What's New in Avaya Aura® Release 7.0

Release 7.0
03-601818
Issue 1
August 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.
- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.
- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

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” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel

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

Copyright

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

Virtualization

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

How to Get Help

For additional support telephone numbers, go to the Avaya support Website: http://www.avaya.com/support. If you are:

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's “telecommunications equipment” includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, “networked equipment”).

An “outside party” is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a “malicious party” is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company’s Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya’s customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user’s authority to operate this equipment.

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable

protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   - answered by the called station,
   - answered by the attendant,
   - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   - routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

- A call is unanswered
- A busy tone is received
- A reorder tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ａ 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ｂ 情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

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 is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document provides an overview of the new and enhanced features of the following Avaya Aura® 7.0 components:

- Appliance Virtualization Platform Release 7.0
- Avaya Aura® System Manager Release 7.0
- Avaya Aura® Utility Services Release 7.0
- Avaya Aura® Session Manager Release 7.0
- Avaya Aura® Communication Manager Messaging Release 7.0
- Avaya Aura® Communication Manager Release 7.0
- Avaya Aura® Presence Services Release 7.0
- Application Enablement Services Release 7.0
- Avaya Branch Gateway Release 7.0
- Avaya Aura® Call Center Elite Release 7.0
- WebLM Release 7.0
- Avaya Media Server Release 7.7

Intended audience

This document is for the following audience:

- Contractors
- Employees
- Channel associates
- Remote support
- Sales representatives
- Sales support
- On-site support

- Avaya Business Partners

Related resources

Documentation

The following table lists the documents related to the components of Avaya Aura® Release 7.0. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Implementation			
—	*Deploying Avaya Aura® applications from Avaya Aura® System Manager*	Describes the procedures for installation, configuration, initial administration, and basic maintenance checklist and procedures for deploying Avaya Aura® applications in Virtualized Environment by using Avaya Aura® System Manager Solution Deployment Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
—	*Upgrading and Migrating Avaya Aura® applications from Avaya Aura® System Manager*	Describes the procedures and checklists for upgrading Avaya Aura® applications to Release 7.0	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administration			
555-233-504	Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network components of Communication Manager Release 7.0, such as gateways, trunks, FAX, modem, TTY, and Clear-Channel calls.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-300509	Administering Avaya Aura® Communication Manager	Describes the procedures and screens used for administering Communication Manager Release 7.0.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
—	Administering Avaya Aura® System Manager	Describes the procedures for configuring System Manager	Solution Architects, Implementation

Table continues…

Document number	Title	Description	Audience
		Release 7.0 and the Avaya Aura® applications and systems managed by System Manager.	Engineers, Sales Engineers, Support Personnel
—	Avaya Aura® Presence Services Snap-in Reference	Describes the steps to deploy and configure Presence Services Release 7.0.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Understanding			
555-245-205	Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-602878	Avaya Aura® Communication Manager Screen Reference	Describes the screen and detailed field descriptions of Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-603324	Administering Avaya Aura® Session Manager	Describes how to administer Session Manager by using System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
555-245-207	Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware devices that can be incorporated in a Communication Manager telephony configuration.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Maintenance and Troubleshooting			
03-300431	Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers	Provides commands to monitor, test, and maintain hardware components of Avaya servers and gateways.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.

2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Downloading documents from the Support website

About this task

To download the latest version of Avaya documents from the Support website, perform the following steps:

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. At the top of the Avaya Support homepage, click the **Documents** tab.
3. In the **Enter Your Product Here** field, type the product name for which you want to download the documents. Once you start typing the product name, the website displays the results matching to the entered text. You can select the complete product name from the displayed list.
4. In the **Choose Release** field, select **7.0.x**.
5. Click **Enter**.

   Note:

   To refine the search results, select a document category. You can also select multiple categories. If no category is selected, the website displays all the documents for the selected product and release.

   The website displays a list of documents for the selected product and release.
6. To open a document, click the document title.

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
Avaya Aura® core implementation	
1A00234E	Avaya Aura® Fundamental Technology
4U00040E	Avaya Aura® Session Manager and System Manager Implementation
4U00030E	Avaya Aura® Communication Manager and Communication Manager Messaging Implementation
10U00030E	Avaya Aura® Application Enablement Services Implementation
8U00170E	Avaya Aura® Presence Services Implement and Support
AVA00838H00	Avaya Aura® Media Server and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Aura® Media Server and Gateways Implementation Workshop Labs
Avaya Aura® core support	
5U00050E	Session Manager and System Manager Support
5U00060E	ACSS - Avaya Aura® Communication Manager and CM Messaging Support
4U00115I 4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.x to R6.x)
1A00236E	Avaya Aura® Session Manager and System Manager Fundamentals
2008W	What is New in Avaya Aura® Application Enablement Services 7.0
2008T	What is New in Avaya Aura® Application Enablement Services 7.0 Online Test
2009W	What is New in Avaya Aura® Communication Manager 7
2009T	What is New in Avaya Aura® Communication Manager 7.0 Online Test
2010W	What is New in Avaya Aura® Presence Services 7.0
2010T	What is New in Avaya Aura® Presence Services 7.0 Online Test
2011W	What is New in Avaya Aura® Session Manager and Avaya Aura® System Manager 7.0
2011T	What is New in Avaya Aura® Session Manager and Avaya Aura® System Manager 7.0 Online Test
2013V	Avaya Aura® 7 Administration
Avaya Aura® core administration and maintenance	
9U00160E	Avaya Aura® Session Manager for System Administrators
1A00236E	Avaya Aura® Session Manager and Avaya Aura® System Manager Fundamentals
5U00051E	Avaya Aura® Communication Manager Administration

Table continues…

Course code	Course title
5M00050A	Avaya Aura® Communication Manager Messaging Embedded Administration, Maintenance & Troubleshooting
2012V	Migrating and Upgrading to Avaya Aura® 7.0
2012I	Migrating and Upgrading to Avaya Aura® 7
2017	Avaya Aura® 7 Administration Delta
2017V	Avaya Aura® 7 Administration Delta
Unified Communications soft clients	
5U00150E	Knowledge Access: Avaya UC Soft Clients Implementation and Support
5106	Avaya UC Soft Clients Implementation and Maintenance Test
8U00030O	What's New in Avaya Multimedia Messaging 2.1, Avaya Communicator for Android 2.1 and Avaya Communicator for Windows 2.1
2002W	What is New in Avaya Communicator 2.1 for iPhone and Android

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Avaya Aura® 7.0 components

Product component	Release version
Communication Manager	7.0
Session Manager	7.0
System Manager	7.0
Branch Gateway	7.0
Presence Services	7.0
Application Enablement Services	7.0
Call Center Elite	7.0
Utility Services	7.0
Communication Manager Messaging	7.0
Avaya Media Server	7.7
WebLM	7.0

Product compatibility

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

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.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service

request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Avaya platform offer

Avaya supports the following models:

- Avaya-provided appliance: System Manager Release 7.0 with the Solution Deployment Manager service runs on an Avaya-provided appliance. Avaya-provided appliance contains server hardware and Appliance Virtualization Platform. Appliance Virtualization Platform contains the ESXi hypervisor and the application OVA.

  From Release 7.0, Avaya Aura® does not support templates.

  The new Common Server Release 2 servers that Avaya offers contain preinstalled Appliance Virtualization Platform. For the new S8300D or S8300E server installation, Appliance Virtualization Platform is installed at the customer site. In this offer, System Manager is a mandatory application.
- Virtualized Environment: Customers provide Virtualized Environment with a standard ESXi environment on which customers can deploy the System Manager and other Avaya Aura® virtual applications that Avaya provides.

Avaya virtual appliance model

The Avaya virtual appliance model includes:

- An Avaya-defined common server platform.
- An operating system for allocating and managing servers among virtual machine instances running on the server. The hardware resources include CPU, memory, disk storage, and network interfaces.
- A Secure Access Gateway that supports a Secure Access Link for remote diagnosis by Avaya or Avaya Business Partner. However, Secure Access Link is optional.

Appliance Virtualization Platform overview

From Release 7.0, Avaya uses the VMware®-based Avaya Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya appliance offer.

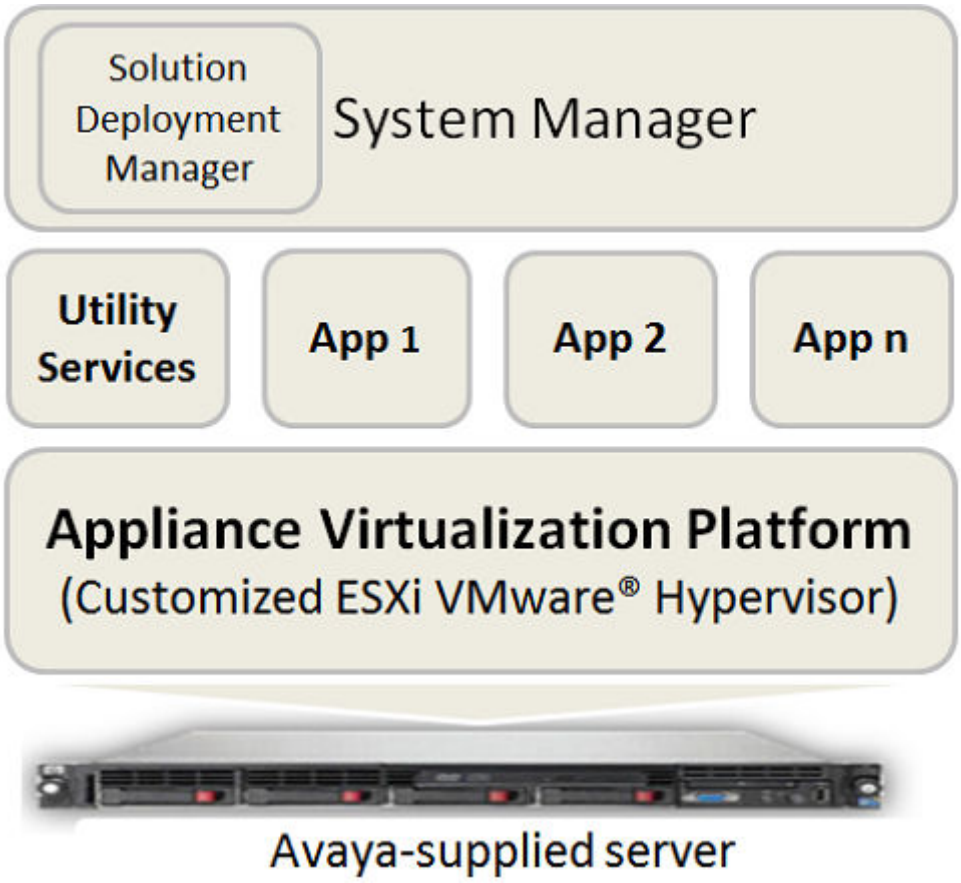
Avaya-appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, HP ProLiant DL360 G7, and HP ProLiant DL360p G8
- S8300D and S8300E

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. With Appliance Virtualization Platform, customers can run any combination of supported applications on

Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.

Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware® tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.



In Release 7.0, Appliance Virtualization Platform replaces System Platform.

Avaya Aura® Release 7.0 supports the following applications on Appliance Virtualization Platform:

- Utility Services 7.0
- System Manager 7.0
- Session Manager 7.0
- Branch Session Manager 7.0
- Communication Manager 7.0
- Application Enablement Services 7.0
- WebLM 7.0
- Engagement Development Platform 3.1
- SAL 2.5

- Communication Manager Messaging 7.0
- Avaya Aura® Media Server 7.7

Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to suite of Avaya Aura® 7.0 applications. Solution Deployment Manager supports the operations on customer Virtualized Environment and Avaya-provided appliance model.

Solution Deployment Manager provides the combined capabilities that Software Management, Avaya Virtual Application Manager, and System Platform provided in earlier releases.

System Manager Release 7.0 is the primary management solution for Avaya Aura® 7.0 applications.

System Manager with the Solution Deployment Manager runs on:

- An Avaya-provided appliance: Contains server, Appliance Virtualization Platform, and Avaya Aura® application OVA. Appliance Virtualization Platform includes a VMware ESXi 5.5 hypervisor.

  From Release 7.0, Appliance Virtualization Platform replaces System Platform.
- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, certified VMware® hardware.

With Solution Deployment Manager, you can perform the following operations in Virtualized Environment and Avaya appliance models.

- Deploy Avaya Aura® applications
- Upgrade and migrate Avaya Aura® applications
- Download Avaya Aura® applications
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications:
  - Communication Manager and associated devices, such as gateways, media modules, and TN boards.
  - Session Manager
  - Branch Session Manager
  - Utility Services
  - Appliance Virtualization Platform. The ESXi host running on Avaya-provided appliance.

The upgrade process involves the following key tasks:

- Discover the Avaya Aura® application.
- Analyze and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade the Avaya Aura® application.

Solution Deployment Manager options

Avaya provides the following Solution Deployment Manager options:

- Centralized Solution Deployment Manager: The System Manager capability to deploy, upgrade, migrate, and install software patches for Avaya Aura® applications. Release 7.0 supports migration of System Platform-based Avaya Aura® 6.x applications to Release 7.0 on Avaya-provided appliance.

  However, in Release 7.0, Solution Deployment Manager does not support migration of Virtualized Environment-based 6.x applications to 7.0 in customer Virtualized Environment. Use vSphere Client to migrate to customer Virtualized Environment.
- Solution Deployment Manager client: A lightweight tool that can reside on the computer of a technician. The technician can gain access to the client by using the web browser.

  Use the Solution Deployment Manager client to:

  - Deploy virtual appliances on Virtualized Environment or Avaya-provided appliance.
  - Upgrade System Manager, install System Manager patches, and install hypervisor patches.
  - Start, stop, and restart a virtual machine.
  - Change the footprint size based on the capacity requirements of the Avaya Aura® application.

The centralized and client Solution Deployment Manager provide the following capabilities:

Centralized Solution Deployment Manager	Solution Deployment Manager client
Manage virtual machine lifecycle	Manage virtual machine lifecycle
Deploy Avaya Aura® applications	Deploy Avaya Aura® applications
Deploy hypervisor patches only for Appliance Virtualization Platform	Deploy hypervisor patches only for Appliance Virtualization Platform
Upgrade Avaya Aura® applications Release 7.0 supports upgrades from Linux-based or System Platform-based to Virtualized Environment or Appliance Virtualization Platform. Release 7.0 does not support Virtualized Environment to Virtualized Environment upgrades.	Upgrade System Platform-based System Manager
Install software patches for Avaya Aura® applications	Install System Manager patches
Discover Avaya Aura® applications	Deploy System Manager
Analyze Avaya Aura® applications	-
Create and use the software library	-

Solution Deployment Manager client

For the initial System Manager deployment or when System Manager is inaccessible, you can use the Solution Deployment Manager client. The client can reside on the computer of the technician.

The Solution Deployment Manager client provides the functionality to install the OVAs on an Avaya-provided server or customer-provided Virtualized Environment. The user interface of the Solution Deployment Manager client looks similar to the centralized Solution Deployment Manager.

System Manager supports the Solution Deployment Manager client. A technician can gain access to the user interface of the Solution Deployment Manager client from the computer or web browser.

The Solution Deployment Manager client runs on Windows 7.0 and Windows 8, 64 bit.

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Virtualized Environment or Avaya appliances.
- Upgrade System Platform-based System Manager and install System Manager and hypervisor patches.
- Start, stop, and restart a virtual machine.
- Change the footprint size based on the capacity requirements of the Avaya Aura® application.

You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.

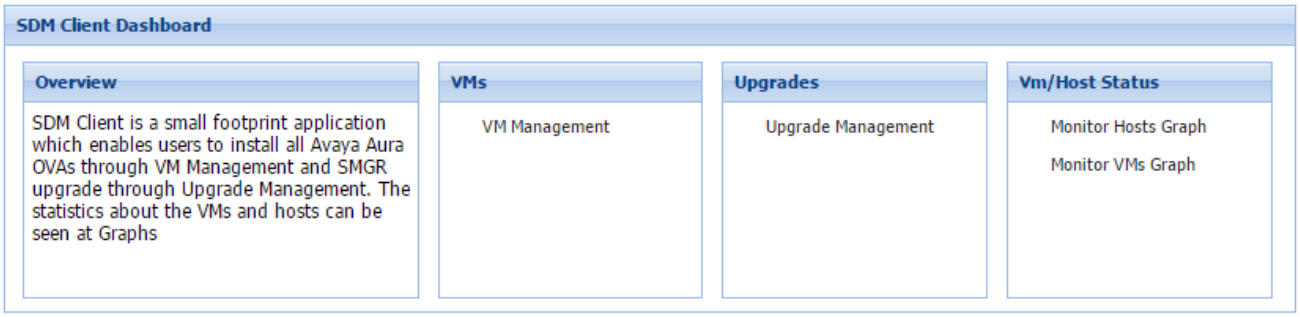


Figure 1: Solution Deployment Manager client dashboard

Solution Deployment Manager

The Solution Deployment Manager capability simplifies and automates the deployment and upgrade process.

With Solution Deployment Manager, you can deploy the following Avaya Aura® Release 7.0 applications:

- Utility Services 7.0
- System Manager 7.0
- Session Manager 7.0
- Branch Session Manager 7.0
- Communication Manager 7.0

- Application Enablement Services 7.0
- WebLM 7.0
- Engagement Development Platform 3.1
- SAL 2.5
- Communication Manager Messaging 7.0
- Avaya Aura® Media Server 7.7

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

- Linux-based Communication Manager and the associated devices, such as Gateways, TN boards, and media modules.
- Linux-based Session Manager
- System Platform-based Communication Manager
  - Duplex CM Main / Survivable Core with Communication Manager
  - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- System Platform-based Branch Session Manager
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services

Note:

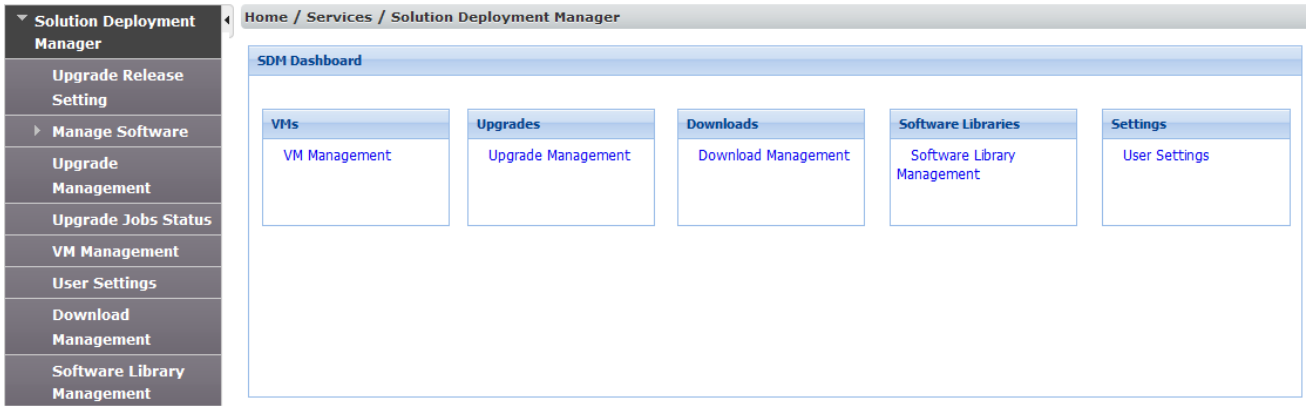
However, you must manually migrate Services VM that is part of the template.

You require only one SAL or Services VM per enterprise to support an Avaya Services offer.

The centralized deployment and upgrade process provide better support to customers who want to upgrade their systems to Avaya Aura® Release 7.0. The process reduces the upgrade time and error rate.

Solution Deployment Manager dashboard

You can gain access to the Solution Deployment Manager dashboard from the System Manager web console or by installing the Solution Deployment Manager client.



Solution Deployment Manager capabilities

With Solution Deployment Manager, you can perform deployment and upgrade-related tasks by using the following links:

- **Upgrade Release Setting**: To select **Release 7.0** or **6.3.8** as the target upgrade. Release 7.0 is the default upgrade target.
- **Manage Software**: To upgrade the legacy Communication Manager, IP Office, and B5800.
- **VM Management**: To deploy OVA files for the supported Avaya Aura® application.
- **Upgrade Management**: To upgrade Communication Manager, Session Manager, Communication Manager Messaging, Utility Services, Avaya Aura® Branch Session Manager to Release 7.0.
- **User Settings**: To configure the location from where System Manager displays information about the latest software and firmware releases.
- **Download Management**: To download the OVA files to which the customer is entitled. The download source can be the Avaya PLDS or an alternate source.
- **Software Library Management**: To configure the local or remote software library for storing the downloaded software and firmware files.

Avaya Aura® applications upgrade

With System Manager Solution Deployment Manager, you can upgrade the following Avaya Aura® applications to Release 7.0:

- Communication Manager
- Session Manager
- Branch Session Manager
- Utility Services

Note:

You must upgrade System Manager to Release 7.0 by using the Solution Deployment Manager client before you upgrade the Avaya Aura® applications to Release 7.0.

Chapter 3: What's new in System Manager

This chapter provides an overview of the new features and enhancements of System Manager Release 7.0.

What's new in System Manager

Avaya Aura® System Manager Release 7.0 supports the following new features and enhancements:

- Avaya offers the following:
  - Avaya-provided appliance: System Manager Release 7.0 with the Solution Deployment Manager service runs on an Avaya-provided appliance. Avaya-provided appliance contains server hardware and Appliance Virtualization Platform. Appliance Virtualization Platform contains the ESXi hypervisor and the application OVA.

    From Release 7.0, Avaya Aura® does not support templates.

    The new Common Server Release 2 servers that Avaya offers contain preinstalled Appliance Virtualization Platform. For the new S8300D or S8300E server installation, Appliance Virtualization Platform is installed at the customer site. In this offer, System Manager is a mandatory application.

    Release 7.0 does not support deploying or upgrading Avaya Aura® application to System Platform.
  - Virtualized Environment: Customers provide Virtualized Environment with a standard ESXi environment on which customers can deploy the System Manager and other Avaya Aura® virtual applications that Avaya provides.
- Solution Deployment Manager, a centralized capability to:
  - Deploy Avaya Aura® applications that System Manager supports
  - Upgrade and migrate Avaya Aura® applications, such as Communication Manager, Communication Manager Messaging, Utility Services, Session Manager, and Branch Session Manager to Release 7.0
  - Install service packs and software patches of Avaya Aura® applications
- The Solution Deployment Manager client that can be installed on the computer
- The Solution Deployment Manager client:
  - Deploy System Manager and other Avaya Aura® applications

  - Upgrade System Manager
  - Install System Manager software patches
- Support for the following web browsers:
  - Microsoft Internet Explorer Release 9.x, 10.x, and 11.x
  - Mozilla Firefox Release 36, 37, and 38

  Note:

  System Manager does not support Firefox releases earlier than 36.
- Virtual machine management:
  - Add an ESXi and Appliance Virtualization Platform host
  - Create and edit a location
  - Create and edit a virtual machine
  - Start, stop, and restart virtual machines
  - Map the ESXi host to an unknown location
  - Monitor CPU and memory usage of hosts and virtual machines
- View and delete the following upgrade-related jobs:
  - Refresh elements
  - Analyze
  - Pre-Upgrade check
  - Upgrade
  - Commit
  - Rollback
  - Uninstall
- Communication Manager 6.3.100 support that includes discovery, inventory, upgrade, update, and new MIBS.

  Note:

  For upgrades to Communication Manager 6.3.100, customer must reconfigure the SNMP alarming on the upgraded system.
- User Management enhancements: User Management interface displays administration fields that apply to administering tasks for applications that the customer solution supports. For example, if a customer solution contains only one Communication Manager, Session Manager, and Communication Manager Messaging, you cannot select more than one server. If a customer solution does not contain Conferencing servers, the Conferencing communication profile is unavailable for the administrator.
- Security enhancements: Integration of System Manager Release 6.3.8 Certificate Authority Generation Utility in System Manager Release 7.0.

Supports SRVname in the **SubjectAltName** field. When you select this option, the system includes the service name in the certificate.

- SIP users and devices enhancements:
  - Scale increased to support 250000 SIP users from 125000 users
  - Scale increased to support 350000 SIP Endpoint devices from 150000 devices
  - Scale increased to support 28 instances of Session Manager from 12 instances of Session Manager
- Directory synchronization enhancements: LDAP synchronization of Active Directory administrator groups with System Manager administrator roles. The capability includes system roles and custom roles on System Manager.
- Bulk import and export enhancements:
  - Import and export of the CM Agent profile data of the user by using Excel and XML files.
  - Import and export of the Work Assignment profile by using Excel and XML files.

Directory synchronization enhancements

System Manager supports LDAP synchronization of Active Directory administrator roles with System Manager administrator roles. The capability includes system roles and custom roles on System Manager.

Out of Band Management in System Manager

Out of Band Management is two physically or logically separated network connections or both that connects to a private management network of the customer. The network connection provides secure management and administration of Avaya products. With Out of Band Management, you can separate the management network and data network traffic to System Manager.

System Manager provides the following network interfaces:

- The regular eth0 interface that was present in releases earlier than System Manager 7.0, is called the Management interface or Out of Band Management interface. The IP address is called as the Management IP address. The Management interface is mandatory for configuration.

  The following are the examples of System Manager Management network traffic:

  - Database replication with Session Manager
  - Element management. For example, Session Manager, Communication Manager, and Engagement Development Platform.
  - User management
  - Solution deployment, upgrades, and software patch install

- If Out of Band Management is enabled, then the Public interface is configured with Public IP address and used for the nonmanagement traffic. This is an optional configuration.

  The following are the examples of System Manager nonmanagement or public network traffic:

  - End-user self-provisioning
  - Client devices getting certificates through SCEP
  - Tenant Management

Out of Band Management configuration persists across System Manager upgrades, updates, and restarts.

For configuring Out of Band Management in System Manager, System Manager must be installed on an Appliance Virtualization Platform host that is configured with Out of Band Management. Out of Band Management is enabled during the deployment of Appliance Virtualization Platform.

Out of Band Management in a Geographic Redundancy setup

When you configure Geographic Redundancy, provide Management network details only. Validation fails if you configure Geographic Redundancy with Public network details. In Geographic Redundancy setup, you do not disable or enable Out of Band Management on both primary and secondary System Manager virtual machine. You can enable Out of Band Management on the primary System Manager virtual machine and disable Out of Band Management on the secondary System Manager virtual machine, and vice versa.

Restoring System Managerbackup

While restoring backup on System Manager with different Out of Band Management network details, the restore operation fails at validation phase.

Tenant Management on Out of Band Management-enabled System Manager

By default, the Multi Tenancy feature is disabled on System Manager when Out of Band Management is enabled. You must enable Multi Tenancy on Out of Band Management-enabled System Manager for the Tenant Management administrator to manage tenant users.

Upgrade job status

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

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

Upgrade target release selection

For backward compatibility, System Manager supports upgrading Communication Manager to Release 6.3.6 or later. By default, the target version is set to Release 7.0. Based on entitlements, to upgrade Communication Manager and the associated applications to Release 6.3.6, you must select Release 6.3.8 as the upgrade target release.

Supported upgrades and migrations

Supported upgrades

With Solution Deployment Manager, you can upgrade the following Avaya Aura® applications to Release 7.0:

- Linux-based Communication Manager and the associated devices, such as media gateways, TN boards, and media modules.
- System Platform-based Communication Manager
  - Duplex CM Main / Survivable Core with Communication Manager
  - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- Branch Session Manager associated with Communication Manager
- Linux-based Session Manager
- For customer-provided Virtualized Environment solutions, System Manager Solution Deployment Manager and the Solution Deployment Manager client does not support upgrade and migration from Release 6.x to Avaya Aura® Release 7.0.

Supported updates

With Solution Deployment Manager, you can install service packs, feature packs, and software patches for the following Avaya Aura® Release 7.0 applications:

- Communication Manager and the associated devices, such as media modules, TN boards, and media gateways
- Session Manager
- Branch Session Manager
- Communication Manager Messaging
- Utility Services

- Appliance Virtualization Platform, the ESXi host running on Avaya-provided appliance

Supported upgrades from the Solution Deployment Manager client

You can perform the following only from the Solution Deployment Manager client:

- Upgrading System Manager
- Installing software patches and service packs on System Manager

Chapter 4: What's new in Utility Services

This chapter provides an overview of the new features and enhancements for Avaya Aura® Utility Services 7.0.

S8300E support for Utility Services Release 7.0

The S8300E server is based on a 2.0 GHz, dual core Intel Ivy Bridge processor. The S8300E server supports Utility Services Release 7.0. The S8300E server is certified by VMware as VMware Ready.

For more information see, *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207

IP Phone Firmware Removal

Utility Services no longer bundles the IP Phone firmware within the build. To ensure that Utility Services has the correct IP Phone firmware for the installation, you must download the latest version of the firmware from PLDS. You can download the latest IP Phone firmware to store on Utility Services at any time. The IP Phone firmware management features remain unchanged from the previous versions.

Audit Account Addition

Utility Services Release 7.0 supports an auditor account. You can use the auditor account to view the configuration and log files on Utility Services Release 7.0. However, you cannot alter any configuration. During the time of installation, the default password for the auditor account is `audit01`. You can change the default password at any given instance by starting an SSH session to Utility Services Release 7.0.

Utility Services in the Avaya-appliance model

In Avaya Aura® Release 7.0, Utility Services replaces the console domain (C-dom). Utility Services runs the Services Port connection that was previously run through Dom-0 on System Platform. As a result, Utility Services with the Services Port virtual machine becomes a key component, and must be deployed on all virtual machines in Avaya-appliance offer in Release 7.0.

With Services Port, you can connect a laptop directly to Ethernet 1 on an Avaya-supported server, and connect the laptop to any of management interface of applications that run on an Appliance Virtualization Platform host. On the S8300D and S8300E, Services Port is on the front plate. The Services Port virtual machine also supports ASG logins and install of a customer ASG file on to the system. By default, a generic ASG file is available on the system.

The Services Port virtual machine incorporates the Serviceability Agent for alarming and log collection from System Manager.

From Avaya Aura® Release 7.0, Utility Services does not include IP Phone firmware. The administrator must download the latest version of the firmware from PLDS and install on Utility Services.

Utility Services migration

In Avaya-appliance offer on Appliance Virtualization Platform, you require Utility Services for services static routing. Therefore, you must deploy Utility Services if Utility Services is part of the solution.

In the following two use cases, you might require to deploy Utility Services.

1. Migration of Communication Manager or Session Manager on Linux® server: Utility Services is mandatory for migration of systems running on Linux® server. In this case, before you migrate, you must deploy Utility Services from VM Management.
2. Migration of Communication Manager or Session Manager on System Platform: In this case, the template already contains Utility Services. In this case, the process migrates Utility Services, and you do not require to deploy Utility Services separately.

Chapter 5: What's new in Session Manager

The following sections describe the new features and enhancements for Avaya Aura® Session Manager Release 7.0.

Automatic Alarm Clearing

Session Manager clears alarms automatically when possible.

Session Manager clears an alarm when:

- The alarm condition has been resolved. For example, an alarm is generated when the Security Module periodic test fails. Session Manager automatically clears the alarm when the test passes.
- The alarm condition is not seen for a certain amount of time.

Session Manager does not clear an alarm if:

- Avaya Technical Services must be involved in correcting the issue.
- The alarm is generated for log event. For example, an alarm indicating a failure event.
- Session Manager cannot determine if the alarm condition has been resolved.

When Session Manager does not automatically clear the alarm, the customer or Avaya Technical Services must manually clear the alarm.

Branch Session Manager Support

The following features and enhancements are supported for Release 7.0:

- Branch Session Manager is now available as an OVA for both appliance (embedded or stand alone) and VE configurations. Branch Session Manager does not need to be located on the same server as the Communication Manager Survivable Remote, but requires a Survivable remote in the configuration.
- The S8300E Embedded Server supports Branch Session Manager.
- Scalability enhancements. The hardware on which the Branch Session Manager is running and the chosen footprint determine the number of SIP devices supported.

- Management GUI improvements.
- Response time enhancements.
- Large numbers of Branch Session Manager instances can be pre-staged within the configuration using the Maintenance Mode service state. The Maintenance Mode service state puts the Branch Session Manager into a dormant state to prevent unnecessary warnings, alarms, and system monitoring.

Emergency Call Notification to Adjunct Emergency Location Server

With the Multiple Device Access (MDA) feature, users can register with multiple devices. In the past, the multiple devices usage with one extension number, may have resulted in a problem establishing the exact location of an emergency call. However, in 7.0, the callers exact location can now be determined. This allows Session Manager to support the tracking of an emergency caller in large campus settings. The advanced communication applications guide the emergency crew to the exact location of the emergency call using LED display units near the main entrance of the site.

The applications use the capabilities of the following Avaya Aura® components:

- Session Manager shares the IP address of the caller's SIP device.
- Communication Manager shares the identity of the emergency caller from the database.

Session Manager adds an Emergency Call (EC) Alert to the existing Adjunct Emergency Location Server (AELS) interface for the SIP users. The AELS establishes the exact location of the emergency caller.

The caller may be a SIP user registered through System Manager or an unregistered/unknown user.

End-to-End Secure Call Indication

Starting with Release 7.0, endpoints display an icon that indicates whether a call is secure or not. The call security indication is only for point to point SIP calls. The icon is similar to the icon displayed by web browsers when visiting a secured web site.

A typical two-party call between enterprise SIP endpoints routes through several SIP elements, specifically Session Manager, Communication Manager, and Session Border Controller. All of these elements can impact the end-to-end security of the call.

A SIP entity marked secured is one that does not expose the signaling and media streams to unauthorized monitoring or modification. A call is considered secure if all the signaling hops between the two entities (for example, TLS) and all media streams are secure (for example, SRTP). Any call crossing an entity that is not administered as securable will not be considered a secure call even if the entity meets the rest of the security constraints.

The Session Manager administrator has the option to mark a SIP entity as not secure if the entity is a third party entity or an older version.

Note:

When you administer the SIP entities using System Manager, mark the following Avaya Aura® elements as secure. To mark the elements as secure, click the **Enable End to End Secure Call Indication** check box on the Session Manager Administration page to turn the feature on globally and then mark each element on the Sip Entity page.

If you mark any other element that is not listed here as secured, the End-to-End Secure Call Indication feature might not give correct indication about a call security.

- Communication Manager Release 7.0 or later
- Avaya SBCE Release 7.0 or later

License Enforcement per Session Manager instance

Each instance of Avaya Aura® Session Manager or Branch Session Manager that is running on a server or virtual instance must have a Session Manager instance license. Session Manager is licensed through a single license file that includes the following information associated with the Session Manager instance:

- Major release
- Instance licenses
- Feature settings for the Session Manager instance

Session Manager instance licensing:

- Uses the Product Licensing and Delivery System (PLDS) for license generation and delivery.
- Uses the System Manager Web License Manager (WebLM) as the license server.
- Controls the Session Manager software version at the major release level. For example, the license is valid only for Release 7.0.
- Provides a 30-day license grace period before any license enforcement action is taken.

Session Manager licensing provides the right to use the Session Manager software.

The number of license requests to WebLM is based on the number of administered Core Session Manager and Branch Session Manager instances.

The Session Manager Element Manager prevents customers from adding a new Session Manager or Branch Session Manager if the number of instances exceeds the feature capacity of their purchased software entitlements. Customers can still modify or delete Session Manager and Branch Session Manager instances.

Note:

The instance license capacity shortfall is applied to Branch Session Manager instances before being applied to the Core Session Manager instances.

Session Manager licensing has no special redundancy considerations. In the case of geo-redundant System Manager, the license file is installed on the active System Manager and shared by the standby System Manager. The active System Manager provides all licensing and mirrors information such as license modes and grace period information, to the standby System Manager. When the standby System Manager becomes active, the standby System Manager takes over the license operations and information from where the active System Manager stopped.

License Modes

The Session Manager Element Manager maintains separate license modes for each Session Manager instance.

There are three license modes:

- **License Normal Mode:** No license errors exist for the Session Manager instance and full Session Manager functionality is available.
- **License Error Mode:** A license error exists. The 30-day grace period is active and full Session Manager functionality is available.
- **License Restricted Mode:** A license error exists and the 30-day grace period has expired. Session Manager functionality is restricted. The Session Manager instance has been placed into the **Deny New Service** state. The service state cannot be changed to **Accept New Service** until the license error issue has been resolved.

For any Session Manager instance with a license error, the Session Manager Dashboard page and the Session Manager Element Manager Administration page displays a warning message at the top of the page.

If a Session Manager Element Manager license request to the WebLM does not receive a response from the WebLM or receives a response that no license file is installed, the Session Manager Element Manager:

- Logs a license error against all Session Manager instances.
- Sets the license mode of any Session Manager instance currently in **License Normal Mode** to **License Error Mode**.
- Starts the 30-day license grace period for the Session Manager instance that did not receive a response to the license request.

Lync integration simplification

Previously, for Lync integration, the administrator had to enter or administer the Presence Services handle of an Avaya Aura® user twice: once as the Avaya Presence/IM (formerly XMPP) handle, and the second time as the Avaya SIP handle. The duplicate administration was required for proper routing of the Lync originated subscription and IM requests.

Starting with Session Manager Release 7.0, the Presence Services handle only needs to be administered once.

To support tighter integration with Microsoft Lync, Session Manager:

- Supports routing rules, configured in System Manager, to deliver Lync Presence/IM traffic to Presence and Avaya Multimedia Messaging as appropriate.
- Recognizes and routes on the Presence/IM handle type.
- Inserts the media type (mtype) parameter in the Route header when routing to SIP entities.

Note:

The Lync server does not connect with a Branch Session Manager in branch locations.

Maintenance Mode Service state

To support deployment and maintenance of many Session Manager or Branch Session Manager instances, a non-operational Session Manager or Branch Session Manager can be set to the **Maintenance Mode** service state. The **Maintenance Mode** service state essentially places Session Manager or Branch Session Manager into a dormant state. **Maintenance Mode** is not a SIP service state and is independent of the **Deny** and **Accept New Service** states.

Use the **Maintenance Mode** service state for:

- Staging installations where Session Manager or Branch Session Manager is not provisioned on the network.
- Pre-administering a large number of Branch Session Manager instances before installing or configuring the machines.
- Upgrading an existing Session Manager or Branch Session Manager.
- Preventing large amounts of error logging and alarming during a temporary outage.

When you change the service state to **Maintenance Mode**, the system:

- Changes the service state of Session Manager or Branch Session Manager to the **Deny New Service** state if the service state is **Accept New Service**.
- Does not generate alarms.

Service Observing from SIP Phone

Using the Service Observing feature, a supervisor or authorized user can use a telephone to activate an observing session towards a station, an agent LoginID, or VDN to listen in and possibly talk on calls received by the station/agent or VDN for quality control and training purposes. The audio from the observed connection is switched in to the first idle appearance on the phone being used for the Service Observing feature. The observer remains off-hook or idle during the call.

The **sip-sobsrv** button appears on the station form for the 96x1 SIPCC and an Avaya one-X® Agent defined as a SIPCC station type only if the **Call Center Release** field is set to 7.0 or later. This button is not available for assignment to any other station type and limited to one per endpoint.

When the user assigns this button to a 96x1SIPCC station type, the following two options appear:

- **listen-only? :** The default is **n**. The service observing activation is in listen-only mode and cannot be changed to the **listen-talk** mode. An observer can change the talk mode from **listen-only** to **listen-talk**, and vice-versa, *only* while the observer is actively observing a call. The talk mode cannot be changed while the observer is in the wait state. If the observer changes the talk mode during a call, that specific talk mode stays active after the observed call is cleared, unless the user changes the talk mode prior to the clearing of the call.
- **coach?:** The default is **n**. The observer can activate coaching while observing a call that is connected to a local station or agent if the observer is in either listen-only or listen-talk mode.

The text string presented on the display of the endpoint depends on the observed entity's type (Station, AgentID, or VDN) and on the type of called number (Station, AgentID (DAC), or VDN).

For more information about this feature, see the following documentation on the Avaya Support website:

- *Avaya Aura® Call Center Elite Feature Reference*
- *Avaya Aura® Call Center Elite Overview and Specification*
- *Administering Avaya Aura® System Manager*
- *Administering Avaya Aura® Communication Manager*

Session Manager Scale increases

Session Manager 7.0 increases capacities to support an Avaya Aura® solution of up to 250K total users, 350K total devices, overall.

Up to 250K users or 350K devices are supported by any N+M sparing Session Manager configuration consisting of a Common Server R2 or comparably sized VMware server and connection devices. The customer must adequately distribute devices across primary and secondary servers to accommodate the configuration. For example, the typical Session Manager solution with N+1 sparing supports 350K devices across 15 Session Manager instances for a single Session Manager failure. Similarly, a dual data center (N+N) supports 350K devices across 28 Session Manager instances (14 in each data center).

SIP Header Removal

Avaya Aura® Session Manager customers can use the Adaptation Modules to remove specific headers from SIP messages. The administrator defines sets of headers to be removed in the ingress (message entering Session Manager) and egress (messages leaving Session Manager)

directions. As part of the Adaptation Module processing, Session Manager removes the specified headers from the messages.

A customer could inadvertently include some of the mandatory and/or required headers in the list of headers to be removed. Session Manager will not remove any mandatory SIP headers, even if the headers are included in the set of exempted headers in adaptations.

The header removal feature does not change the adaptation module selection criteria.

Note:

The SIP Header Removal feature only removes headers. The feature does not remove parameters to decrease the header size. Session Manager removes the headers that are either Avaya proprietary or deemed excessive and unnecessary for non-Avaya elements.

SIP Health monitoring

Starting with Release 7.0, Session Manager can monitor the health of a SIP entity and share the health reports.

SIP Health Monitoring is based on the client-server model. The client, a non-Session Manager element, places the request to monitor the health of the links between particular SIP entities (monitored entities) and a Session Manager instance (monitoring entity). In response, the server (Session Manager) shares the current state of the link(s). When the state of any of the links changes, the server shares the updated reachability state with the client. Monitoring continues until the client requests the health monitoring to stop.

An API specifies the monitoring entity and the monitored entities. The API supports specifying more than one monitored entity in a single request. Only one active request can exist for a particular monitoring entity. If a request is already active, the new request overwrites the existing request.

Upgrade improvements

The Solution Deployment Manager is an application that replaces the System Platform CDOM functions. With the Solution Deployment Manager, Session Manager supports:

- **Centralized Upgrades:** The user can now upgrade from System Manager using the Solution Deployment Manager.
- **Upgrade rollback:** The Solution Deployment Manager supports upgrade rollback.
- **Patch rollback:** The Solution Deployment Manager supports full patch rollback, including platform security updates.

Chapter 6: What's new in Communication Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® Communication Manager 7.0.

For more information about these features, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Media encryption using AES-256

In Communication Manager Release 7.0, the AES encryption option now includes AES-256 cipher suite. AES-256 applies to voice media streams and video media streams for the IP network region that governs the IP codec set. The feature also introduces a mechanism to define the encrypted SRTCP policy for calls governed by the IP network region.

Encrypted SRTCP

Use the Encrypted SRTCP feature to provide enhanced security for the media control streams associated with the RTP media stream.

Note:

The RTP and RTCP streams are two consecutive UDP ports. The RTCP control stream conveys usage data. An example of usage data is the identification of the two parties on a given call.

Avaya Aura® Media Server

The Avaya Aura® Media Server is used by Communication Manager to provide IP audio capabilities similar to legacy H.248 media gateways or port networks with media processors. These capabilities include:

- Terminating RTP audio streams
- Conferencing of RTP audio streams
- Playing and recording announcements
- Generating system tones
- Collecting digits

Media Server instances and channels are licensed features. Each Media Server must obtain an instance license from a WebLM server. Media Server channels are licensed through the Communication Manager feature license file which specifies the number of Media Server channels allowed on Communication Manager. Media Server channels can be established on any Media Server configured in Communication Manager.

For information about Avaya Aura® Media Server integration feature for Communication Manager Release 7.0, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Allow direct input of Route Pattern for SIP station routing

The Allow direct input of Route Pattern for SIP station routing feature is introduced to simplify the routing configuration of a SIP station.

The feature is introduced to reduce configuration errors by bypassing AAR and ARS routing for SIP OPTIM routing. This feature also allows System Manager to automatically suggest the correct route pattern by identifying the IP address and port on the signaling group associated with the route pattern.

End-to-end secure call indication

With the End-to-end secure call indication feature, a SIP phone displays an icon indicating the security of a SIP call.

The SIP phone displays the security icon when the end-to end call has the following setup:

- Media is SRTP.
- SIP signaling is TLS.
- Media Server signaling links or Media Gateway, if applicable, is TLS.

The End-to-end secure call indication feature is applicable only for point-to-point calls. The icon on the SIP phone displays the call as secure only for two-party calls. However, when a third-party is

involved, such as a conference, the icon displays the call as unsecured even if the call is on a secured network.

SIP Agent Reachability

The SIP Station Reachability feature determines the availability of a SIP station from the perspective of Communication Manager and an AES application.

The registration state for a SIP station is maintained by Session Manager. However, the station might not be reachable from Communication Manager because of a network outage between the station and Session Manager and Avaya Session Border Controller for Enterprise, or a disruption between Communication Manager and Session Manager. In such instances, Communication Manager receives no information about the reachability status of the station. If the feature is enabled, Communication Manager can detect a SIP station's reachability status and take actions as configured.

S8300E server

The S8300E server is based on a 2.0 GHz, dual core Intel Ivy Bridge processor. The S8300E server is supported in the G430 Branch Gateway and G450 Media Gateway. The S8300E server supports Appliance Virtualization Platform and Communication Manager Release 6.3.8 and later. The S8300E server is certified by VMware as VMware Ready.

SIP digit handling

The Request URI in a SIP INVITE message, REFER message, or 3xx redirect response for INVITE message contains the following types of digits:

- Called-party digits
- Called-party and extra end-to-end digits

  For example, an authorization code or a voice mail password.

By default, Communication Manager assumes that the Request URI contains extra end-to-end digits, which might lead to incorrect call routing.

For example, a Request URI with 12 digits can match a Dial Plan entry of 7 digits. But Communication Manager processes the last 5 digits as extra digits. Similarly, for a SIP connection, if the Request URI does not contain extra digits, then the calls can be wrongly routed. The user can configure the Request URI as **called number-only** to avoid calls being wrongly routed.

With the SIP digit handling feature, you can configure Communication Manager to allow or restrict the extra end-to-end digits in the message.

Media Gateway VoIP Capacity Test 1718

This test sends a query to the media gateway to get the VoIP resources hardware state. If a failure is returned, there could be busied-out and hardware-faulted VoIP media resources. The associated failure error code that might be displayed with this test indicates the percentage of busied-out or faulted resources.

Call Type Digit Analysis

With the Call Type Digit Analysis feature, you can specify how Communication Manager must modify a telephone number to route a call when the call is made using:

- Call logs
- Contacts
- A corporate directory

The telephone number in a call log, contact, or corporate directory might not in a routable format. Communication Manager performs the digit analysis without matching the number with the Dial Plan Analysis screen. For example, the number (212) 848-2249 cannot be routed directly. The number must be dialed as (91212) 848-2249. To convert the number to a routable format, the Communication Manager:

- Enables the endpoint to modify the number.
- Modifies the number using the Call Type Digit Analysis feature.

With the Call Type Digit Analysis feature in Communication Manager Release 7.0, the system can:

- Process the plus sign (+) in the missed or answered call log of an H.323 or a SIP endpoint.
- Perform location-based digit conversion on numbers dialed from an endpoint, even when the numbers are not dialed from a call log, contact, or corporate directory. You must set the **Location-Based Call Type Analysis** field to enable location-based digit conversion. The dialed number must match with an entry in the Dial Plan Analysis screen.

Out-of-Band management

Using the Out-of-Band management feature, you can set up a dedicated network connection to your network to securely manage Communication Manager. The network connection can be a physical or virtual connection.

Support for Full-call model in Feature Server

Communication Manager 7.0 can be configured as a feature server with ASAI enabled to support the full-call model. A whole call or multiple half calls are mapped to a unique ASAI caller ID for ASAI to process all calls as a whole call. ASAI also supports mapping multiple half calls to a unique caller ID if IMS is not enabled in all Session Manager instances. ASAI generates the same call processing messages for the full-call model in the feature server as the evolution server.

Special applications

Special applications, also known as green features, meet special requirements of customers. Communication Manager supports many of these special applications at no additional cost, without the need for new licenses. You can log in as a super user and activate these applications. Although these applications are available for use, they are not extensively tested.

Some special applications require exact configuration and expert intervention. If these applications are not configured accurately, they may not operate as expected or the system may slow down or both. To activate these applications, go to the Avaya Support website at http://support.avaya.com and open a service request.

For more information about special applications, see *Avaya Aura® Communication Manager Special Application Features*.

Chapter 7: What's new in Communication Manager Messaging

This chapter provides an overview of the new features and enhancements of Communication Manager Messaging Release 7.0.

Support for software currency and interoperability

The Communication Manager Messaging Release 7.0 is enhanced to support software currency and interoperability with the Avaya Aura® 7.0 solution:

- The Linux OS has been updated to Red Hat Enterprise Linux version 6.
- Communication Manager Messaging is integrated with the Avaya Virtual Platform and Solution Deployment Manager.
- Communication Manager Messaging supports the Avaya SIP Reference Architecture and Security guidelines for encryption protocols.

Deprecated capabilities

The following deprecated capabilities have been removed from Communication Manager Messaging Release 7.0:

- Communication Manager Messaging is no longer supported as an embedded application in Communication Manager. With Release 7.0, Communication Manager Messaging is installed as an instance of its own virtual machine.
- H.323/Q.Sig integration is no longer supported. Customers should convert the Communication Manager Messaging application to a SIP integration prior to an upgrade to Release 7.0.
- Migrations from Intuity Audix and Intuity Audix LX are no longer supported. The capability to migrate within the backup and restore procedure is no longer supported in Communication Manager Messaging.

Supported upgrades

You can directly upgrade to Communication Manager Messaging Release 7.0 from the following Communication Manager Messaging releases:

- Release 6.3.100 SP5 and later
- Release 6.3 SP4, 6.3 SP5, and later
- Release 6.2 SP3
- Release 6.0.1 SP5
- Release 5.2.1

Note:

If the release of your currently installed Communication Manager Messaging is not listed above, you need to upgrade to one of the latest release versions listed above prior to upgrading to Communication Manager Messaging Release 7.0.

For more information, see the following documents:

- *Deploying Communication Manager Messaging using VMware® in the Virtualized Environment*
- *Upgrading and Migrating Avaya Aura® applications to Release 7.0*

Chapter 8: What's new in Presence Services

This chapter provides an overview of the new and enhanced features of Presence Services Release 7.0.

Deployment of Presence Services snap-in

Presence Services 7.0 is deployed as a snap-in on the Engagement Development Platform instance. This migration enables Presence Services to provide most of the current capabilities while adding increased scale and redundancy options like High Availability. This migration also supports rapid application development in a robust, scalable environment.

Enhanced High Availability

Presence Services 7.0 provides a new active-active high availability option that helps provide business continuity in case of the failure of a Presence Services instance.

Support for blocking Instant Messaging between Tenants

This feature enables administrators to restrict the exchange of Instant Messaging between users on the same presence server.

This capability is enabled if Multi-tenancy mode is enabled for the Aura system.

Message Archiver

Message Archiver enables Presence Services to store all incoming and outgoing IMs in a local database.

Users must provide a reliable storage server to which Presence Services can periodically transfer the files from the database.

Support for enhanced federation

Presence Services 7.0 enables the exchange of presence and instant messages between two or more Avaya Aura® systems in a clustered Presence Services environment. This feature provides flexibility for customers deploying Presence Services in large environments where clustered solutions are required.

Offline IM Storage

If Offline IM Storage is enabled and a user sends an IM to an offline user, Presence Services:

- Stores the IM in a local database. These IMs survive events such as Presence Services restarts and High Availability failovers.
- Delivers the IM when the offline user logs in to an IM-capable endpoint.

Presence Services does not provide an indication to the sender that the IM is temporarily stored or is delivered to the user.

Chapter 9: What's new in Application Enablement Services

This chapter provides an overview of the new features and enhancements for Application Enablement Services Release 7.0.

AE Services Virtualized Appliance support

AE Services 7.0 does not support the System Platform and Bundled offers. The AE Services 6.3.3 or earlier servers based on the System Platform or Bundled offer cannot be directly upgraded to AE Services 7.0. These servers can be migrated to AE Services 7.0 by reconfiguring the servers for the Avaya Virtualized Appliance model based on Appliance Virtualization Platform. The supported servers are Dell PowerEdge R610 and R620 , and HP ProLiant DL360 G7 and G8 servers. The total memory on these servers should be upgraded to a total minimum of 12 GB. AE Services 7.0 will continue to support the Software-Only and Virtualized Environment offers.

Note:

For more information on backup and restore functions, see the following topics in *Deploying Avaya Aura® Application Enablement Services in a Virtual Environment for VMware*:

- Backing up the AE Services server data
- Restoring the AE Services server data.

Device Media Call Control (DMCC) scale to 8000 instances

Currently, a single AE Services server can support a maximum of 4,000 Device Media Call Control (DMCC) instances. Call Center as a Service (CCasS) deployments continue to increase in scale and the current limit of 4,000 DMCC forces the deployment of additional AE Services servers in circumstances where full time recording is required for over 4,000 agents. To support the customer demand for this increased scale, the maximum number of DMCC instance will increase to 8000.

Increased number of domain control associations

AE Services 7.0 supports usage of up to 8 domain controllers per station for better scaling, particularly for Customer Engagement OnAvaya Aura – Contact Center as a Service and large Elite opportunities. Previously, the number of domain controllers used for each service supported on AE Services was limited to only 4 domain controllers per station.

Geographic Redundancy High Availability enhancement

From AE Services 7.0 onwards, Geographic Redundancy High Availability (GRHA) is supported on servers deployed in the Virtualized Environment. Fast Reboot High Availability (FRHA) is not supported in AE Services 7.0. Customers previously using FRHA can use GRHA. GRHA has all the functionality that FRHA provides, and supports servers to be on the same network.

Infrastructure update

In AE Services 7.0, the RHEL release has been updated to Release 6.5.

Additional support is now added for Internet Explorer 11. DMCC SDK support is now added for Java 8.

Increased endpoint support

AE Services 7.0 provides support for the 9601 SIP-only endpoint.

Note:

Administer the 9601 SIP-only endpoint as a 9608 SIP endpoint.

Detection of unreachable SIP endpoints and logging out unreachable SIP agents

This enhancement is intended to address situations where a SIP endpoint becomes unreachable and the Communication Manager (CM) would have no information about the issue. If a Contact Center (CC) Elite agent is logged in to the endpoint the Communication Manager will still see everything as being correct. In practice, the agent could be logged in but with the endpoint

unreachable and with CM still seeing the agent as available when the agent is not. Reporting systems will also still show the agent as logged in.

Default certificate change

The AE Services server comes pre-installed with a set of default server certificates for lab use, that is, out-of-the-box deployments. For AE Services 7.0, the Certificate Authority (CA) used to sign the server default certificate has changed. To allow your client to connect to the AE Services 7.0 server using a TLS socket connection for lab testing, the new AE Services CA certificate will need to be exported from the server, and imported into your client trust store.

Note:

Do not use the default server certificates in a production environment. Avaya recommends that you must replace all the default installed certificates with new certificates.

Out of Band Management enhancement

Out of Band Management provides the ability to move the AE Services Management Console Web based management and configuration traffic of the server to a dedicated subnetwork.

Chapter 10: What's new in Branch Gateway

This chapter provides an overview of the new features and enhancements for Branch Gateway 7.0.

Media encryption using AES-256

In Branch Gateway 7.0, support has been added for the AES-256 cipher suite. AES-256 can now be selected on the Communication Manager SAT administration screen under the AES encryption option. AES-256 applies to voice media streams and video media streams for the IP network region that governs the IP codec set. The feature also introduces a mechanism to define the encrypted SRTCP policy for calls governed by the IP network region.

Enhancements to security features

In Branch Gateway 7.0:

- TLS is upgraded to include support of TLS version 1.2. SSLv2 and SSLv3 are no longer supported and OpenSSL is upgraded to version 1.0.1L
- Online Certificate Status Protocal (OCSP) support is added as an alternative certificate validation technique to Certificate Revocation Lists (CRLs).
- Greenwich Mean Time (GMT) Timezone offset awareness is also added to provide greater accuracy when validating a certificate's expiration.
- Gateway login password policy is enhanced. The date and time of the last login and the number of login failures is displayed on the console everytime a user logs onto the gateway.
- SHA-2 signed certificates are supported for firmware images downloaded to the gateway.

Out-of-Band management

Using the Out-of-Band management feature, you can set up a dedicated network connection to your network to securely manage the Avaya products. The network connection can be a physical or virtual connection.

Encrypted SRTCP

Use the Encrypted SRTCP feature to provide enhanced security for the media control streams associated with the RTP media stream.

Note:

The RTP and RTCP streams are two consecutive UDP ports. The RTCP control stream conveys usage data. An example of usage data is the identification of the two parties on a given call.

Chapter 11: What's new in Call Center Elite

This chapter provides an overview of the new and enhanced features of Call Center Elite Release 7.0.

New in this release

- Number of trunks that can be measured is increased from 12,000 to 24,000.
- Capacity of logged-in agent-skill pairs increased from 100,000 to 360,000, on a single instance of Communication Manager.
- Number of Communication Manager locations supported by Call Center Elite increased from 250 to 2000.
- Capability to detect and log out unreachable SIP agents and stations.
- Support for setting Call Prompting timeout period to 2 seconds.
- Service Observing Whisper Coaching added on H.323 and DCP deskphones.
- Support for Avaya Aura® Media Server.
- New field named **Attribute** added to the Agent LoginID screen.

Feature description

Call Center Elite enhances the business value of every customer interaction, ensures a consistent customer experience, and drives costs down.

Business Advocate

Business Advocate is a Call Center Elite feature that uses a patented routing algorithm to:

- Manage agents and call volumes.
- Meet service levels.
- Predict call wait time.

- Reduce agent burnout.

Business Advocate automates the activation of reserve agents to prevent overflow of calls in a queue.

Dynamic Advocate, which is a Business Advocate feature, automatically adjusts the overload threshold based on the service level requirements.

Business Advocate leverages the following features to balance business needs such as service levels, caller segmentation, and multiskilled agent management:

- Percent Allocation for call selection and Percent Allocation Distribution (PAD) for agent selection
- Predicted Wait Time (PWT), which is applicable during call surplus conditions, as a systemwide call selection measurement
- Service Level Supervisor (SLS) with Call Selection Override and Reserve Agent
- Service Objective (SO) by Skill or Vector Directory Number (VDN)

For more information, see *Using Avaya Business Advocate* on the Avaya Support website at http://support.avaya.com.

Call Vectoring

Call Vectoring is the process of defining vector programs for call routing and call treatment.

Call vectors are a series of user-defined commands that you can use to route internal or network calls and to determine the treatment for each call. You can route calls to on-network or off-network destinations, or to staffed ACD agents.

Communication Manager directs all incoming calls to an administered VDN which could represent a service category, such as Billing, Customer Service, or Sales. The VDN directs calls to a vector with commands such as **`announcement`**, **`busy`**, **`collect digits`**, **`goto step`**, or **`wait-time`** for call routing and call treatment.

Use vector commands to perform the following call-related functions:

- Collection of touchtone digits
- Call treatment such as an announcement or a busy tone
- Call routing to more than one skill if an agent fails to answer the call
- Conditional and unconditional branching from one vector step to another step or vector
- Execution of voice scripts on a Voice Response Unit (VRU) to provide information to the caller

For information about Call Vectoring features and commands, see *Avaya Aura® Call Center Elite Feature Reference* and *Programming Call Vectoring Features in Avaya Aura® Call Center Elite* on the Avaya Support website at http://support.avaya.com.

Expert Agent Selection

Expert Agent Selection (EAS) is a skill-based routing feature that reduces the call transfer and call holding time by matching caller needs with agent skills.

When **EAS** is set to y, Communication Manager associates each phone with an agent login ID, which is an extension in the dial plan, and not with a skill hunt group. Hence, when an agent logs in, Communication Manager associates the phone with all the skill hunt groups that a system administrator assigns to the agent login ID.

Using Call Center Elite an administrator can assign up to 120 skills to an agent. The administrator can set the call handling preference, that is, administer distribution of calls with the greatest need before skill level under call surplus conditions. Conversely, staffed agents can be moved to handle calls under agent surplus conditions. Agent occupancy and the administered skill levels determine which agents handle calls under agent surplus conditions.

EAS supports a Direct Agent Calling (DAC) capability that a caller can use to speak with a specific agent. Communication Manager prioritizes and delivers a direct agent call before a skill hunt group call. Communication Manager receives the call as an ACD call but delivers or queues the call to the agent and not to a skill hunt group.

For more information, see *Avaya Aura® Call Center Elite Feature Reference* on the Avaya Support website at http://support.avaya.com.

Multisite Best Service Routing

Multisite Best Service Routing (BSR) is a virtual routing feature that ensures efficient use of network resources by comparing local and remote skills for call routing to the resource that can provide the best service.

Agents that share a common skill set are part of a single virtual pool where Communication Manager routes calls based on the administered agent selection criteria and the distribution algorithms regardless of the agent location.

Location Preference Distribution is another Call Center Elite feature that is quite popular in addition to the traditional Avaya Virtual Routing settings of Multisite BSR and Look Ahead Interflow (LAI).

Virtual routing builds on the LAI feature to route calls to the best skill. Communication Manager uses a series of **consider** vector steps to determine the best skill and interflows the call using the **queue-to best** or **check best** vector commands.

For information about vector steps and vector commands, see *Programming Call Vectoring Features in Avaya Aura® Call Center Elite* on the Avaya Support website at http://support.avaya.com.

In a call surplus condition, Communication Manager treats a skill as best if the skill has the shortest Expected Wait Time (EWT). In an agent surplus condition, the administered **Available Agent Strategy** field on the Communication Manager server which receives the call determines the best skill for handling the call or work item.

For more information, see *Avaya Aura® Call Center Elite Feature Reference* on the Avaya Support website at http://support.avaya.com.

Increase in the number of trunks that can be measured

In this release, the number of trunks that can be measured is increased from 12,000 to 24,000.

Increase in the Agent-Skill Pair Limit

In this release, the agent-skill pair limit is increased from 100,000 to 360,000 on a single instance of Communication Manager. Using the increase in the logged-in agent-skill pair limit you can assign more skills to existing logged in agents.

L24 language support based on Switch-Processor Interface enhancement

In this release, Switch-Processor Interface (SPI) is enhanced to upgrade the language support to L24. The L24 enhancement provides the addition of future capacity increases and features while still supporting all previous features.

Support for 2000 Communication Manager locations

SPI language 24 supports 2000 locations and Communication Manager 7.0 supports SPI L24. Therefore, Communication Manager locations supported by Call Center Elite are increased from 250 to 2000.

Detect and log out unreachable SIP Call Center Elite agents and stations

Detect and log out unreachable SIP Call Center Elite agents

When you set **Enable SIP Agent Reachability** to y on the System-Parameter Features screen, Communication Manager polls SIP endpoints for monitoring the reachability of logged in Call Center Elite SIP agents. Communication Manager polls SIP endpoints in either a default 5 minute window or a window based on a user-defined interval. If Communication Manager does not receive a response from the SIP endpoint, the state of the Call Center Elite agent is changed to the AUX work mode with an optional reason code. To determine that the problem is not a short term one, Communication Manager continues to poll the SIP endpoint at a faster interval. If the SIP endpoint fails to respond based on the administered parameters, Communication Manager logs out this agent.

Detect and log out unreachable SIP stations

Similarly, the reachability function can also be extended to domain-controlled SIP stations. The domain-controlled reachability monitoring is independent of the agent reachability monitoring and does not require an agent to be staffed. Communication Manager uses domain-controlled reachability to send the station reachability information to CTI applications that need to track the status of this station. You can enable or disable the domain-controlled reachability at the system level on the System-Parameter Features screen using the **Enable Reachability for Station Domain Control** setting. You can also administer domain-controlled reachability on a station-by-station basis on the Station screen using the **Enable Reachability for Domain Control SIP Stations** setting.

Support for setting the Call Prompting time-out period to 2 seconds

The Call Prompting time-out period is set to 10 seconds by default. This time-out period can be changed to a value between 2 to 10 seconds using the **Prompting Timeout** field on the Feature-Related System Parameters screen.

Caution:

Avaya recommends that you do not set the time-out period to less than 4 seconds, except in special cases. If the time-out is set to less than 4 seconds, the short time-out can cause the caller to miss entering the next digit in a sequence. The caller can miss entering the next digit in a sequence if the caller is unaware that the digits must be entered quickly. The setting of this timer is system-wide and affects digit entry for all collect digits steps in all vectors.

Support for Service Observing Whisper Coaching

Using Service Observing Whisper Coaching, a service observer can talk to the agent while a call is connected without being heard by the caller. Service Observing Whisper Coaching improves agent training and performance because a supervisor using Service Observing can coach the agent by whispering advice to the agent. Customers cannot hear the advice that the supervisor provides to the agent. Supervisors can coach only in the following scenarios:

- The supervisor is Service Observing an ACD agent in the Listen-Only or Listen & Talk modes and not in the No-Talk mode.
- The supervisor is Service Observing an active call, which is not in a conference or on-hold.

In case of a Vector Directory Number (VDN) observing, the supervisor can coach only when the call connects to a local ACD agent. You can have more than one observer for a call, but only one observer can provide coaching.

Addition of the Attribute field in the Agent LoginID screen

In this release, a new field named **Attribute** is added to the Agent LoginID screen. The **Attribute** field is an alphanumeric field that can be left blank or contain up to 20 characters. The content of the **Attribute** field is sent to CMS. Call Center Elite customers can enter a character string that represents a combination of characteristics of that agent defined by the call center management for use in reporting.

Changes to the **Attribute** field on the Agent LoginID screen are reflected only after agents log out and log back in.

Support for Avaya Aura® Media Server

Call Center Elite uses Avaya Aura® Media Server (Avaya Aura® MS) to provide IP audio capabilities similar to legacy H.248 media gateways or port networks with media processors.

Avaya Aura® MS is a software-based media application platform. Avaya Aura® MS is scalable and supports clustering or high availability.

Call Center Elite agents and supervisors can hear zip tone, VDN of Origin Announcements, and warning tones from Avaya Aura® MS instead of VAL boards and Communication Manager media gateways. You can use Avaya Aura® MS to play recorded announcements to customers. Call Center Elite supports a mix of Avaya Aura® MS, VAL boards, and Communication Manager media gateways to provide IP audio capabilities.

Call Center Elite administrators can easily program call vectoring because they do not need to know whether Avaya Aura® MS or a media gateway is providing the announcement, collect digits, and other vector commands that depend upon media capture or playback. To administer announcements, administrators only need to populate information on the system administration screens with which the administrators are familiar. Avaya Aura® System Manageris the preferred method of uploading and administering announcements on Avaya Aura® MS.

Avaya Aura® MS uses a software platform to provide channels for compliance recording products and therefore does not require a media gateway for compliance recording.Avaya Aura® System Manager

Appendix A: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) if any software update. For example, a PCN must accompany a service pack or a update that must be applied universally.Avaya issues product-support notice (PSN) when there is no update, 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 work around 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 **DOCUMENTS**.
3. On the 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 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 Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to the Avaya Support Web Tips and Troubleshooting: E-Notifications 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

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W