Value	Description
NTP server 3		
NTP server 4		

Ping targets configuration

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

Appendix 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		

Appendix C: Managed element worksheet for SAL Gateway

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

Managed device (virtual machine)	IP Address	SE ID	Product ID	Model	Notes
System Domain (Dom 0)				VSP_2.0.0.0	System Domain (Dom 0) does not have alarming enabled; however, it has its own Product ID (Alarm ID). Console Domain (cdom or udom) has alarming enabled. System Domain sends all syslog (system logs) to Console Domain, which then triggers alarms on behalf of System Domain.
Console Domain (cdom or udom)				VSPU_2.1.1.2	

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

Appendix D: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) in case of any software update. For example, a PCN must accompany a service pack or a patch that needs to be applied universally. Avaya issues product-support notice (PSN) when there is no patch, service pack, or release fix, but the business unit or services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a workaround for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.

   Note:

   If the Avaya Support website displays the login page, enter your SSO login credentials.

2. On the top of the page, click **DOWNLOADS & DOCUMENTS**.
3. On the Downloads & Documents page, in the **Enter Your Product Here** field, enter the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select **Documents** as the content type.
6. Select the appropriate filters as per your search requirement. For example, if you select Product Support Notices , the system displays only PSNs in the documents list.

Note:

You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new services packs are available. The Avaya E-Notifications process manages this proactive notification system .

To sign up for notifications:

Procedure

1. Go to the Avaya Support Web Tips and Troubleshooting: eNotifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#.
2. Set up e-notifications. For detailed information, see the **How to set up your E-Notifications** procedure.

Index

A

activating license entitlements 73
admin password 61
administering customer login 92
AFID 78
    obtaining from System Platform 78
AFS 76
    starting 76
authentication file 77, 78
    creating for new system 77
    installing 78
authentication files 76
    about 76
Avaya Mentor videos 11
Avaya S8300D 39
Avaya S8800 39
Avaya S8xxx Servers 151
    accessing the System Management Interface ... 151

B

beginning installation of template 88
Branch Session Manager page 94
    field descriptions 94

C

check_install command 157
Check_install command 157
checking date and time settings 150
checking network configuration 62
checklist 22
    Communication Manager installation 22
checklist of hardware and software requirements 19
command line 67, 68
    accessing Console Domain 68
    accessing System Domain 67
Communication Manager 13
    overview 13
Communication Manager installation overview 13
Communication Manager installation wizard 89
Communication Manager template 17
configuring Branch Session Manager 94
configuring DHCP 93
configuring duplication parameters 145
configuring network 142
configuring server role 138
Confirm Installation page 96
    button descriptions 96
confirming installation 95
confirming template network configuration 97
console domain 53
    configuring network settings 53
Console Domain 68
    accessing command line 68
Console Domain Network Configuration screen 53
    configuring 53
craft password 61
creating 36
    EPW file 36
cust password 61
Customer Login page 93
    field descriptions 93

D

date 59
    configuring 59
Date/Time and NTP setup screen 59
    configuring 59
Dell™ PowerEdge™ R610 39
DHCP 93
    configuring 93
DHCP DNS Server IP address 93
DHCP field descriptions 93
DHCP network address 93
DHCP pool IP address range 93
DHCP router address 93
DHCP subnet mask 93
DHCP WINS Server IP address 93
document purpose 9
Downloading patches 99
downloading software 28
duplicated server 72
    licensing 72
duplication parameters 144
Duplication Parameters page 145
    field descriptions 145
DVD 30, 157
    does not mount automatically 157
    requirements 30

writing ISO image 30
DVD does not read 159

E

entering virtual machine IP address and hostname ... 91
without using EPW file 91
EPW file 36, 89
creating 36
equipment 22
Avaya-provided 22

F

feature packs 69
field descriptions 114, 116, 117, 126, 133, 139, 142, 145
Duplication Parameters page 145
Managed Element page 133
Network Configuration page 142
Patch Detail page 117
Patch List page 116
Proxy Server page 126
Search Local and Remote Patch page 114
Server Role page 139
Firefox 42
disabling proxy servers 42

G

Gateway Configuration 124
field descriptions 124
Guardian 36
license error mode 36
Guardian enforcement 34, 35
dot releases 35
service packs 34

H

host ID 73
obtaining 73
HP ProLiant DL360 G7 39

I

installation 39, 46, 48, 163
process 39
using laptop 46
using server console 48
worksheet 163
installation prerequisites for Communication Manager 175
installation tests 149
installing Branch Session Manager 94
installing Communication Manager templates 81
installing Communication Manager using Installation Wizard 91
Installing Kernel patch on duplex configuration 102
Installing Kernel patch on high availability configuration 106
Installing Kernel patch on simplex configuration 100
Installing patches 100
Installing Regular patch on duplex configuration 104
Installing Regular patch on simplex configuration 101
Installing Security patch on duplex configuration 105
Installing Security patch on high availability configuration 107
Installing Security patch on simplex configuration 102
Intended audience 9
Internet Explorer 42
disabling proxy servers 42
IP forwarding 65
disabling 65
enabling 65
IP settings 41
configuring on laptop 41
ISO image 29, 30, 43
verifying on DVD 43
verifying on Linux-based computer 29
verifying on Windows-based computer 29
writing to DVD or CD 30

K

keyboard 48
selecting type 48
Keyboard Type screen 48

L

laptop 41, 46, 64
configuring to connect to server 41
connecting to server 64
using to install System Platform 46
ldap password 61
legal notice 2
license 152
viewing status 152
license entitlements 73
activating 73
license features 32

mapping to Communication Manager Customer Option features 32
license file 75
installing 75
License Status 153
field descriptions 153
licensing 71, 72
about 71
duplicated server 72

M

managed element 133, 179
adding in SAL Gateway 133
worksheet for SAL Gateway 179
Managed Element page 133
field descriptions 133

N

network configuration 141
Network Configuration page 142
field descriptions 142
Network Management Systems page 131
field descriptions 131
network settings 44, 50, 53
configuring for console domain 53
configuring for system domain (domain-0) 44, 50
Network Settings page 92
field descriptions 92
NMS 130, 131
configuring for SAL Gateway 130
field descriptions 131
NTP server 59
configuring in System Platform 59

O

overview 13, 14
Communication Manager 13
System Platform 14

P

passwords 60
configuring in System Platform 60
default 60
Passwords screen 60, 61
configuring 60
field descriptions 61
Patch Detail page 117
field descriptions 117
Patch installation 100
Patch List page 116
field descriptions 116
patches 69
about 69
Patches 98
PCN 181
PCN notification 181
PCNs 181
PLDS 27, 28, 71
about 71
downloading software 28
powering on a server 46
Product ID 121
changing for System Platform 121
product registration 120
proxy 99
configuring for System Platform 99
proxy server 125
configuring for SAL Gateway 125
Proxy Server page 126
field descriptions 126
proxy servers 42
disabling in Firefox 42
disabling in Internet Explorer 42
PSN 181
PSN notification 181
PSNs 181

R

registering 27
registration 26
of system 26
related resources 11
Avaya Mentor videos 11
remote server 129, 130
configuring 129
field descriptions 130
Remote Server 130
field descriptions 130
Removing Kernel patch when the status of the patch is active on duplex configuration 110
Removing Kernel patch when the status of the patch is active on high availability configuration 113
Removing Kernel patch when the status of the patch is active on simplex configuration 108
Removing Kernel patch when the status of the patch is installed 107
Removing Regular patch when the status of the patch is active on duplex configuration server 111

Removing Regular patch when the status of the patch is active on simplex configuration 109
Removing Regular patch when the status of the patch is installed 108
Removing Security patch when the status of the patch is active on duplex configuration 112
Removing Security patch when the status of the patch is active on high availability configuration 113
Removing Security patch when the status of the patch is active on simplex configuration 109
Removing Security patch when the status of the patch is installed 108
requirements 22
for System Platform installation 22
reviewing summary information 95
reviewing the template state 150
on System Platform Web Console 150
root password 61

S

SAL Core Server 127, 128
configuring 127
field descriptions 128
SAL Gateway .. 26, 119, 120, 122, 123, 125, 127–133, 136
adding a managed element 133
applying configuration changes 132
browser requirements 122
configuring 123
configuring a proxy server 125
configuring network management system 130
configuring NMS servers 131
configuring remote server 129, 130
configuring SAL Core Server 127, 128
configuring Secure Access Concentrator Core Server 127
disabling 136
managing service control and status 131
prerequisites for configuration 120
registering 26
starting user interface 122
Search Local and Remote Patch page 114
field descriptions 114
Search Local and Remote Template page 87
field descriptions 87
Secure Access Gateway Server 119
Select Template page 91
button descriptions 91
server 64, 155
connecting laptop 64
Server 49
hardware checks 49
server console 48
using to install System Platform 48
server installation 40
server role configuration 137
Server Role page 139
field descriptions 139
servers 39, 151
accessing the System Management Interface ... 151
Service Packs and Dot Release Guardian 31
overview 31
services port 65
accessing System Platform through 65
Services Virtual Machine (VM) 56
installing 56
Services VM 57, 58
network configuration 57
field descriptions 57
VM footprint size 58
field descriptions 58
signing up for PCNs and PSNs 182
SNMP trap receivers 135
adding 135
software installation 39
solution template 26, 84
installing 84
registering applications 26
Status 131
SAL Gateway service 131
support 11
contact 11
survivable server 154
registration 154
system 82
configuring 82
System Configuration page 82
configuring 82
field descriptions 82
System Domain 67
accessing command line 67
system domain (domain-0) 44, 50
configuring network settings 44, 50
System Domain Network Configuration screen 52
field descriptions 52
System Platform 14, 26, 157
check_install command 157
overview 14
registering 26
System Platform Web Console 66
accessing 66

T

technical assistance 9
Telnet 46
    opening session from laptop to System Platform server 46
template 84
    installing 84
Template Details page 89
    button descriptions 89
Template Installation page 89
    button descriptions 89
time 59
    configuring 59
time zone 58
    configuring 58
Time Zone Selection screen 58
    configuring 58
training 11
troubleshooting 157–161
    DVD does not mount 157
    DVD does not read 159
    failure to access Web console 158
    failure to ping Console Domain 158
    service port not working 160
    Session Manager fails to install 161
    survivable server fails to sync with main 160
    system time drifts over a period of weeks 160
Troubleshooting 157
    System Platform installation problems 157

U

uploading EPW file 90

V

verify 96
    virtual machine installation 96
verify if active 155
verify if the server is standby 155
verifying server is active 155
verifying software version 154
videos 11
    Avaya Mentor 11
Viewing 33, 34
    software publication date 34
    support end date 33
Viewing PCN from the Support site 98
Viewing Release Notes from the Support site 98
Virtual Machine 58
    footprint size 58
Virtual Machine Management page 87
    field descriptions 87
VSP Console Domain Network Configuration screen 53, 54
    configuring 53
    field descriptions 54
vspmediacheck 43

W

Warranty 12
Web Console 66
    accessing 66
WebLM 72, 73
    accessing from System Platform 72
    obtaining host ID 73
worksheet 163, 179
    installation 163
    SAL Gateway managed elements 179