What's New in Avaya Aura® Release 7.0.1

Release 7.0.1
Issue 2
August 2016

© 2015-2016, Avaya, Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” 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, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” 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 is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For

Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or 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

The following applies if the product is deployed on a virtual machine. 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: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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: https://support.avaya.com or such successor site as designated by Avaya.

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: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://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: https://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 Avaya Aura® 7.0.1 components.

This document is intended for the following audience:

- Contractors
- Employees
- Channel associates
- Remote support
- Sales representatives
- Sales support
- On-site support
- Avaya Business Partners

Avaya Aura® 7.0.1 components

Product component	Release version
Appliance Virtualization Platform	7.0.1
Communication Manager	7.0.1
Session Manager	7.0.1
System Manager	7.0.1
Branch Gateway	7.0.1
Presence Services	7.0.1
Application Enablement Services	7.0.1
Call Center Elite	7.0.1
Utility Services	7.0.1

Table continues…

Product component	Release version
Communication Manager Messaging	7.0
Avaya Media Server	7.7.1
WebLM	7.0.1

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.

Chapter 2: Avaya Aura® Virtualized offers

Starting with Release 7.0, Avaya Aura® supports the following two Avaya virtualization offers based on VMware:

- Avaya Aura® Virtualized Appliance (VA) - Avaya-provided server, Avaya Appliance Virtualization Platform, based on the customized OEM version of VMware® ESXi 5.5.
- Avaya Aura® Virtualized Environment (VE) - Customer-provided VMware infrastructure

The virtualization offers, provides the following benefits:

- Simplifies IT management using common software administration and maintenance.
- Requires fewer servers and racks which reduces the footprint.
- Lowers power consumption and cooling requirements.
- Enables capital equipment cost savings.
- Lowers operational expenses.
- Uses standard operating procedures for both Avaya and non-Avaya products.
- Deploys Avaya Aura® virtual products in a virtualized environment on Avaya provided servers or customer-specified servers and hardware.
- Business can scale rapidly to accommodate growth and to respond to changing business requirements

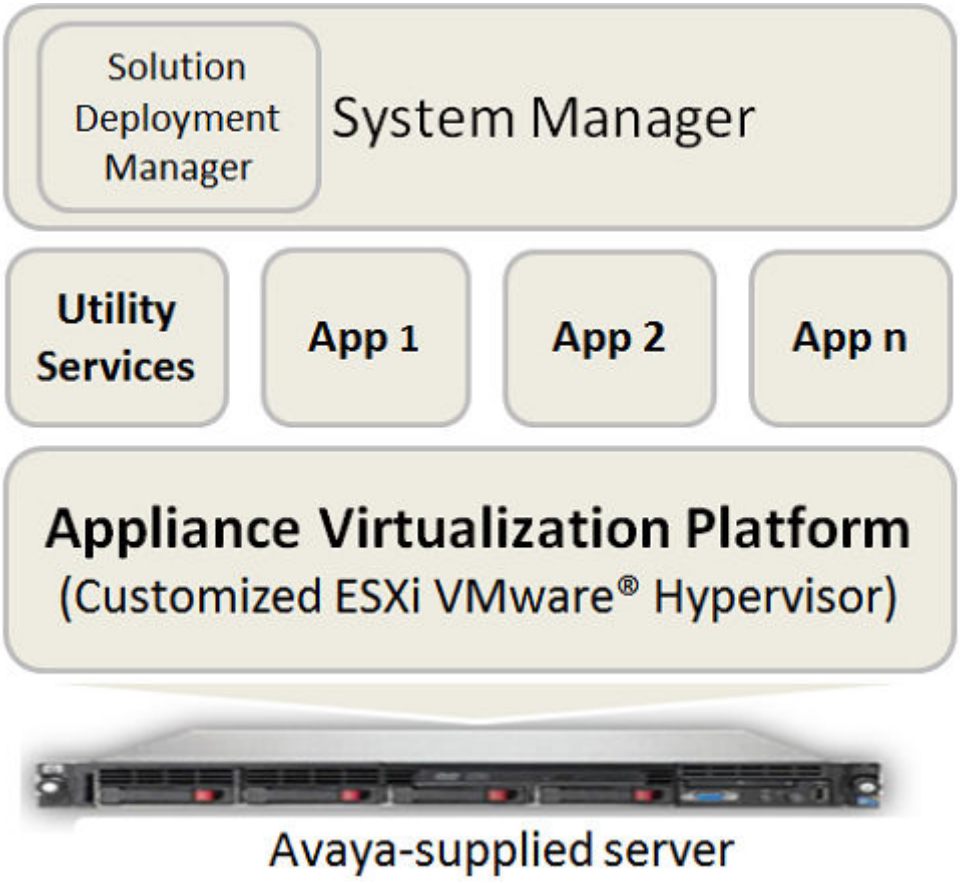
Appliance Virtualization Platform overview

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

Avaya Aura® Virtualized Appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, HP ProLiant DL360 G7, HP ProLiant DL360p G8, Dell™ PowerEdge™ R630, and HP ProLiant DL360 G9
- 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.



From Release 7.0, Appliance Virtualization Platform replaces System Platform.

Avaya Aura® Release 7.0.1 supports the following applications on Appliance Virtualization Platform:

- Utility Services 7.0.1
- System Manager 7.0.1
- Session Manager 7.0.1
- Branch Session Manager 7.0.1
- Communication Manager 7.0.1
- Application Enablement Services 7.0.1
- WebLM 7.0.1
- Avaya Breeze™ 3.1.1
- SAL 2.5
- Communication Manager Messaging 7.0
- Avaya Aura® Media Server 7.7.0.292 (SP3)
- Avaya Scopia® 8.3.5
- Avaya Proactive Contact 5.1.2

For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

Solution Deployment Manager overview

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

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

Note:

In Release 7.0.1, Solution Deployment Manager does not support migration of Virtualized Environment-based 6.x applications to Release 7.0.1 in customer Virtualized Environment. Use vSphere Client to migrate to customer Virtualized Environment.

Release 7.0 and later supports a standalone version of Solution Deployment Manager, the Solution Deployment Manager client. For more information, see *Using the Solution Deployment Manager client*.

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

System Manager with the Solution Deployment Manager runs on:

- Avaya Aura® Virtualized Appliance: Contains a 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, VMware® certified hardware.

With Solution Deployment Manager, you can perform the following operations in Virtualized Environment and Avaya Aura® Virtualized 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 that is running on the Avaya Aura® Virtualized Appliance.

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Refresh applications and associated devices, and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade Avaya Aura® applications.
- Install software patch, service pack, or feature pack on Avaya Aura® applications.

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 7.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

Related links

Solution Deployment Manager client on page 14

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.

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 64-bit, Windows 8 64-bit, and Windows 10 64-bit.

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Avaya appliances and Virtualized Environment.
- Upgrade System Platform-based System Manager.
- Install System Manager software patches, service packs, and feature packs.
- Install Appliance Virtualization Platform patches.
- Restart and shutdown the Appliance Virtualization Platform host.
- Start, stop, and restart a virtual machine.
- Change the footprint of Avaya Aura® applications that support dynamic resizing. For example, Session Manager and Avaya Breeze™.

Note:

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

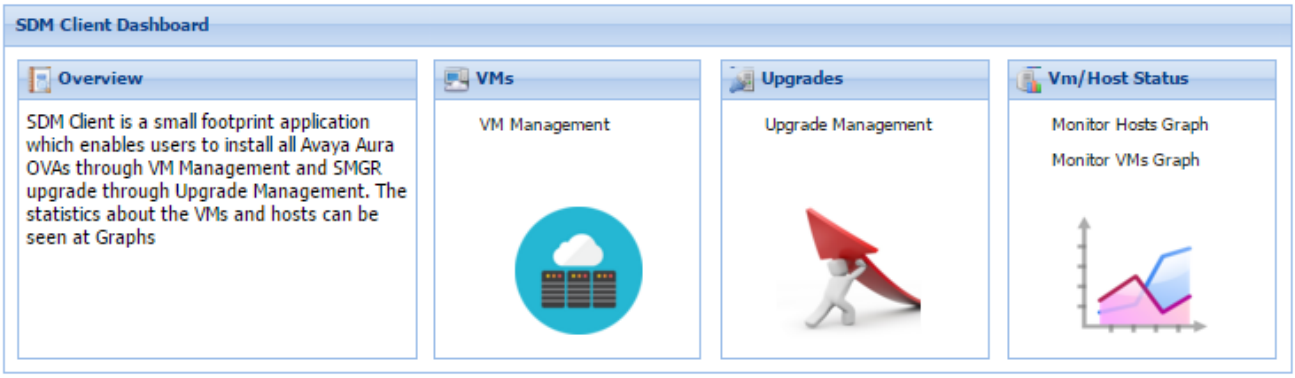


Figure 1: Solution Deployment Manager client dashboard

Related links

Solution Deployment Manager overview on page 13

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® applications in Release 7.0.1:

- Utility Services 7.0.1
- System Manager 7.0.1
- Session Manager 7.0.1
- Branch Session Manager 7.0.1
- Communication Manager 7.0.1
- Application Enablement Services 7.0.1
- WebLM 7.0.1
- Avaya Breeze™ 3.1.1
- SAL 2.5
- Communication Manager Messaging 7.0
- Avaya Aura® Media Server 7.7.0.292 (SP3)
- Avaya Scopia® 8.3.5
- Avaya Proactive Contact 5.1.2

  For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

Note:

You must deploy the Release 7.0 OVA, and then install the Release 7.0.1 file on the Avaya Aura® Release 7.0 application.

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

- Linux-based Communication Manager 5.x and the associated devices, such as Gateways, TN boards, and media modules.

  Note:

  In bare metal Linux-based deployments, the applications are directly installed on the server and not as a virtual machine.

- Linux-based Session Manager 6.x
- 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

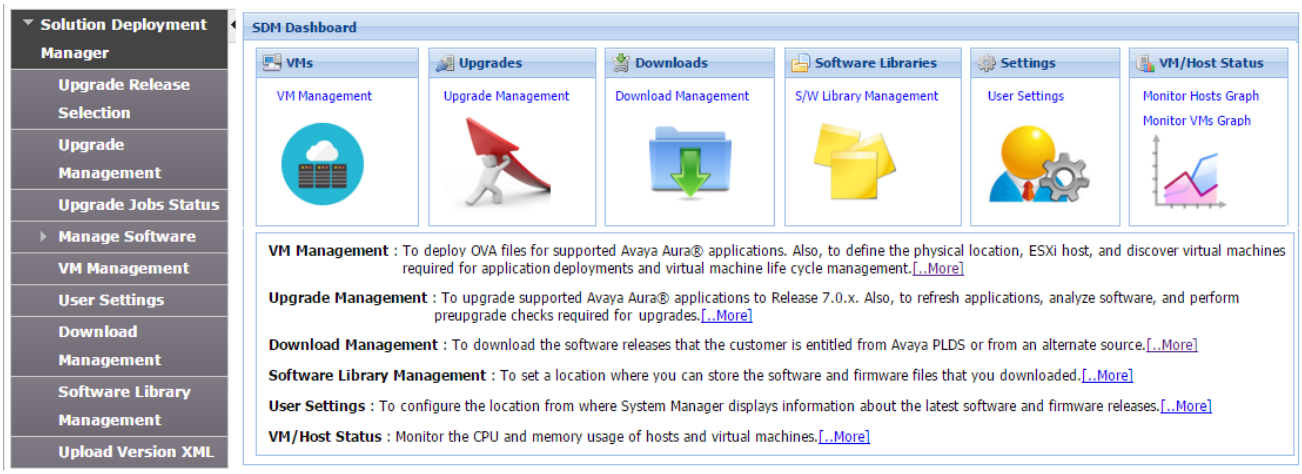
Note:

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

The centralized deployment and upgrade process provide better support to customers who want to upgrade their systems to Avaya Aura® Release 7.0.1. 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 7.0.1 is the default upgrade target.
- **Manage Software**: To upgrade IP Office.
- **VM Management**: To deploy OVA files for the supported Avaya Aura® application.
- **Upgrade Management**: To upgrade Communication Manager that includes TN boards, media gateways and media modules, Session Manager, Communication Manager Messaging, Utility Services, Branch Session Manager to Release 7.0.1.
- **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 and firmware 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.
- **Upload Version XML**: To save the `version.xml` file to System Manager. You require the `version.xml` file to perform upgrades.

Avaya Aura® applications upgrade

With System Manager Solution Deployment Manager, you can upgrade the following Avaya Aura® applications to Release 7.0.1:

- Communication Manager
- Session Manager
- Branch Session Manager

- Utility Services

Note:

You must upgrade System Manager to Release 7.0.1 by using the Solution Deployment Manager client before you upgrade the Avaya Aura® applications to Release 7.0.1.

Support for Common Server 3.0

In the Avaya Aura® Virtualized Appliance offer, Avaya Aura® Release 7.0.1 supports common server Release 3.0, that includes Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9.

Support for VMware ESXi 6.0

Avaya Aura® Release 7.0.1 supports deployment and upgrades on VMware ESXi version 6.0 in customer Virtualized Environment offer.

Chapter 3: What's new in Appliance Virtualization Platform

This chapter provides an overview of the new features and enhancements for Avaya Aura® Appliance Virtualization Platform Release 7.0.1.

Related links

What's new in Appliance Virtualization Platform on page 19

What's new in Appliance Virtualization Platform

Appliance Virtualization Platform Release 7.0.1 supports the following new features and enhancements:

- Deployment and upgrades on Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9 common servers.
- Install the Appliance Virtualization Platform patch from the ESXi host CLI.
- Remove the Appliance Virtualization Platform patch from the ESXi host CLI.
- Enable and disable SSH on the Appliance Virtualization Platform host from CLI and Solution Deployment Manager.
- Solution Deployment Manager checks the origin and validity of certificates of Appliance Virtualization Platform hosts for TLS connections
- Reset and shutdown the Appliance Virtualization Platform host from CLI and Solution Deployment Manager.

Related links

What's new in Appliance Virtualization Platform on page 19

Chapter 4: What's new in Utility Services

This chapter provides an overview of the new features and enhancements for Avaya Aura® Utility Services 7.0.1.

New plugin support on Utility Services

Utility Services supports a plugin mechanism for upgrade from Release 7.0 to later releases.

Solution Deployment Manager in System Manager needs to record information of existing application and virtual machine while the upgrade is in process. Types of information recorded are:

- IP address
- Networking information
- Configuration information
- File settings for the application

Note:

The plugin does not record and provide admin user names and passwords and System Manager enrollment password.

Solution Deployment Manager uses key value pair to access the output information from the plugin and helps automatically deploy the new virtual machine.

For more information, see *Upgrading Avaya Aura® System Manager to Release 7.0.1*.

Out of Band Management

Out of Band Management is a physically and logically separate network connection. It connects to a customer's private IT management network and provides for secure management and administration of Avaya products.

From Utility Services Release 7.0.1, you can activate out-of-band management even after deployment.

Utility Services Release 7.0.1 and later support a full out of band management configuration. Therefore, you can deploy Utility Services with two IP addresses and split the user and management traffic to different Ethernet interfaces on different IP networks.

When Utility Services is set for out of band management, the following services are allocated for full or Utility Services-only mode:

Application	Interfaces for traffic
Phone firmware download	Public
Phone settings file	Public
Gateway firmware download	Public
DHCP Server	Public
Myphone User	Public
SSH	Out of Band Management / Services
Myphone Admin	Out of Band Management
CDR connection to CM	Out of Band Management
Main admin web pages	Out of Band Management / Services
Alarm source	Out of Band Management
SAL connection (SSH, HTTP)	Out of Band Management

When Utility Services is set for out of band management, the following services are allocated for services port-only mode:

Application	Interfaces for traffic
SSH	Out of Band Management / Services
Alarm source	Out of Band Management
SAL connection (SSH, HTTP)	Out of Band Management
Main admin web pages	Disabled
Phone firmware download	Disabled
Gateway firmware download	Disabled
Phone settings	Disabled
Gateway firmware download	Disabled
DHCP Server	Disabled
Myphone Server	Disabled
CDR connection to CM	Disabled
Myphone admin	Disabled

Note:

If a network is not mentioned for service when Out of Band Management is enabled, the service must be disabled on that interface.

Chapter 5: What's new in System Manager

This chapter provides an overview of the new features and enhancements of System Manager Release 7.0.1.

What's new in System Manager

Avaya Aura® System Manager Release 7.0.1 supports the following new features and enhancements:

- Supports Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9 common servers in Avaya appliance offer.
- Supports deployment of Avaya Aura® applications on ESXi 6.0 in the customer Virtualized Environment offer
- Enhancements to Solution Deployment Manager dashboard
- Enhancements to VM Management:
  - Enable and disable SSH on Appliance Virtualization Platform
  - Wizard-based VM deployment page
  - Real time data update of license status of hosts, certificate validity, and the state of virtual machines
  - Configure a Network Time Protocol (NTP) server for a host.
  - Reset and shutdown the Appliance Virtualization Platform host
  - View the job history of operations that are performed on VM Management
- Use of non-local vCenter administration log in with Solution Deployment Manager.

  System Manager Solution Deployment Manager and Solution Deployment Manager client user can log in to vCenter to authenticate to an external Active Directory Authentication server. The new authentication option enables customer who do not allow vCenter local logon credentials to vCenter to use the services and functionality that Solution Deployment Manager provide. The feature also enables the Avaya management tools to be compliant with customer security requirements.
- Upgrade Management enhancements:
  - Save and edit upgrade configuration

- Upgrade Avaya Aura® applications directly to Release 7.0.1 by using Solution Deployment Manager.
- Clean up the current pending or pause state of applications during upgrade.
- Patch installation workflow enhancements:
  - Enhancements to the workflow when uploading hot fixes, patches, service pack, and feature packs for Aura 7 application into the defined software library. When a customer does not use or permit direct connection to Avaya PLDS, you require additional manual steps to upload the software in the software library. The new workflow eases the file upload and eliminates the use of CLI to move files.
  - With the new custom patch deployment process, advanced administrative users can install software, such as software patch, service pack, or a feature pack, to an Avaya Aura® application. The new custom patch deployment option does not use the System Manager automation and analysis functions, so that advanced administrators can fully control the deployment of hot fixes, patches, service pack, and feature packs.

    You can install custom patches for the following Avaya Aura® applications:

    - Communication Manager
    - Session Manager
    - Branch Session Manager
    - Utility Services
    - Communication Manager Messaging
    - WebLM

- Flexibility to select application and data port numbers during the Solution Deployment Manager client installation.
- System Manager upgrade management:
  - Upgrade System Manager directly to Release 7.0.1 by using the System Manager upgrade manager on the Solution Deployment Manager client.
- Geographic Redundancy enhancements:
  - The same server construct requirement at the primary and secondary System Manager system is removed. You can use System Manager in a Geographic Redundancy configuration in a shared or standalone mode. For example, Common Server Release 2.0 Large at the primary site with a mix of Avaya Aura® applications and Common Server Release 2.0 Medium at the secondary site with a different mix of Avaya Aura® applications.

    Note:

    The Resource Profile and the System Manager software release must be the same at both locations.

    With this flexibility, you can maximize the deployment of Avaya Aura® 7.x applications on Avaya-provided appliances, eliminate the requirement to have System Manager running standalone when deployed in a Geographic Redundancy setup, and use several combinations of server constructs.

- End User Self Provisioning enhancements:
  - Change password for SIP Communication profile, CM Station profile, and Messaging profile
  - Support local or external LDAP for authentication
  - Support the following LDAP applications for authentication:
    - Active Directory 2003, 2008, and 2012
    - OpenLDAP 2.4.21
    - IBM Domino 7.0
    - Novell eDirectory 8.8
    - SunOne Directory and Java System Directory 6.3
- Support for the following web browsers:
  - Microsoft Internet Explorer Release 11.x
  - Mozilla Firefox Release 40, 41, and 42
- SIP users and devices enhancements:
  - Scale increased to support 500 instances of Branch Session Manager
- Support for the following:
  - CallrId and K2500 Analog Phone types from the System Manager Endpoint management and User Management interfaces

    CallrId and K2500 default phone templates that can be used during Communication Manager endpoint administration. The feature is used to support customers with Avaya Integrated Management applications.

    Customers in hospitality, universities, and medical applications who still use CallrId and K2500 Phone types can now use System Manager to support these set types.
  - Add and remove Agent Skill from the SIP phone
  - Hunt group busy position button for 96x1 SIP phones in a non-Contact Center Environment
- System Manager and Communication Manager administrator connection optimization: Enhancement to establish and maintain connections between System Manager and Communication Manager during the Communication Manager administration by pooling Communication Manager connections. You can configure connection pools and view the connection usage.

  With System Manager and Communication Manager connection pooling, an administrator can establish dedicated or pinned connections between System Manager and Communication Manager with the associated management for creating, deleting, and viewing the status of connection pools.

  You can define:

  - 40 pinned connections across all Communication Manager systems for System Manager Release 7.0.1 Profile 1 and Profile 2

- 60 pinned connections across all Communication Manager systems for the high capacity System Manager Release 7.0.1 Profile 3

With connection pooling you can ensure that an administrative session from System Manager to a specific Communication Manager is always available. Communication Manager has a limit of 22 ports. With connection pooling, you can maximize the Communication Manager port usage when using System Manager.

- Support for Avaya Aura® Device Services as an adopter. With Avaya Aura® Device Services, clients and endpoints can store centrally and retrieve data such as configuration and deployment data. You can manage the data from any device.

  Avaya Aura® Device Services supports the following services for devices:

  - Contact Services includes Directory Service, User Service, Picture Service
  - Notification Service
  - Dynamic Configuration Service
  - Web Deployment Service
- Avaya Aura® Device Services: Support for off-pbx-telephone feature-name-extensions in Communication Manager Sync.

Certification validation

With System Manager Solution Deployment Manager and Solution Deployment Manager client, you can enable a certificate-based TLS connection between the Solution Deployment Manager service and a host that is running Avaya Aura® 7.x applications. This enables to establish secure communications between System Manager Solution Deployment Manager or the Solution Deployment Manager client and Appliance Virtualization Platform or ESXi hosts.

The certificate-based sessions apply to the Avaya Aura® Virtualized Appliance offer using host self-signed certificates and the customer-provided Virtualization Environment using host self-signed or third party certificates.

You can check the following with certificate based TLS sessions:

- Certificate valid dates
- Origin of Certificate Authority
- Chain of Trust
- CRL or OCSP state
- Log Certificate Validation Events

Solution Deployment Manager checks the certificate status of hosts. If the certificate is incorrect, Solution Deployment Manager does not connect to the host.

For the correct certificate:

- The fully qualified domain or IP address of the host to which you are connecting must match the value in the certificate and the certificate must be in date.

- Appliance Virtualization Platform and VMware ESXi hosts do not automatically regenerate their certificates when host details such as IP address or hostname and domain changes. The certificate might become incorrect for the host.

If the certificate is incorrect:

- For the Appliance Virtualization Platform host, Solution Deployment Manager regenerates the certificate on the host and then uses the corrected certificate for the connection.
- For the VMware ESXi host or vCenter, the system denies connection. The customer must update or correct the certificate on the host or vCenter.

  For more information about updating the certificate, see "Updating the certificate on the ESXi host from VMware".

Note:

Solution Deployment Manager:

- Validates certificate of vCenter
- Does not validate certificates for hosts that vCenter manages

With Solution Deployment Manager, you can only accept certificate while adding vCenter. If a certificate changes, the system gives a warning that the certificate does not match the certificate in the trust store on Solution Deployment Manager. You must get a new certificate, accept the certificate as valid, and save the certificate on the system.

To validate certificates, you can directly log on to the host and confirm that the details in the `/etc/vmware/ssl/rui.crt` file match the details displayed on the screen.

Bulk import and export enhancements

System Manager provides the following bulk import and export enhancements:

- An option to export user data by using Excel or XML files.
- Time zone field for Avaya Aura® Messaging subscribers.

  The value must be in the standardized name format. For example, America/Phoenix. Otherwise, the system sets the Avaya Aura® Messaging subscriber time zone to the System Manager server time zone.

Avaya Aura® Device Services element

System Manager supports Avaya Aura® Device Services as an element.

With Avaya Aura® Device Services, clients and endpoints can store centrally and retrieve data such as configuration and deployment data. You can manage the data from any device.

Avaya Aura® Device Services supports the following services for devices:

- Contact Services: The service provides the following end user-focused services that are centrally located:
  - Directory Service: Manages your contacts from any of your devices. Performs an enterprise search of existing sources of contacts such as System Manager through PPM, and exchange local contacts, enterprise directory.

    Only a provisioned user can use Contact Services.
  - User Service: Sets and retrieves information such as your preferred names, picture, and other preferences.
  - Picture Service: Supports creating (overrides default enterprise), deleting, and updating a picture of user and provides a centralized, firewall-friendly interface to present picture URLs in the contact information or search results.
- Notification Service: Provides a common infrastructure for a client or endpoint to subscribe to receive events from a number of service resources with a single connection.
- Dynamic Configuration Service: Provides discovery of configuration settings to UC Clients that can be customized on a global, group, individual or platform basis. This simplifies the configuration process of users, and skips manual configuration and makes ready for use. Clients only need to only provide identity information such as email address or Windows userid and enterprise credentials.
- Web Deployment Service: Supports publishing and deploying UC client updates for end users.

Chapter 6: What's new in Session Manager

The following sections describe the new features and enhancements for Avaya Aura® Session Manager Release 7.0.1.

Session Manager and Avaya Aura® Device Services integration

Avaya Aura® Device Services overview

Avaya Aura® Device Services (AADS) provides a set of services to Avaya Aura® Communicator 3.0. AADS is co-resident with Session Manager 7.0.1. and is delivered as a separate OVA.

The following services are provided when using AADS with Avaya Aura® Communicator 3.0:

- **Contact:** To use the Contact service, a user must be a provisioned user on LDAP Server. Using the contact service, you can:
  - Manage the contact detail from any device.
  - Perform an enterprise search of existing sources of contacts, such as, exchange local contacts, and enterprise directory that is also known as the Directory service.
  - Set and retrieve information, such as, preferred names, picture, and preferences. Using the Picture service, you can create and override, delete, and update the picture of a user. This also provides a centralized, firewall-friendly interface to include these picture urls in the contact information or search results.
- **Notification:** The Notification service provides a common infrastructure that allows a client or endpoint to subscribe to receive events from a number of service resources using a single connection.
- **Dynamic Configuration:** The Dynamic Configuration service provides discovery of configuration settings to UC Clients. You can customize these settings on a global, group, individual, or platform basis. The Dynamic Configuration service uses the automatic configuration feature of Avaya Communicator 3.0 to facilitate the configuration details to the UC clients. This helps the user to avoid manual configuration of their client. To log in to the client, the user needs to enter their credentials, such as, email address or Windows user id, along with their enterprise credentials.

The Dynamic Configuration service is supported on the following Avaya Communicator Release 3.0 devices:

- Avaya Communicator for Android
- Avaya Communicator for iOS
- Avaya Communicator for Mac
- Avaya Communicator for Windows

- **Web Deployment:** The Web Deployment service publishes and deploys the UC client updates to the devices of the end users. The Web Deployment service is supported on the following devices of the Avaya Communicator Release 3.0:
  - Avaya Communicator for Mac
  - Avaya Communicator for Windows

Cassandra clustering and data replication overview

With Session Manager Release 7.0.1, if the **Enable Data Storage Cluster** field on the Session Manager Administration page is selected, Session Managers are added to the Cassandra database cluster. Each Cassandra is running in a cluster of 1 node and there are N clusters, where N is the number of Session Managers.

The Cassandra nodes are configured to have a single cluster of Cassandra nodes. If the **Enable Data Storage Cluster** field is not selected, all the Cassandra nodes run in standalone mode.

Cassandra clustering is done only when Avaya Aura® Device Services (AADS) servers are configured and paired with Session Manager.

Cassandra data distribution uses the administration on the User Data center page to identify the Session Manager instances that are within the same datacenter.

For administering Cassandra data distribution:

1. Enable data storage clustering.
2. Create a data center.
3. Assign co-located Session Managers to the data center.
4. Add the AADS instance to the inventory.
5. Pair a Session Manager instance with an AADS node.

Add/remove skill button

Add/remove skill button

From Release 7.0.1, Personal Profile Manager (PPM) supports download of an assigned add/remove skill button on 96x1 SIP phone when the phone registers to Session Manager.

Agents or supervisors can use add/remove skills button to add or remove an assigned skill.

Communication Manager prompts the agent while adding or removing a skill and displays the updated set of skills.

For more information about Add/remove skill button, see *Avaya Aura® Call Center Elite Feature Reference*.

Hunt Group Log in/Log out button for SIP phones in a non-CC Environment

When the Unified Communications (UC) users in customer configurations are members of a department hunt group, they need to log in and out of the hunt group and see a visual indication of their status.

With Release 7.0.1,Session Manager has a Hunt Group Log in/Log out button, with which you can:

- Log in and out from receiving calls distributed in a hunt group.
- Activate or deactivate the feature with a single button click by using the Hunt Group Log in/Log out toggle-button.
- See the status of feature activation. A visible indicator is available to show the status, whether the feature is turned on or off.

For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

TLS mutual authentication for SIP endpoints

Session Manager provides validation of the endpoint Transport Layer Security (TLS) certificate. This authentication is applicable to SIP and HTTP traffic.

From Release 7.0.1, Session Manager provides the ability for administrators, while authenticating SIP devices, to choose the following:

- No Mutual Authentication
- Optional Mutual Authentication
- Mandatory Mutual Authentication

The **TLS Endpoint Certificate Validation** field has three options:

- **None**: No mutual authentication occurs. There is no certificate validation and SIP endpoint can establish the connection.
- **Optional**: Communication occurs if the endpoint presents a valid certificate or otherwise.

- **Required**: Communication occurs only if the endpoint presents a valid certificate trusted by Session Manager.

The default setting for the upgrades, as well as new installations, is optional mutual authentication. You can decide to change the setting to no or mandatory mutual authentication. If you select mandatory mutual authentication for the **TLS Endpoint Certificate Validation** field, Session Manager rejects the connection request if:

- a client does not provide a certificate or,
- the client certificate is invalid or not trusted by Session Manager.

Note:

If you select the **Required** option for Pre 7.0.1 Session Manager, it results to the **Optional** option to support backward compatibility.

Implementation of the new TLS validation policy supports network configuration of Session Manager 7.0 and later with the earlier versions of Session Manager or Branch Session Manager.

Chapter 7: What's new in Communication Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® Communication Manager 7.0.1.

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

Opus Codec for Inter-Gateway calls

The calls involving media gateways and media servers now supports Opus codec, an open source audio-codec. This feature is limited to inter-gateway and inter-media server calls where the media resource of each gateway or media-server is used to connect the call between the two gateways or media-servers.

Hunt Group Busy Position Button

The **Hunt Group Busy position (hntpos-bsy)** button facilitates non-ACD hunt group users to voluntarily opt-in or opt-out of hunt group calls. Currently, similar behavior can be achieved by **aux-work** button only on H.323 endpoints. Aux-work works with both ACD and non-ACD hunt. This new button is implemented for 96x1 SIP endpoints.

Streaming Music On Hold from an external source

Communication Manager can be configured to source music from Avaya Aura® Media Server (MS). The Avaya Aura® Media Server (MS) is associated with external or remote servers and hosts media files using the new **Live Streaming Audio** feature. The external source can be an Internet source or a central server the announcement files are stored.

Support for Opus codecs

Communication Manager Release 7.0.1 supports Opus codec for SIP calls. Following Opus-codec sets are supported in the current release:

- OPUS-NB12K
- OPUS-NB16K
- OPUS-WB20K
- OPUS-SWB24K

Enhanced interaction between Coverage Answer Group and Call Pickup Group

With Communication Manager Release 7.0.1, a new **Call Pickup for call to Coverage Answer Group** field is introduced. When the default value of this field is set to n and a call rings at a Coverage Answer Group member, Communication Manager does not trigger call pickup alerting if the Coverage Answer Group member is part of a Call Pickup group. This is applicable for the H.323, DCP, Analog, and SIP endpoints.

MLPP support for Precedence Calling to SIP endpoints

With Communication Manager Release 7.0.1, the MLPP feature now includes dialing precedence calls to 17 SIP endpoints. However SIP endpoints cannot initiate Priority or above precedence calls. SIP endpoints can initiate Routine level calls though.

Multi-country tone support through Avaya Aura® Media Server (MS)

Avaya Aura® Media Server (MS), as a VoIP resource can provide tones as per user location. However, if more than one users are involved in a call from different locations, the system uses the Avaya Aura® MS native location that is configured on the SIP signaling group page.

Commercialization of TLS

With Communication Manager Release 7.0.1, you can use TLS with or without enabling the FIPS mode.

Increased capacity for TLS user

Communication Manager Release 7.0.1 supports 18000 H.323 users when TLS mode is enabled.

Note:

TLS session should be configured to operate in TTS-TLS mode. This is accomplished by going to the **IP Network Region** form and going to the **H.323 Profile** and entering the value of **H323TLS**.

Chapter 8: What's new in Presence Services

This chapter provides an overview of the new and enhanced features of Presence Services Release 7.0.1.

Support for XMPP federation with Openfire

Presence Services Release 7.0.1 supports federation of a Presence Services Release 7.0.1 system with Openfire.

Support for XMPP federation between Presence Services 7.0.1 and Presence Services 6.2.6

Presence Services Release 7.0.1 supports federation of a Presence Services Release 7.0.1 system with a Presence Services Release 6.2.6 system.

Presence domain sharing

Presence Services Release 7.0.1 supports deployment of Presence Services solution that shares the same addressing domain.

Support for Geographic Redundancy

Presence Services Release 7.0.1 supports Geographic Redundancy. This feature enables Presence Services solution to be deployed with both High Availability and clustered solutions in different geographic regions.

Support for Cisco Jabber Federation

Presence Services Release 7.0.1 supports federation with Cisco Jabber enabling the exchange of presence and IM information between users. This feature will only be compatible with Aura endpoints that support true federation.

Upgrade scripts for XCP controller data

Presence Services Release 7.0.1 enables the administrator to maintain the XCP controller data when migrating/upgrading from Presence Services Release 6.2.x to Presence Services Release 7.0.x without the need to manually configure the configuration settings in Presence Services Release 7.0.x.

Support for Note Aggregation

Presence Services Release 7.0.1 provides a mechanism to aggregate the availability description that is sent to endpoints to be delivered along with presence of the user.

Support for forwarding IM traffic to Avaya Multimedia Messaging

Presence Services Release 7.0.1 provides an option to forward all IM traffic to Avaya Multimedia Messaging if an Avaya Multimedia Messaging is deployed as part of the solution.

Support for Common Server

Presence Services Release 7.0.1 supports Common Server Release 3.0.

Support for Interoperability among clients

Presence Services Release 7.0.1 will be compatible with existing Avaya endpoints that are used with Presence Services Release 6.2.x and 7.0. Presence/IM capable devices:

- 96X0 SIP (XMPP IM not supported)
- 96X1 SIP
- OneXC SIP
- OneXC H323
- Avaya Communicator
- Summit (XMPP IM not supported)
- One-X Agent

Non Presence/IM capable devices:

- 96X0 H323
- 96X1 H323

Supported migration paths

The supported migration paths for Presence Services Release 7.0.1 are:

Release	Requirement
5.2.x	Upgrade to 6.x and then upgrade to 7.0.1.
6.0.x	Direct upgrade to 7.0.1.
6.1.x	Direct upgrade to 7.0.1.
6.2.x	Direct upgrade to 7.0.1.
7.0.0.0.x	Direct upgrade to 7.0.1.
7.0.0.1.x	Direct upgrade to 7.0.1.

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 7.0.1.

Application Enablement Services 7.01 OVA for virtualized environment

Application Enablement Services 7.01 OVA VMWare Virtual Appliance offer supports a fresh installation of Application Enablement Services 7.0.1 running on the ESXi 5.x or 6.0 VMM. The OVA may be installed as a virtual machine on a system running VMWare's vSphere version 5.0, 5.1, 5.5 or 6.0 virtualization platform.

Application Enablement Services 7.0.1 ISO for Software-only version

The Avaya-supplied Application Enablement Services ISO will contain the following software:

- Application Enablement Services 7.0 or 7.0.1
- Third-party software for Application Enablement Services
- Customer-provided server hardware and the RHEL 6.5 OS software

Support for Appliance Virtualization Platform 7.0.1 platform

Application Enablement Services 7.0.1 software is deployable on Appliance Virtualization Platform Release 7.0.1.

Bin files as a method for Application Enablement Services deployment

Application Enablement Services 7.0.1 can be deployed over the 7.0 GA version. Application Enablement Services 7.0.1 bin file can be deployed from the Application Enablement Services system command prompt.

Application Enablement Services 7.0.1 Embedded WebLM Server

This feature will provide a local WebLM server to Application Enablement Services for use in an Enterprise-Wide licensing environment.

Support for VMware ESXi 6.0

The virtual appliance offer will be installed as a virtual machine running on VMware ESXi 5.0, 5.1 and 5.5 platforms. However, for Application Enablement Services 7.0.1, support has been expanded to include VMware ESXi 6.0.

Support for SNMP v3

From a security point of view, it is recommended to enable products only with SNMP v3, with authentication and privacy modes. Therefore, SNMP v3 with authentication and privacy modes is now the mandatory requirement for both current and future development for all Avaya products.

Logging Enhancements

Application Enablement Services configuration changes will be logged through Syslog which will enable the changes to be tracked in logs that can be automatically audited by operations. Customers will need to export logs for regular backups. With this capability the exports can be automatic rather than manual. This enables improved manageability and monitoring and will address customer concerns about audit gaps.

Support for Common Server Release 3 (CSR3) hardware

Application Enablement Services 7.0.1 supports CSR3 hardware.

Support of Internet Explorer 9, 10, and 11

Application Enablement Services OAM web pages can now be correctly displayed when using the Internet Explorer Web browser versions 9, 10, and 11.

Chapter 10: What's new in Media Server

The following sections describe the new features and enhancements for Avaya Aura® Media Server Release 7.7.1.

Audio Codecs

The Element Manager (EM) task to configure audio codecs is simplified for easier use. EM enhanced to enable administrators to configure the newly supported Opus codec. Opus is defined by the Internet Engineering Task Force (IETF) in RFC 6716. IETF adds enhanced interactive speech and music transmission capabilities to the media server.

Aurix Speech Search Engine

Avaya Aura® Media Server 7.7 interfaces with Aurix SSE for speech analytics services. These services enable the system to analyze recorded voice by using phonetic speech search technology. After a recording is analyzed and indexed, the speech it contains is searchable. Aurix SSE can also monitor audio streams in real-time by using a specified query set.

Backup using SFTP

Avaya Aura® Media Server 7.7 adds EM and command-line backup tool support for SFTP backup destinations. Previous releases only supported FTP destinations for backups.

Content Store on Standard nodes

Content Store components are enabled by default on cluster servers with the Role designation of Standard. In releases before Avaya Aura® Media Server 7.7, the Content Store component is disabled by default on Standard cluster servers.

Dual unicast monitoring

Avaya Aura® Media Server 7.7 supports Prognosis from Avaya DevConnect Technology Partner, Integrated Research. Prognosis performance management software monitors voice quality, availability and performance in real-time by monitoring the RTCP packets generated by Avaya Aura® MS.

System Manager enrollment

Some Avaya solutions which adopt Avaya Aura® MS use Avaya Aura® System Manager to provide an integrated point of management. You can use Avaya Aura® MS Element Manager (EM) to enroll media servers in Avaya Aura® System Manager.

Enrollment enables Avaya Aura® MS cluster management, single sign-on (SSO), and role-based access control (RBAC) managed by Avaya Aura® System Manager. After enrollment administrators access the Avaya Aura® MS EM using Avaya Aura® System Manager administrative accounts which have permission to use EM.

Chapter 11: What's new in Branch Gateway

This chapter provides an overview of the new features and enhancements for Branch Gateway 7.0.1.

CLI Commands

Two new CLI Commands are introduced in Release 7.0.1:

- **`set allow-unencrypted`**: System administrator can use this command to allow or disallow media encryption requests from Communication Manager.
- **`set link-encryption`**: System administrator can use this command to specify what TLS versions will be offered by the gateway when connecting to a server.

FIPS-mode

FIPS-mode is a feature that is currently not supported in Release 7.0.1 for use by our customers since it is pending FIPS certification by a 3rd-party at this time. It is targeted to be available in a post 7.0.1 release after achieving FIPS certification.

OPUS Codec

The MP120 and MP160 VOIP modules are now capable of supporting the Opus codec in narrowband mode.

Chapter 12: What's new in Call Center Elite

This chapter provides an overview of the new and enhanced features of Call Center Elite Release 7.0.1.

New in this release

New features for Avaya Aura® Call Center Elite 7.0.1:

- Service Observing added on 96X1 SIP agent deskphones.
- Service Observing Whisper Coaching added on H.323, DCP, and 96X1 SIP agent deskphones.
- Support for treating AUX work mode as idle for controlling the agent MIA queue.
- Support for treating adjunct routed calls as ACD calls.
- Support to allow ASAI Single Step Conference calls to ignore Exclusion.

New features for Avaya Aura® Call Center Elite 7.0:

- 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.
- Support for Avaya Aura® Media Server.
- Addition of the **Attribute** field to the Agent LoginID screen.

Support for Service Observing for SIP phones

You can now use Avaya 96X1 SIP agent deskphones to observe a call. Using Service Observing, a call center supervisor can observe agents when agents are on a call. Service Observing is useful for agent training and improving agent performance.

Support for treating adjunct routed calls as ACD calls

In Call Center Elite Release 7.0.1, you can configure adjunct routed calls to be treated as ACD calls. Thereby, adjunct routed calls can also be counted as an ACD call for a skill in reports. You can administer this feature on a per VDN basis. By default, the feature is set to no.

Support for treating AUX work mode as idle for controlling the agent MIA queue

In Call Center Elite Release 7.0.1, you have the option for the Most Idle Agent (MIA) skill queues to consider agents idle while they are in the AUX work mode.

When the agent logs on, the agent is queued if the **AUX Agents Considered Idle (MIA)** field is set to the following parameters:

- `y` on the Agent LoginID screen.
- `system` on the Agent LoginID screen and `y` on the Feature-Related System Parameters screen.

Agent queuing also depends on the value set in the **ACW Agents Considered Idle** field. If the agent was not previously in the queue, agent queuing depends on when the agent enters the AUX work mode.

Chapter 13: Resources

Documentation

The following table lists the documents related to the components of Avaya Aura® Release 7.0.1. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Implementation			
—	*Deploying Avaya Aura® applications from 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 to Release 7.0.1 from System Manager*	Describes the procedures and checklists for upgrading Avaya Aura® applications to Release 7.0.1.	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 7.0.1, 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 7.0.1.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Table continues…

Document number	Title	Description	Audience
—	*Administering Avaya Aura® System Manager*	Describes the procedures for configuring System Manager Release 7.0.1 and the Avaya Aura® applications and systems managed by System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
—	*Avaya Aura® Presence Services Snap-in Reference*	Describes the steps to deploy and configure Presence Services Release 7.0.1.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Using			
	Using the Solution Deployment Manager client	Deploy and install patches on Avaya Aura® applications.	System administrators
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

Table continues…

Course code	Course title
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
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

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

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

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

H

L

M

N

O

P

R

S

T

U

V

W

X