What's New in Avaya Aura® Release 6.2 Feature Pack 2

Release 6.2 Feature Pack 2
May 2013

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

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

Heritage Nortel Software

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

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

Copyright

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

Virtualization

Each virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the end-user customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances 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

Manufacturer's Port Identifier	FIC Code	SOC/ REN/A.S. Code	Network Jacks
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 that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document provides an overview of the new and enhanced features for:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Branch Gateway
- Avaya Aura® Presence Services
- Application Enablement Services
- Avaya Aura® Call Center Elite

Intended audience

This document is for the following audiences:

- Avaya Contractors
- Avaya 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 this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Implementation			
03-603558	Implementing Avaya Aura® Communication Manager	Describes the implementation instructions for Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
18-603644	Implementing Avaya Aura® Communication Manager Messaging	Describes procedures for implementing and configuring CMM 6.2 (embedded).	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administration			
555-233-504	Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network connectivity for Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-300509	Administering Avaya Aura® Communication Manager	Describes the procedures and screens used in administering Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Document number	Title	Description	Audience
—	Administering Avaya Aura® System Manager	Describes the procedures for configuring System Manager and the Avaya Aura® applications and systems that System Manager manages.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
—	Administering Avaya Aura® Call Center Elite	Describes the procedures for configuring Call Center Elite.	Implementation Engineers and System Administrators
—	Configuring V.150.1 on the Avaya G450 Branch Gateway	Describes the procedures to configure V.150.1 on the Avaya G450 Branch Gateway	Implementation Engineers and System Administrators
—	Avaya Aura® Communication Manager Release 6.2 and Radvision Scopia Release 7.7 and 8.0 Interoperability	Describes the steps to set up SIP and H.323 video endpoints.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
—	Administering Avaya Aura® Presence Services	Describes the steps to configure Presence Services.	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 references and detailed field descriptions of Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Document number	Title	Description	Audience
03-603324	Administering Avaya Aura® Session Manager	Describes how to administer Session Manager 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
18-603645	Avaya Aura® Communication Manager Messaging Documentation CD	Describes the documentation set for Avaya Aura® Communication Manager Messaging that includes, General reference, System administration, User information, Maintenance information, and Message Manager Basics card.	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

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
AVA00383WEN	Avaya Aura® Communication Manager Overview
AVA00279WEN	Communication Manager - Configuring Basic Features
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
ATI02348IEN, ATI02348VEN	Avaya Aura® Communication Manager Implementation
AVA00836H00	Communication Manager Basic Administration
5U0041I	Avaya Aura® Communication Manager Administration
AVA00834WEN	Avaya Communication Manager- System Features and Administration
ATC00838VEN	Avaya Media Servers and Gateway Implementation Workshop Labs
AVA00821H00	Avaya CM Architecture and Gateways: H.248, H.323, and Proprietary
5U00104W	Session Manager 6.2 Delta Overview
5U00105W	Avaya Aura® Session Manager Overview
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
ATC01840OEN	Survivable Remote Session Manager Administration
5M00050I, 5M00050IV, 5M00050A	Avaya Aura® Communication Manager Messaging Embedded Administration, Maintenance and Troubleshooting
5U00106W	Avaya Aura® System Manager Overview
5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00103W	Avaya Aura® System Manager 6.2 Delta Overview
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop
AVA00821H00	Avaya CM Architecture and Gateways: H.248, H.323, and Proprietary
ATA01739WEN	Avaya Aura® Application Enablement Services Design
E9U00103O	AES 6.1 GA Knowledge Transfer Recording
ATI02595VEN	Avaya Aura® Application Enablement Services Implementation and Adminstration
9C00385V	Avaya Aura® Application Enablement Services AES Installation, Admin & Maint
ATI02210VEN	Presence Services Overview

Course code	Course title
AUCC100010632	Avaya Aura® Presence Overview

Avaya Mentor videos

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

Go to http://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 site.

Avaya Aura® 6.2 Feature Pack 2 components

Product component	Release version
Communication Manager	6.3.0
Communication Manager Messaging	6.3.0
Session Manager	6.3.2
System Manager	6.3.2
Branch Gateway	6.3.0
Presence Services	6.2.0
Application Enablement Services	6.3.0
Call Center Elite	6.3.0

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.

Warranty

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

Support

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

Chapter 2: Avaya Aura® Suite Licensing

Avaya Aura® Suite Licensing bundles Avaya Aura® features into three offers that can be combined on a per-user basis within an enterprise. Customers purchase the number of licenses they need of each suite based on the communication requirements of the individual users. It provides the flexibility to give each user the level of mobility and collaboration they need.

- Foundation Suite provides all the necessary elements for the Avaya Aura® Core infrastructure for desktop workers — SIP, soft clients, desktop UC integration, and core applications survivability.
- Mobility Suite enables complete enterprise mobility and bring-your-own-device (BYOD) solutions for any employee. In addition to providing Foundation Suite, the Mobility offer includes Avaya Flare® Experience for the iPad, and Avaya one-X® Mobile for SIP, iOS, Android, and Windows smartphones. It also includes Avaya Aura® Messaging and Avaya Session Border Controller for advanced messaging, secure network access and VPN-less secure remote communications.
- Collaboration Suite enables any enterprise to gain full business collaboration using audio, video or the web. This offer adds Avaya Aura® Conferencing 7 to the features of Mobility and Foundation Suites, and a user-based Scopia® desktop and mobile license.

Product	Foundation Suite	Mobility Suite	Collaboration Suite
Avaya Agile Communication Environment™	Y	Y	Y
Avaya Aura® Communication Manager	Y	Y	Y
Avaya Aura® Communication Manager Messaging	Y	Y	Y
Avaya Flare® Experience for PC	Y	Y	Y
Avaya one-X® Communicator	Y	Y	Y
Point-to-point video	Y	Y	Y
Avaya Aura® Presence Services	Y	Y	Y
Avaya Aura® Session Manager	Y	Y	Y
Avaya Aura® System Manager	Y	Y	Y
Avaya Aura® System Platform	Y	Y	Y
Avaya Aura® Messaging	N	Y	Y
Avaya Flare® Experience for iPad	N	Y	Y
Avaya one-X® Mobile	N	Y	Y

Product	Foundation Suite	Mobility Suite	Collaboration Suite
Avaya Session Border Controller	N	Y	Y
EC500 (Extension to Cellular)	N	Y	Y
Avaya Aura® Conferencing 7	N	N	Y
Scopia Desktop/Mobile	N	N	Y

Contact your Avaya Partner or Avaya Account Representative for more information about the new Avaya Aura® Suite Licensing.

Avaya Aura® Release 6.2 products use the Product Licensing and Delivery System (PLDS) for license administration. For more information about PLDS, including training, documentation, and job aids, see http://plds.avaya.com.

Chapter 3: What's new in Communication Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® Communication Manager 6.3, which runs on the S8300D, S8510, S8800, HP ProLiant DL360 G7, and Dell™ PowerEdge™ R610 servers.

Increase in Coverage Answer Group capacities

In Communication Manager, you can create coverage answer groups that allow multiple telephones to ring simultaneously when calls are redirected to the group. All the users in a coverage answer group can answer an incoming call.

The following enhancements are delivered to Communication Manager 6.3:

- The number of phones in a CAG is increased from 8 to 100.
- The number of CAGs on large platforms, Avaya Common Server and Avaya Aura Virtual Environment, has increased from 1,000 to 1,500. The CAG limit remains at 1,000 for Midsize Enterprise (ME) and S8800 platforms.
- On large platforms, the total number of CAG members has increased from 8000 to 33,000, and the simultaneous number of answer group call has increased from 8000 to 12,000. These parameters have not increased for ME or S8800 platforms.

Increase in Locations and Network Regions

With the increasing need for organizations to have multiple branch offices and the need to manage bandwidth over different network regions or branches, Communication Manager now supports a maximum of 2000 locations and networks regions. This increase in the number of network regions is applicable to customers who use Communication Manager installed on S8800, S8510, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.

For more information about increase in Location and Network Regions, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205 and *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Increase in Maximum Simultaneous Calls Being Classified

In Communication Manager Release 6.3, the system limit of Switch Classified Calls (SCC) is 1200. The system can make up to 1200 switch classified calls simultaneously.

Increase Port Network media resources

Communication Manager supports 32,767 media processing channels for port networks. This enhancement allows customers to scale in large IP deployments where the number of recording resources can be increased.

Simultaneous Communication Manager administration session logins

The system level limit on the number of concurrent SAT sessions is increased to 22. This limit is only for login profiles 18 to 69 and not for system logins. However, this functionality is only provided for Communication Manager with large and extra-large memory configurations. Communication Manager with small memory configuration still has the system limit of 17 concurrent sessions.

With the **SAT Limit** feature, you can assign up to five concurrent sessions or retain the default value. On assigning the default value, the account is not restricted at the login level. However, the system level restriction on the concurrent sessions still applies.

Multiple Call Handling

With the Multiple Call Handling feature, a user can administer the destination mailbox for forward-switched calls or rerouted calls that are covering to voicemail. The destination mailbox can be of the principal party or the last-forwarded-to party. Based on the Communication Manager configuration, the greeting of the administered party is played to the caller.

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

Multi-Device Access

With the Multi-Device Access (MDA) feature, a SIP user can register more than one SIP device with a single extension. For example, if the user has four devices registered with the same extension, the user can answer the call from any one of the four devices. The maximum number of devices that can be registered for a SIP user is 10.

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

SIP Direct Media enhancements

Using the SIP Direct Media feature, SIP endpoints establish a direct communication path for subsequent calls, Extension to Cellular (EC500) calls, 3PCC calls, forked video calls, and forked calls to multiple devices (MDA). The direct communication path is established before the call connects between the endpoints. Communication Manager uses the TDM resources or loops the media back to the Communication Manager server only if required.

For more information about SIP Direct Media enhancements, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

SIP Dual Mode

With the SIP Dual Mode feature, the dual mode device can use the EC500 feature as well as the Wi-Fi and cellular networks to receive calls. The dual mode device is a combination of SIP WiFi and EC500 cellular wireless phone.

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

Fax over IP

With the Fax over IP feature, enterprise networks interoperate with PSTN networks to transfer fax messages over IP. Only G430 and G450 gateways support the Fax over IP feature.

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

V.150.1 Modem-over-IP

Communication Manager supports the industry standard Modem-over-IP (MoIP) to interoperate with secure terminals and third-party SIP gateways. Modem-over-IP uses the Simple Packet Relay Transport (SPRT) protocol to transmit data packets between modem devices. Modem devices use the V.150.1 protocol to transmit V-series modem signals between modems and telephony devices. The V.150.1 protocol is a standard recommended by International Telecommunication Union (ITU) to use a modem over IP networks that support dialup modem calls. The V.150.1 protocol defines how to transmit modem traffic between modems and telephony devices over an IP network.

With the Modem-over-IP feature, secure terminals establish a secured connection over SIP and H.323 trunks and the Avaya proprietary Inter-gateway Connections (IGCs).

The Modem-over-IP feature works only with:

- G450 gateways that use the new DAR4 card
- Branch gateways Release 6.2 and later

For more information about V.150.1 Modem-over-IP, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205 and *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Dial Plan Transparency

Communication Manager-DPT is the traditional form of the dial plan transparency feature that provides call continuation services during a network outage. For Communication Manager-DPT to work, the following must be considered:

- The same Communication Manager must serve both the calling and the called endpoints.
- The call must be a direct call to the endpoint and not a redirected or a forwarded call. Any kind of a call that has a group feature associated with the call, for example, hunt groups, does not trigger DPT during a network outage.

Note:

From Communication Manager Release 6.2 Feature Pack 2 onwards, DPT is supported for SIP endpoints too.

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

Communication Manager handling of plus (+) digits

If you set the **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers** field on the SIP Signaling Group screen to y and if Communication Manager uses the public-unknown-numbering table, Communication Manager inserts a leading plus (+) digit in the calling, alerting, diverting, or connected numbers.

If you set the **Prepend '+' to Outgoing Calling Number** field on the SIP Signaling Group screen to y, Communication Manager inserts a leading plus (+) digit in a calling, alerting, or diverting number.

If you set the **Remove '+' from Incoming Calling Numbers** field on the SIP Signaling Group screen to y and if a leading plus (+) digit is present in the number of an incoming call, Communication Manager removes the leading plus (+) from the number.

If you set the **Remove '+' from SIP Number** field on the CTI Link screen to y and if a leading plus (+) digit is present in the number of a call sent over a CTI link, Communication Manager removes the leading plus (+) digit from the number.

If you set the **Remove '+' from SIP Number** field on the CDR System Parameters screen to y and if a leading plus (+) digit is present in the number of a call sent over a CDR adjunct, Communication Manager removes the leading plus (+) digit from the number.

For more information about the fields to administer this feature, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

Patch management for Communication Manager

Communication Manager supports the System Platform service pack infrastructure. You can now install the following patches and service packs, when available, by using Console Domain (cdom):

- Communication Manager dot release
- Security
- Kernel

For information on installing, downloading, and removing patches, see *Implementing Avaya Aura® Communication Manager*, 03-603558.

Hardware

Supported servers

Communication Manager runs on the following servers:

- S8300D
- S8510
- S8800
- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R610

The servers mentioned in the preceding list are the ones that have the required memory and disk space to run Communication Manager on System Platform.

Only the S8300D server, HP DL360 G7, and Dell R610 are currently being sold. If you have an S8800 or S8510 server, you might need to add the necessary memory and hardware to upgrade to Communication Manager Release 6.3.

For information on the supported servers, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

New telephones

Communication Manager provides native support for the following telephones:

- 9400 series digital telephones: Avaya 9404 and Avaya 9408 digital telephones.
- 9600 series H.323 and SIP deskphones: 9608SIP, 9611SIP, 9621SIP, 9641SIP, 9608SIPCC, 9611SIPCC, 9621SIPCC, 9641SIPCC, 9608, 9611, 9621, and 9641

In addition to call processing features, Communication Manager also supports the following features for the 9400 series digital telephones:

- Fixed feature buttons, such as Hold, Conference, Transfer, Message waiting lamp, Drop and Redial
- Message button
- Customized button labels
- Forty Unicode, Eurofont, or Kanafont character display message support

- Speakerphone functionality, including Group Listen
- Support for the same set of Communication Manager call processing features that are supported by the 1416 digital deskphones

For the 9600 series H.323 and SIP deskphones, Communication Manager supports:

- Permanently labeled feature buttons, including Speaker, Mute, Volume, Headset, Contacts, Home, History, Message, and Phone.
- Languages: Arabic, Brazilian Portuguese, Simplified Chinese, Dutch, English, Canadian French, Parisian French, German, Hebrew, Italian, Japanese (Kanji, Hiragana, and Katakana), Korean, Latin American Spanish, Castilian Spanish, and Russian.

For more information on the list of telephones, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Supported gateways

The Communication Manager Branch Gateways form part of the Avaya Aura® solution for extending communication capabilities from the headquarters of an organization to all collaborative branch locations. Communication Manager integrates seamlessly with the following gateways:

- G250
- G350
- G430
- G450
- IG550
- G650
- G700
- G860

Note:

Only G430, G450, IG550, and G650 are currently being sold.

DAR cards supported for G450

The G450 gateway supports the combination of DSP boards of different types. The following table provides the possible combinations of DAR cards supported in a G450 chassis configuration.

Combination of cards	DAR1 card (MP80)	DAR2 card (MP20)	DAR4 card (MP80)
Combination 1	-	-	2
Combination 2	-	2	1
Combination 3	2	-	1
Combination 4	1	1	1

A G450 gateway with two DAR4 cards supports up to 320 channels, irrespective of the administered audio codec type.

Video support for H.323 and SIP Multi-Communication Manager connections

Video calls are now supported across multiple Communication Manager and Session Manager. Existing recovery and failover capabilities remain consistent with existing product failover aspects.

The supported configurations are:

- One Session Manager with multiple Communication Manager as Evolution Server (CM-ES)
- Multiple Session Manager with multiple Communication Manager as Evolution Server (CM-ES)

For more information about the video support for Multi-Communication Manager and Session Manager, see *Avaya Aura® Communication Manager Release 6.3 and Radvision Scopia Release 7.7 and 8.0 Interoperability*.

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 and on the same license. 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. Avaya has identified these special applications as restricted applications. To activate these restricted applications, go to the Avaya Support website at http://support.avaya.com and open a service request.

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

Chapter 4: What's new in Session Manager

This chapter presents an overview of the new features and enhancements for Avaya Aura® Session Manager, which runs on the S8300D, S8510, S8800, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.

SIP Call Loop elimination

SIP Loop calls are the similar INVITE requests that Session Manager receives in a short interval. These INVITE requests have an identical set of the R-URI, To, From, and PAI (optional) header fields. Call Looping events can have a detrimental effect on the performance of the network as these events can deplete critical network resources. Session Manager provides administration features to track and terminate call looping instances in the network.

For more information about SIP Call Loop elimination, see *Administering Avaya Aura® Session Manager Release 6.3*.

Multi-Device Access

The Multi-Device Access (MDA) feature enables a SIP user to register multiple SIP devices with a single extension. The maximum limit of SIP devices that can be registered with a single extension is 10. Session Manager simultaneously forks an incoming call to all the registered SIP devices of the SIP user.

For example, if the user has four devices registered with the same extension, the user can answer the call from any one of the four devices. Session Manager forks the call to all the registered SIP devices simultaneously. When the call is answered at one of the devices, Session Manager cancels the call request from the other devices and sends a cancelled call notification to the inactive devices, which then display the cancelled call notification as a simulated bridged appearance. The inactive devices can join the call by using the simulated bridged appearance. Whenever a user joins an already active call from another device, a barge-in tone is played on the call.

You can specify the maximum number of SIP endpoints that can simultaneously receive calls in the Session Manager communication profile section on the User Profile page.

For more information about MDA, see *Administering Avaya Aura® Session Manager Release 6.3*.

SIP Dial Plan Transparency

Dial Plan Transparency (DPT) is a business continuity feature that preserves the dial plan and reroutes an existing call over the PSTN to connect endpoints during a network outage. Communication Manager and Session Manager support DPT in the Listed Directory Number (LDN) and the DTMF method as follows:

- A PSTN call routes to a single LDN at the far end.
- The PSTN call carries the identity of the calling party.
- The far end answers the call, and the calling side sends identifying DTMF digits of the called party.

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

Dynamic Overload Control

Session Manager queries Communication Manager for status of various features. In case of a system-wide failover or failback, the polling (query) traffic can overload Communication Manager. The Dynamic Overload Control feature is now available for traffic between Session Manager and Communication Manager.

For more information about this feature, see *Administering Avaya Aura® Session Manager Release 6.3*.

SIP sessions count

Session Manager enables monitoring and reporting of the number of license usages in the system. The number of license usages is equivalent to the number of concurrent active SIP INVITE sessions used in the system. This number is cumulative of all the concurrent active SIP INVITE sessions currently being used on each Session Manager instance in the system.

Session Manager Element Manager collects, monitors, and logs the number of concurrent SIP sessions that the system or the individual Session Manager uses.

SNMP MIB

Network Management Systems (NMS), supporting the earlier software versions such as Session Manager 6.2, use the SNMP MIBs for network monitoring purposes.

Administrators can download a zip archive file containing the definitions of Session Manager supported SNMP MIBs, alarm traps, and informs.

For more information about SNMP MIB, see *Administering Avaya Aura® Session Manager Release 6.3*.

Session Usage Tracking

Element Manager collects, monitors, and logs the number of concurrent SIP sessions in the system. As the total number of WAS licenses used is equal to the number of concurrent SIP sessions, you can use the SIP Sessions Count feature to monitor and report the number of WAS licenses used by the system.

For more information about this feature, see *Administering Avaya Aura® Session Manager Release 6.3.*

VMware enablement

Session Manager 6.3.2 supports the installation on VMware platform for the following configurations.

VMware resource	SM 6.3.2 - configuration for 3,500 users	SM 6.3.2- configuration for 7,000 users	SM 6.3.2 - configuration for 10,000 users
Operating System	RHEL 6.2 – reusing SM kick start, 64-bit	RHEL 6.2 – reusing SM kick start, 64-bit	RHEL 6.2 – reusing SM kick start, 64-bit
SM Software release	6.3.2	6.3.2	6.3.2

VMware resource	SM 6.3.2 - configuration for 3,500 users	SM 6.3.2- configuration for 7,000 users	SM 6.3.2 - configuration for 10,000 users
vCPUs	Four	Eight	Twelve
Minimum CPU Resources	9,600 MHz (4 x 2400 MHz)	19,200 MHz (8 x 2400 MHz)	28,800 MHz (12 x 2400 MHz)
Minimum CPU speed	2400 Mhz Xeon E5620 or equivalent	2400 Mhz Xeon E5620 or equivalent	2400 Mhz Xeon E5620 or equivalent
Memory	6 GB	10 GB	12 GB
Storage reservation	150GB	150GB	150GB
Shared NIC(s)	Four virtual NICs @ 1000 Mbps - eth0 - Management, eth1 - Services port, eth2 - Asset, eth3 - NIC bonding (if used). **Note:** The Services port is never used in a VMware installation. The NIC bonding is seldom used.		
Users	3,500 to 4000	7,000 to 8,000	10,000 to 12,000

For more information about this feature, see *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide*.

Support for Radvision endpoints registered to Session Manager

Customers using Radvision and Avaya endpoints can now easily integrate video and audio calls. Radvision XT5000, XT4200, and XT Executive 240 can all be registered to one Session Manager to make point-to-point audio and video calls. These endpoints can also join multipoint calls on Scopia Elite MCU registered to iView or Scopia Management and XT Embedded MCU registered to Session Manager. Limited mid-call features are also supported.

For more information about support for Radvision endpoints, see *Avaya Aura® Communication Manager Release 6.3 and Radvision Scopia Release 7.7 and 8.0 Interoperability*.

Related topics:

Radvision XT with embedded Multipoint Control Unit on page 33

Radvision XT with embedded Multipoint Control Unit

XT 5000 endpoint with optional 4 Port or 9 Port Multipoint Control Unit (MCU) registered to Session Manager enables a small video MCU to be deployed within an Avaya Aura® network. Other Radvision XT endpoints and Avaya endpoints that are registered to Session Manager can be hosted on the MCU.

You cannot host the following devices on the XT MCU registered to Session Manager:

- Avaya Desktop Video Device (ADVD)
- H.323 Avaya one-X® Communicator registered to Communication Manager as Evolution Server (CM-ES)
- Radvision endpoints registered to iView or Scopia Management

For more information about Radvision XT with MCU, see *Avaya Aura® Communication Manager Release 6.3 and Radvision Scopia Release 7.7 and 8.0 Interoperability*.

Chapter 5: What's new in System Manager

Avaya Aura® System Manager Release 6.3.2 supports the following features and enhancements:

- System Manager Geographic Redundancy (GR) feature on VMware ESXi 5.0 and 5.1
- Configuration of the following during the installation of System Manager Release 6.3.2 on VMware ESXi 5.0 and 5.1:
  - Multiple DNS addresses
  - NTP server
  - Time zone
  - Virtual FQDN and Backup definition rule
- Data migration from System Manager 6.2 on VMware ESXi 5.0 to System Manager Release 6.3.2 on VMware ESXi 5.1
- Recovery when the secondary System Manager server is active. This feature makes System Manager services available when the system recovers to the primary System Manager server.

  In Release 6.3.2, System Manager services are unavailable during the recovery process from the secondary System Manager server to primary System Manager server. In Release 6.3, you deactivate the secondary System Manager server during the recovery process.
- Resending the failed GR notification messages to elements. The administrator can resend failed GR notification messages such as Enable replication and Secondary Activated to elements from the Manage Elements page on System Manager Web Console.
- System Manager backup or restore to remote servers using the SFTP protocol to establish secure communications
- Data Replication Service (DRS) initial load refactoring. For larger databases, the initial load refactoring takes longer that makes the main database unavailable for longer durations. The DRS Refactoring feature creates the replica of the main database and performs the initial load refactoring on the database. While the initial load refactoring is in progress, all clients of the database can access the main database.

  When the initial load refactoring on the replica database is complete, the system switches to the main database from the replica database. This makes the main database available for longer durations when initial loading is in progress.

- System Manager Reverse Proxy Agent, an Avaya Services client that runs on System Manager. The Services team can use Reverse Proxy Agent to start CS 1000 element managers from System Manager on remote access session through SAL Gateway.
- Removal of the Subscriber Manager feature in System Manager. The User Management (UM) service of System Manager now supports the administration of the user profile data for the CS 1000 and CallPilot endpoints that was earlier provisioned through Subscriber Manager.
  - The Subscriber Manager data can be migrated to UM or the user data can be added in UM using methods such as LDAP synchronization, entry through the Web console, bulk import, and Web services.
  - With user data populated, the CS 1000 and CallPilot Synchronization feature can be executed to link existing phones or mailboxes to users based on finding a name match between them.
  - The CS 1000 Corporate Directory application has a dependency on the data in UM. The user data and profile data must be populated in UM to generate the CS 1000 Corporate Directory report.

Support for Communication Manager element and IP Office element

Software Management

As part of the Avaya Integrated Management (AIM) transition of Enterprise Network Management, the Software Update Manager (SUM) functionality has now moved to System Manager. System Manager has expanded the product coverage of Software Management beyond B5800 and IP Office to include Software Management of Communication Manager, TN boards, Media Modules, and Gateways.

Using Software Management, you can:

- Download the necessary software to manage Avaya devices.
- Compare the current software version with the latest versions available from Avaya.
- Recommend updates when a new version is available.
- Update the software on your devices.
- Perform prescheduled software updates and installations. You can also perform these operations in bulk.
- Download a new release of a software from the Avaya PLDS website, and store the software locally for subsequent use.

- Retrieve the required software for Avaya devices from the Web, and download the software to the appropriate device.
- Copy files containing embedded software to the server.
- Upgrade gateways, media modules, and TN boards.
- Upgrade Communication Manager from release 5.0 to 5.2.1.

  Note:

  Software Management does not support upgrading from one release of Communication Manager to another release of Communication Manager in certain scenarios. For example, you cannot upgrade directly from Communication Manager Release 5.2.1 to 6.0. In these scenarios, you must perform the normal upgrade procedure for Communication Manager on System Platform.
- Update Communication Manager Release 5.0 and later.
- Perform rollback for Communication Manager servers and gateways.
- Reset Communication Manager servers after updates.

Granular role-based access control

With the Granular role-based access control feature, you can restrict access to Communication Manager resources, such as gateways and servers, and objects on resources, such as Agent Login ID.

Based on the role that a user has, System Manager supports range permissions along with the operation permissions assigned to the user. You can assign permissions or a combination of permissions to users. The permissions include adding, editing, deleting, and duplicating objects. For example, if you assign a range of 1000:4000 and define permissions for Add, Edit, and Delete operations, the user can create, edit, and delete extensions within the range of 1000:4000.

The default value in the specific **Range** field is asterisk (*). If you retain this value, the user has access to the entire defined range.

You can define range-level granular permissions for the following Communication Manager objects:

- Endpoints
- Agent Login ID
- Announcement
- Audio Group
- Best Service Routing Pickup Group

- Holiday Table
- Variables
- Vector
- Vector Directory Number (VDN)
- Vector Routing Table
- Service Hours Table
- Coverage Answer Group
- Coverage Path
- Coverage Remote
- Coverage Time-of-Day
- Group-Page
- Hunt-Group
- Intercom Group
- Pickup Group
- Terminating Extension Group
- Route-Pattern
- Class of Restriction (COR)

Search component for Communication Manager objects

System Manager supports data and link search for the following Communication Manager objects:

- Agents
- Announcement
- Audio Group
- Communication System
- Data Module
- Endpoints
- Hunt Group
- Off PBX Endpoint Mapping
- Signaling Group
- Trunk Group

- Vector
- Vector Directory Number (VDN)
- Vector Routing Table (VRT)

Link-based search

When you click the **Search** field, the system lists the Communication Manager objects that support the Search feature. To go to the home page of an object, from the menu of the listed Communication Manager objects, select the object. For example, if you select **Hunt Group** , you directly go to the Hunt Group page.

Data search

The Search feature supports the free-text search and the specific search. For example, when performing a free-text search, if you type `endpoint 100` in the **Search** field, the system displays a list of endpoints that contain 100 in the extensions. If you move the pointer over one of the listed endpoints, the system displays the configured settings of the endpoint in the left side of the search results. To modify the settings, you can click the **View**, **Edit**, or **Delete** buttons at the bottom of the settings window.

If you type the name of a Communication Manager object followed by space, the system lists all the searchable fields for that object. You can click a field and search for the objects of that field.

For information about searchable fields for supported Communication Manager objects, see *Administering Avaya Aura® System Manager*.

Communication Manager field validation

System Manager now supports field validations on the Manage Elements page when you add and edit objects for Communication Manager instances. For example, if you enter an invalid Class of Restriction value, the system displays an error message and also the acceptable range of values.

Note:

You cannot use system logins to add Communication Manager objects.

Change in User Interface

In addition to the validation functionality, System Manager provides you with a user interface for easy administration of Communication Manager objects. The following fields have been moved from the **SNMP Attributes** tab to the **General** tab:

- Login
- Password
- Confirm Password
- Secure Shell Service (SSH) Connection
- Port

- Alternate IP Address
- RSA SSH Fingerprint (Primary)
- RSA SSH Fingerprint (Alternate)
- Location
- Enable Notifications

Support for Communication Manager 6.3 features

System Manager supports the following features of Communication Manager 6.3:

- System-level limit for the number of concurrent SAT sessions increased to 22. This limit is for login profiles 18 to 69 and for system logins. This limit is applicable to Communication Manager servers with large and extra-large memory. System Manager prevents you from initiating a new session if you exceed the maximum number of concurrent sessions. The system displays an error message if the maximum number of logins is reached.
- Coverage Answer Groups increased to 1500.
- Coverage Answer Group members increased from 8 to 100.
- Locations for endpoints increased to 2000 .
- Route Patterns increased to 2000.
- IP network regions increased to 2000.
- Location qualifier increased to 2000 in AAR and ARS Analysis.
- AAR and ARS Analysis entries increased to 16000.
- ARS Digit Conversion entries increased to 12000.

Support for new fields and buttons

The following table lists the new fields and the objects where these fields are used:

Fields	Object
Turn on mute for remote off-hook attempt **Note:** • Supported for SIP and H.323 96x0 and H.323 16xx set types. • Available only when **(SA9120) Force Mute for offhook event in shared**	Endpoints

Fields	Object
control mode? on the Special Applications screen is enabled.	
Apply Ringback upon Receipt of	Off-PBX-Telephone-Configuration-Set
Location parameters and Display Parameters	Locations
Stub Network Region	Network Region
Far-end Network Region	Signaling Group
Network Region	IP Network Map
Location	• Off-PBX Endpoint Mapping • Service Hours Table • IP Network Region

The following table provides the new buttons and the objects where these buttons are used:

Buttons	Object
Auto Logout/Login	Agents

Usage options

Use **Usage Options** to add and remove internal dependencies of endpoints.

- Using **Add Options**, you can add references of an endpoint to other endpoint-related objects, such as Intra Switch for CDR Agent, Intra Switch CDR Endpoint, and Intra Switch CDR VDN .
- Using **Remove Options**, you can remove dependencies between endpoints and vectors. For example, if you remove a station entry, a vector step that has a reference to the station extension is also removed.

Support for the IP Office element

IP Office 9.0 is a new System Manager adopter. System Manager 6.3.2 supports up to 2,000 IP Office 9.0 Gateways. System Manager 6.3.2 supports a customized page for adding IP Office instances. In addition, System Manager 6.3.2 provides the following functionality support for IP Office 9.0:

- Alarm management
- Discovery and inventory

- User provisioning
- Configuration and template administration
- Security administration
- Backup and restore
- Central licensing

For more information about System Managersupport for the IP Office element, see *Administering Avaya Aura® System Manager*.

Chapter 6: What's new in Branch Gateway

This chapter provides an overview of new features for Avaya Branch Gateway.

T.38 Fax with Fallback to G.711 Pass-Through

T.38 Fax with Fallback to G.711 Pass-Through feature provides the functionality to enterprise networks managed by Communication Manager to interoperate with the older Verizon networks that currently do not support T.38 Fax for fax transport. A new codec type, T.38 Fax with Fallback to G.711 Pass-Through, is added to the IP codec set for fax mode.

The operation of T.38 Fax with Fallback to G.711 Pass-Through is summarized as follows:

- The call connection is signaled for standard T.38 fax relay.
- In the event of a failure to successfully negotiate T.38 fax relay, Communication Manager issues a re-INVITE to a G.711 mode of operation.
  - With PCM (G.711) codec sampling, there is an effort made to simulate a circuit-switched clear channel transport.
- The fax call is in the G.711 mode until the user disconnects.

Note:

This feature only works over SIP trunks.

For more information about the T.38 Fax Fallback to G.711 feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

T.38 with Error Correction Mode

Prior to Release 6.3, a transmission error occurred when a large fax document was sent. In Branch Gateway Release 6.3 and later, the Error Correction Mode (ECM) feature corrects the transmission error without retransmitting multiple pages.

If part of the data is corrupted or missing while transmission, the receiving end sends a request to resend the data.

The ECM field is available only if FAX Mode is t.38-standard or t.38-G711-fallback.

Table 1: Valid entries for T.38 with Error Correction Mode

Valid Entry	Description
y	Branch Gateway checks and rectifies errors in a fax transmission. Even if the receiver detects errors in the transmission, Branch Gateway does not resend packets.
n	Branch Gateway does not check for errors in a fax transmission. If the receiver detects errors in the transmission, Branch Gateway resends the packets.

List Trace and List Measurement

The List Trace and the List Measurement commands include additional performance and diagnostic information for V.150 / Modem over IP calls.

The standard List Trace command provides enhanced information for the V.150.1 call state information. The goal is to avoid dependency on Wireshark captures and other logging tools. The List Trace command provides easy to read logging information.

The List Measurement command aggregates the usage for V.150.1 calls and provides this in the summary for G.711 equivalent call statistics.

For more information about the List Trace and List Measurement commands, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Server*, 03-300431.

V.150.1 Modem over IP

The V.150.1 Modem over IP (MoIP) feature is an industry-standard compliant V-series MoIP transport for carrying modem traffic over an IP network and for supporting interoperability with secure third-party terminal devices.

Note:

This feature is only available on G450 Branch Gateway and requires the MP160 DSP card.

The V.150.1 MoIP supports the following modem modulation modes:

- V.32 and V.34 up to 33.6 Kbps.
- V.90 and V.92 up to 56 Kbp.

Benefits of V.150.1 MoIP:

- Can transform analog tone events into digital control messages, so that the protocol can pass over hops.
- Can recover from loss and operate at higher speeds up to V.92 as the protocol is sent in sequenced packets.
- Can interoperate with many different vendors.
- Can eliminate extra trunking because of convergence of data, voice, and fax.

For more information about V.150.1 (MoIP), see *Configuring V.150.1 on the Avaya G450 Branch Gateway*.

MP160 DSP daughter board

To support the V.150.1 Modem over IP feature on the G450 Branch Gateway, a new DSP card MP160 is introduced in Release 6.3. MP160 supports up to 160 VoIP channels on the G450 Branch Gateway. MP160 is used for V 150.1 and non V 150.1 calls on the G450 Branch Gateway. The G450 supports mixed DSP boards of different DSP channel capacities. The DSP channel count on G450 Branch Gateway must not exceed 320.

For more information about MP160 DSP daughter board, see *Configuring V.150.1 on the Avaya G450 Branch Gateway*.

Chapter 7: What's new in Presence Services

This chapter provides an overview of the new and enhanced features for Avaya Aura® Presence Services 6.2.

Installation framework enhancements

Presence Services Release 6.2 provides simplified and improved upgrade and installation framework.

- **Upgrades**: Presence Services Release 6.2 introduces a new upgrade framework, which enables system administrators to upgrade an existing Presence Services instance to the latest version without the need to manually uninstall the old software.
- **Installation**: With improvements to the uninstall scripts and to the system checks performed during installations on System Platform, the installation framework is now more simplified and robust.

For more information about installing Presence Services, see *Implementing Avaya Aura® Presence Services*.

Increased support for H.323 and SIP users

PS, increased user support

increased user support, PS

Presence Services 6.2 supports up to 10,000 H.323 users and SIP users per node and up to 50,000 H.323 and SIP users in a five-node cluster. For H.323 and SIP users, Presence Services 6.2 supports an average of 25 buddies, who are contacts and watchers, per user. By default, the Presence Services enforces a maximum of 150 buddies per list. This limit is applicable to the total number of contacts and watchers that a user can have.

VMware support enhancement

Presence Services Release 6.2 supports VMware ESXi 5.0 and 5.1. Presence Services has added support for smaller and larger VMware deployments. In addition to the configuration to support 2,400 endpoints, Presence Services now supports 1,000 and 10,000 endpoint deployment configurations.

The following table details the virtualized environment hardware configurations to support the three configuration options: Small, Medium, and Large.

		Number of end points supported		
		1,000	2,400	10,000
Hardware tab	CPU Sockets	1	2	2
	CPU Cores/Socket	4	4	4
	Memory Size	8 GB	8 GB	32 GB
Resources tab	CPU Reservation	9,600 Mhz	19,200 Mhz	19,200 Mhz
	Memory Reservation	8,192 MB	8,192 MB	32,767 MB

Federation with Openfire

Presence Services 6.2 works with a third-party XMPP server, Openfire, to gather Presence information and support Instant Messaging capabilities. Openfire is a real time collaboration (RTC) server licensed under the Open Source Apache License. Openfire uses the only widely adopted open protocol for Instant Messaging, XMPP, also known as Jabber.

Mapping capability

The mapping capability of Presence Services 6.2 has been enhanced to support mapping of multiple domains to a single Presence domain. Presence Services 6.2 uses Regular Expressions while defining the Domain Substitution rule in System Manager. This feature works only when the user part of the URI is unique in System Manager.

Presence Services uses the domain substitution rule to convert a user ID in System Manager to a valid user ID in Presence Services. By default, the system uses string substitution.

For more information about mapping multiple domains to a single Presence Services domain, see *Administering Avaya Aura® Presence Services*.

Support for new fields for AES Collector

For AES Collector configuration, the following two new fields are available on the Advanced configuration view:

- **Time (minutes) endpoint is on-hook until being declared Away**
- **Time (minutes) endpoint is Away until being declared Out Of Office**

Using AES Collector, Presence Services obtains the presence status of the endpoints when the endpoint is logged out or if the user is away.

In Presence Services 6.2, you can configure two new timers (T1 and T2) at a system level to obtain the presence status of the endpoints.

Consider the following properties while configuring timers:

- Both timers have a default value of 0.
- Timer T1 starts as soon as an endpoint moves to the *Available* state when the endpoint goes on-hook or logs in. Timer T2 is triggered when timer T1 expires.
- Once T1 expires, the presence status is updated to *Away*.
- Once T2 expires, the presence status is updated to *Out of Office*.
- Timers T1 and T2 are reset if the endpoint is used.

Chapter 8: What's new in Application Enablement Services

This chapter presents an overview of the new features and enhancements for Avaya Application Enablement Services (AE Services).

ASAI enhancements

AE Services 6.3 provides the following ASAI capacity increases:

- Increased message rate limit on medium and large Communication Manager templates

  The AE Services 6.3 system message rate limit has increased from 1000 to 2000 messages per second (full duplex). Full bandwidth is available with a single session (that is, to one Communication Manager if only one Communication Manager is in use).

  The Communication Manager 6.3 system message rate limit has increased from 1000 to 2000 messages per second (full duplex) on medium and large templates. Full bandwidth is available with a single session (that is, to one Communication Manager if only one Communication Manager is in use). Full capacity is available over a single Processor Ethernet (PE) Application Enablement Protocol (AEP) connection and requires at least 10 CLANs. (There is no change per CLAN rates.)

  Note:

  There is no change in the message rate on small templates.

- Support for the multicast mechanism available in Communication Manager 6.3

  AE Services 6.3 supports the multicast mechanism available in Communication Manager 6.3. With the multicast mechanism, Communication Manager 6.3 can now pack the same ASAI message that is built for different associations/CTI links into a single AEP message. The multicast mechanism applies to events and route end messages destined for the same AE Services 6.3 server. AE Services 6.3 unpacks these messages and distributes them transparently to the appropriate upstream services.

  Note:

  - Communication Manager 6.3 applies this optimization automatically (where appropriate).

- Optimization applies across all CTI services on the same AE Services server. (Multicast always benefits TSAPI since it uses additional monitors to implement CSTA.)
- Multicast messages appear as normal, individual ASAI messages in Communication Manager MST tracing. The transport level message trace on AE Services shows the actual multicast messages.

• Increased Event Notifications limit on large Communication Manager templates

AE Services 6.3 now supports a maximum of 30,000 Event Notifications up from 10,000 on large Communication Manager templates.

Note:

For small and medium Communication Manager templates, the maximum number of Event Notifications is still 10,000.

• Increased Adjunct Route Requests limit on large Communication Manager templates

AE Services 6.3 now supports a maximum of 8,000 active Adjust Route Requests up from 4,000 on large Communication Manager templates.

Note:

- The increased maximum number of Adjunct Route Requests requires the purchase of the increased Adjunct Route license.
- The maximum number of Adjunct Route Requests has not been increased on small and medium Communication Manager templates.
- The increased maximum number of Adjunct Route Requests requires AE Services 6.3. Communication Manager will restrict the total Adjunct Route Requests to a maximum of 4,000 for all AE Services 6.2 and earlier systems.

• Increased ASAI associations

AE Services 6.3 now supports a maximum of 128,000 ASAI associations across all CTI links. (This applies to TSAPI and CVLAN services.)

AE Services 6.3 also supports a maximum of 32,000 Adjunct Routes per CTI link.

Enhancements for Agile Communication Environment™ and Avaya Aura® Contact Center

AE Services 6.3 provides the following enhancements for Agile Communication Environment™ and Avaya Aura® Contact Center:

- GetTimeOfDay request

  The GetTimeOfDay request provides time information for a specified Communication Manager:

  - year
  - month
  - day
  - hour
  - minute
  - second

  The GetTimeOfDay request requires a switch name as a parameter to specify the switch that the application queries for the time information.

- Support for the Private Direct Number (DN) feature in Communication Manager 6.3

  The Private DN feature provides the following new feature access codes:

  - AACC No Conference Activation feature access code

    When the H.323 or DCP set is in this state, you cannot transfer or conference calls from the designated extension. To use this feature access code, you must administer the AACC No Conference Activation feature access code.

  - AACC One Conference Activation feature access code

    When the H.323 or DCP set is in this state, only one conference is allowed, and you can only transfer one call at a time. To use this feature access code, you must administer the AACC One Conference Activation feature access code.

    Note:

    - Only computer telephony integration (CTI) applications can activate the AACC No Conference and AACC One Conference feature access codes.

      - The extension used to invoke the AACC No Conference and AACC One Conference feature access codes must be a *monitored* extension. The

feature access codes require a designated extension on which these features will be applied.

- The ability to deactivate these features is available **to both** the application and the user (via a physical set).

- You cannot activate the AACC No Conference Mode and AACC One Conference Mode features simultaneously.
- The AACC No Conference Mode and AACC One Conference Mode features are not available currently for Avaya SIP endpoints.

DMCC enhancements

AE Services 6.3 provides the following enhancements for the DMCC clients:

- Endpoint registration events

  The endpoint registration events enable you to:

  - Monitor H.323 endpoints registration activity on Communication Manager for up to three endpoints for a given extension.

    Note:

    The devices are not required to be registered via AE Services.

  - Retrieve information on H.323 endpoints registered to an extension on Communication Manager for up to three endpoints for a given extension.

  These events consume a basic TSAPI license for each extension and require Communication Manager Release 6.3 or later.

- Warning tone generation on a call for DMCC-registered endpoints

  A DMCC recording client can request AE Services to play a warning tone into a call using the following call recording methods:

  - Single Step Conference
  - Multiple Registration
  - Service Observing

Security enhancements

AE Services 6.3 provides the following enhancements for FIPS 140-2 compliance:

- SHA512 encryption for password storage by default

  The Linux passwords are hashed and stored on the server using SHA512 by default. However, you can configure the password encryption to SHA256 if needed.

- SSH client support of SSHv2 protocol only

  - AE Services supports the following ciphers: 3des, aes128, aes192, and aes256.

    SSH uses aes128, aes192, and aes256. AE Services processes use 3des and aes128 for signaling encryption.

  - AE Services supports the following Message Authentication Code (MAC): hmac-sha1.

Note:

SSH clients must be supported with the same ciphers and MAC as supported by AE Services. AE Services does not support CBC ciphers.

Support for Avaya Communication Manager 6.3

AE Services 6.3 is compatible with the following releases of Avaya Communication Manager:

- Avaya Communication Manager 5.2.1
- Avaya Communication Manager 6.0.x
- Avaya Communication Manager 6.2
- Avaya Communication Manager 6.3

AE Services Management Console enhancements

AE Services 6.3 provides the following enhancements to the AE Services Management Console:

- Log Manager

Using the Log Manager feature, you can configure the trace/logging levels for the following services:

- ASAI Link Manager
- CVLAN Service
- DLG Service
- Management Console
- Transport Layer Service
- TSAPI Service
- DMCC Service

Note:

Do not change the trace/logging levels without guidance from an Avaya engineer. Turning on the trace or increasing the logging levels may degrade system performance.

- DMCC Test

  Using the DMCC Test feature, you can make a first party call or third party call to test your DMCC configurations.

- Support for Microsoft Internet Explorer 9 and Microsoft Internet Explorer 10 running on Microsoft Windows 8 Pro and Microsoft Windows 8 Enterprise

Command enhancements for the AE Services on System Platform offer

AE Services 6.3 provides the following command enhancements for the AE Services on System Platform offer:

- swversion command enhancement

  When you run the swversion command from the CDOM of the AE Services VM, the output now displays the AE Services version number with the System Platform version number.

  When you run the swversion command from the System Platform console domain, the output now displays the same information as when you run the swversion command from the AE Services VM with the swversion command from the console domain of VM.

- getlogs command enhancement

  Using the getlogs command from the System Platform console domain, you can now collect logs from both System Platform and the AE Services VM. When you run this

command from the System Platform console domain, the output is stored in `/vspdata/getlogs/data` or `/vspdata/getlogs/archive` depending upon the arguments passed. The getlogs command options are:

`-h` – shows all options for this command

`-l` – shows the list of all VMs in System Platform

`-r` – cleans out the logs

Support for Microsoft Windows 8

The following AE Services 6.3 SDKs and clients support Microsoft Windows 8 Pro and Microsoft Windows 8 Enterprise:

- AE Services DMCC .NET SDK
- AE Services DMCC Java SDK
- AE Services DMCC XML SDK
- AE Services JTAPI SDK
- AE Services TSAPI SDK
- AE Services TSAPI client
- AE Services CVLAN client

Chapter 9: What's new in Avaya Aura® Call Center Elite

Automatic logout and login of agents after skill change

You can use an optional parameter, auto, when changing the skills of logged-in agents to automatically log out and log in the agents. Without the parameter, agents must log out and log in again for the changes to take effect.

The parameter is available with the **`change agent-loginid xxxx`** command and is applicable if you use Expert Agent Selection (EAS).

For more information, see *Administering Avaya Aura® Call Center Elite*.

Logged-in SIP agents capacity increase

The limit for concurrently logged-in SIP Expert Agent Selection (EAS) agents on a single Communication Manager instance is increased from 2500 to 5000.

For more information, see *Avaya Aura® Communication Manager System Capacities Table*.

Used for BSR Polling field administration

You can administer the **Used for BSR Polling** field on the Vector Directory Number screen to prevent Communication Manager from sending polling-related messages to Call Management System (CMS) and Avaya IQ for unmeasured calls.

The field is applicable when you use Best Service Routing (BSR) and Look Ahead Interflow (LAI).

For more information, see *Administering Avaya Aura® Call Center Elite*.

Appendix A: PCN and PSN notifications

PCN and PSN notifications

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

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

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

   Note:

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

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

Note:

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

Signing up for PCNs and PSNs

About this task

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

To sign up for notifications:

Procedure

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

Index

R

S

T

U

V

W