What's New in Avaya Aura® Release 6.2 Feature Pack 3

Release 6.2 Feature Pack 3
October 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 of the following Avaya Aura® 6.2 Feature Pack 3 components:

- Avaya Aura® Communication Manager 6.3.2
- Avaya Aura® Session Manager 6.3.4
- Avaya Aura® System Manager 6.3.4
- Branch Gateway 6.3.1
- Avaya Aura® Presence Services 6.2.2
- Application Enablement Services 6.3.1

Intended audience

This document is for the following audiences:

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

Related resources

Documentation

The following table lists the documents related to the components of Avaya Aura® Release 6.2 Feature Pack 3. 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 procedures to install System Platform, license and authentication files, and Communication Manager 6.3.2.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administration			
555-233-504	Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network components of Communication Manager Release 6.3.2, such as gateways, trunks, FAX, modem, TTY, and Clear-Channel calls.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-300509	Administering Avaya Aura® Communication Manager	Describes the procedures and screens used for administering Communication Manager Release 6.3.2.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
—	Administering Avaya Aura® System Manager	Describes the procedures for configuring System Manager Release 6.3.4 and the Avaya Aura® applications and systems	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Document number	Title	Description	Audience
		managed by System Manager.	
—	Configuring V.150.1 on the Avaya G450 Branch Gateway	Describes the procedures to configure V.150.1 on the Avaya G450 Branch Gateway Release 6.3.1.	Implementation Engineers and System Administrators
—	Administering Avaya Aura® Presence Services	Describes the steps to configure Presence Services Release 6.2.1.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Understanding			
555-245-205	Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-602878	Avaya Aura® Communication Manager Screen Reference	Describes the screen and detailed field descriptions of Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-603324	Administering Avaya Aura® Session Manager	Describes how to administer Session Manager using System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
555-245-207	Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware devices that can be incorporated in a Communication Manager telephony configuration.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Maintenance and Troubleshooting			

Document number	Title	Description	Audience
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

Downloading documents from the Support website

About this task

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

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. At the top of the Avaya Support homepage, click the **Downloads and Documents** tab.
3. In the **Enter Your Product Here** field, type the product name for which you want to download the documents. Once you start typing the product name, the website displays the results matching to the entered text. You can select the complete product name from the displayed list.
4. In the **Choose Release** field, select the product release.
   - For Presence Services, select 6.2.x.
   - For other Avaya Aura® Feature Pack 3 components, select 6.3.x.
5. In the **Select a content type** section, select Documents.

   Note:

   To refine the search results, select a document category. You can also select multiple categories. If no category is selected, the website displays all the documents for the selected product and release.
6. Click **Enter**.
   The website displays a list of documents for the selected product and release.
7. To open a document, click the document title.

Training

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

Course code	Course title
AVA00383WEN	Avaya Aura® Communication Manager Overview
ATI02210VEN	Presence Services Overview
AUCC100010632	Avaya Aura® Presence Overview
5U00104W	Session Manager 6.2 Delta Overview
5U00105W	Avaya Aura® Session Manager Overview
ATU00171OEN	Session Manager General Overview
ATU00170OEN	Session Manager Technical Overview
5U00106W	Avaya Aura® System Manager Overview
AVA00279WEN	Communication Manager - Configuring Basic Features
E9U00103O	AES 6.1 GA Knowledge Transfer Recording
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
ATI02348IEN, ATI02348VEN	Avaya Aura® Communication Manager Implementation
AVA00821H00	Avaya CM Architecture and Gateways: H.248, H.323, and Proprietary
5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00103W	Avaya Aura® System Manager 6.2 Delta 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 3 components

Product component	Release version
Communication Manager	6.3.2
Communication Manager Messaging	6.3.2
Session Manager	6.3.4
System Manager	6.3.4
Branch Gateway	6.3.1
Presence Services	6.2.2
Application Enablement Services	6.3.1
Call Center Elite	6.3.2

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. Customers have the flexibility to combine the license types on a per-user basis or enterprise-wide. Customers purchase the number of licenses they need of each suite based on the communication requirements of the individual users. This licensing model 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® infrastructure for desktop workers, including 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, Mobility Suite includes Avaya Flare® Experience for iPad, and Avaya one-X® Mobile for SIP, iOS, Android, and Windows smartphones. Mobility Suite also includes Avaya Aura® Messaging and Avaya Session Border Controller for Enterprise for advanced messaging, secure network access, and VPN-less secure remote communications.
- Collaboration Suite enables an enterprise to gain full business collaboration by using audio, video or the web. This suite adds Avaya Aura® Conferencing Release 7.0 to the features of Mobility Suite and Foundation Suite, 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

Product	Foundation Suite	Mobility Suite	Collaboration Suite
Avaya one-X® Mobile	N	Y	Y
Avaya Session Border Controller for Enterprise	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 Avaya Aura® Licensing Suite.

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: Supported servers

Avaya Aura® components run on the following servers:

- S8300D
- S8510
- S8800
- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R610
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R620

The servers mentioned in the preceding list have the required memory and disk space to run Avaya Aura® components.

Only S8300D, HP DL360 G7, HP DL360 G8, Dell R610, and Dell R620 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 the latest version.

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

Chapter 4: What's new in Communication Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® Communication Manager 6.3.2.

Communication Manager license utilization

Using the License Utilization feature, you can view the license utilization on the WebLM user interface for Communication Manager, Call Center Elite, and Communication Manager Messaging. License utilization is the number of licenses actually used by a product. For example, if you have a Communication Manager license file that can support 1000 station licenses and you add 900 stations on the Communication Manager server, the WebLM user interface displays 900 licenses.

On the WebLM server, you can view and track the license usage for all Avaya Aura® products. The standalone WebLM server, System Manager WebLM server, and WebLM OVA support the License Utilization feature.

Using the License Utilization feature, you can determine the need for buying extra licenses and identify the unused licenses of one system that you can use to increase the capacity on another system.

On the View License Capacity page of the WebLM user interface, you can view the current license utilization and peak license utilization (high water mark) for the last 7 to 30 days.

Note:

Communication Manager Release 6.3 and earlier displays all feature capacity in use, regardless of the actual utilization on the Communication Manager server.

Video endpoints support for SIP and H.323 dual registration

Video endpoints support the SIP and H.323 dual registration feature.

The following table lists the audio and the video endpoints that support the SIP and H.323 dual registration feature for Release 6.3 and later:

Communication Manager Releases	Audio endpoints	Video endpoints
6.3	96xx and 96x1 H.323 and SIP 1XC H.323 and SIP ADVD	—
6.3.2	96xx and 96x1 H.323 and SIP 1XC H.323 and SIP ADVD	Upcoming release of Flare on iPad SIP Upcoming release of Flare on Windows SIP

Restrict Call Joining

The Restrict Call Joining feature is supported only on Avaya Aura® Contact Center. If you enable this feature, Communication Manager restricts agents from initiating a transfer or a conference operation. You can enable this restriction only for outbound calls.

Note:

Communication Manager Release 6.2 and earlier supported the restriction on H.323 and DCP telephones. Communication Manager Release 6.3 extends this restriction to SIP telephones.

For more information about the Restrict Call Joining feature, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* Release 6.4, 44400-521.

Restrict Second Agent Consult

The Restrict Second Agent Consult feature is supported only on Avaya Aura® Contact Center. If you enable this feature, agents can use only one consult operation at a time. The consult operations consists of transfer and conference. You can enable this restriction only for outbound calls.

You can enable the Restrict Second Agent Consult feature by using one of the following methods:

- Per-station
- Group-level

Note:

Communication Manager Release 6.2 and earlier supported the restriction of the second consult operation on H.323 and DCP telephones. Communication Manager Release 6.3 extends the restriction to SIP telephones.

For more information about the Restrict Second Agent Consult feature, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* Release 6.4, 44400-521.

Support for Global Session Identifier

Communication Manager labels each point-to-point session with a globally unique identifier by generating a 128-bit identifier and inserting the identifier in the Global Session ID (GSID) header of the request.

Communication Manager generates a new GSID header in one of the following situations:

- The originating leg of the call does not have a SIP dialog.
- The originating leg of the call has a SIP dialog without a GSID header.

If the originating SIP dialog has a GSID header, Communication Manager copies the GSID header from the SIP dialog to all the subsequent SIP dialogs of the call.

Communication Manager establishes an association between two SIP dialogs by assigning the Associated Global Session Identifier (A-GSID) parameter to the GSID header of the associated SIP dialog.

To troubleshoot call flows, you can use a tracing tool and filter GSIDs from the relevant logged messages.

Call log support for busy 94xx deskphones

Communication Manager 6.3.2 records all incoming calls when a 94xx deskphone is busy due to the following conditions:

- All but one call appearances reserved for incoming calls are in the non-idle state. The last call appearance is reserved for outgoing calls.
- All call appearances are in the non-idle state.
- The Do Not Disturb feature is active on the endpoint.
- One call appearance is busy on a call because a remote user has put the call on hold or started a transfer or a conference call.

Communication Manager records all missed calls in the missed call log of 94xx deskphones.

Enhanced Bridged Call Appearance

With Enhanced Bridged Call Appearance, you can set the caller information on the bridged call appearances to be the same as the caller information on the principal station. To use this enhancement, set the **Match BCA Display to Principal** field on page 2 of the Class of Service screen to `y`.

Before Communication Manager Release 6.3.2, the display format of incoming calls on the bridged call appearances was <calling name/number> to <principal name/number>, and the display format on the principal station was <calling name/number>. Communication Manager Release 6.3.2 and later supports the display format of incoming calls on bridged call appearances as <calling name/number>.

When the **Match BCA Display to Principal** field on page 2 of the Class of Service screen is set to `n`, the caller information on the bridged call appearances is as follows:

	Calling-party name is available	Calling-party name is not available
Calling-party name is available	<calling name> to <principal name>	<calling number> to <principal name>
Calling-party name is not available	<calling name> to <principal name>	<incoming trunk name> to <principal name>

When the **Match BCA Display** field on page 2 of the Class of Service screen is set to `y`, the caller information on the bridged call appearances is as follows:

	Calling-party name is available	Calling-party name is not available
Calling-party name is available	<calling name> <calling number>	CALL FROM <calling number>
Calling-party name is not available	<calling name>	<incoming trunk name> <incoming trunk access code>

Note:

This enhancement is available only for H.323 and DCP endpoints.

Exclusion

With the Exclusion feature of Communication Manager, users can maintain privacy of telephonic conversations and ensure that unwanted parties cannot join the call.

You can use one of the following three modes to administer Exclusion on an endpoint:

- Manual Exclusion
- Automatic Exclusion
- Buttonless Automatic Exclusion

The Exclusion feature has been enhanced to work with the following features:

- Extension to Cellular
- Bridged Call Appearance
- Service Observing

Feature Name Extensions with Extension to Cellular

When you enable Extension to Cellular, you can activate certain Communication Manager features by dialing Feature Name Extensions (FNEs). Each FNE requires a direct inward dialing (DID) number and must comply with the dial plan. You can create the FNEs and administer the FNEs system wide.

With the Additional Security for an EC500/One-X Mobile Lite call (AEFSC) feature, when a user makes an FNE call from a cellular phone, the system authenticates the call with the station security code (SSC). The call fails without the valid SSC.

To make an EC500 call, the caller must dial the SSC after the FNE number. For example, <FNE>[Dial tone] <SSC># [Dial tone or confirmation tone] <Subsequent digit or extension>#.

Using FNE, if a caller wants to activate or deactivate a feature, the caller must dial the SSC after the FNE number. For example, <FNE>[Dial tone] <SSC># [Confirmation tone or Error tone].

For more information about FNEs, see the Setting up Feature Name Extensions set section.

Support for mid-call features

Communication Manager ensures that mid-call call telephony features work when Avaya endpoints establish video calls with Radvision endpoints.

Earlier, Radvision supported basic video calls between Radvision H.323 devices and Avaya H.323 and SIP devices. However, mid-call features were not fully supported. Activation of mid-call features sometimes caused the system to drop the video or the audio call.

With this enhancement, customers can use the following mid-call features during a video call:

- Video Mute and unmute
- Transfers
- Conferences

Wide-band video codec

Communication Manager now supports G.722 wideband audio codec between Radvision H.323 endpoints and SIP video and audio endpoints. Earlier, Communication Manager supported only G.711 and G.729 codecs due to which customers could not make optimum use of the rich audio features. From Communication Manager release 6.3.2 onwards, endpoints can directly negotiate their preferred wide-band audio setting of G.722.1, and offer rich audio experience.

Note:

Mid-call features do not work for calls between non-Radvision H.323 and Radvision H.323 endpoints functioning in a multi-Communication Manager environment.

Polycom® VVX support

Polycom® VVX 1500 is a video conferencing media phone with a touch screen. Polycom® VVX 1500 supports:

- H.323 and SIP protocols
- H.263 and H.264 video standards
- G.722, G.722.1 and G.722.1C audio codecs
- 6-line call appearances

Polycom® VVX 1500 integrates with Avaya Aura® by:

- Registering directly to Avaya Aura® Session Manager
- Registering to Polycom® DMA, which is registered to Communication Manager

Polycom® VVX supports the following mid-call features:

- Mute video and resume
- Mute audio and resume
- Hold and resume
- Blind transfer for audio
- Warm transfer for audio

Note:

Mid-call features do not work with Polycom® VVX 1500 that is H.323-registered to Polycom® DMA.

Polycom® DMA 7000 support

Communication Manager supports Polycom® DMA (Distributed Media Application) 7000, also known as RealPresence Virtualization Manager.

You can configure Polycom® DMA 7000 with Communication Manager. Communication Manager acts as an H.323 gatekeeper and uses H.323 trunks to connect to Polycom® DMA. In this configuration, you can also have other Polycom® video endpoints and RMX MCU H.323 configured to Polycom® DMA 7000, which is connected to Communication Manager through H.323 trunks. The Polycom® DMA gatekeeper replaces the Polycom® CMA gatekeeper.

In a configuration that includes Polycom® DMA, all Polycom® endpoints and MCUs must be registered to Polycom® DMA. You cannot have some Polycom® endpoints registered to DMA and some registered to Communication Manager or Session Manager.

The Avaya Aura® and Polycom® DMA configuration supports only audio-mute and resume mid-call features.

Note:

Polycom® DMA replaces Polycom® CMA only for the gatekeeper functionality. The management application is provided by the Polycom® CMA gatekeeper.

Encrypted SIP video support for point-to Point Calls

The upcoming release of Avaya Flare® (Release 1.2) and Avaya one-X® Communicator (Release 6.2) can be used to make secured point-to-point audio and video calls.

You can use the following modes for video calls:

- **No SRTP**: Audio and video calls are connected without any media encryption.
- **Best Effort SRTP**: If the call-originating endpoint supports SRTP and the receiving endpoint supports RTP, depending on the IP-codec-set administration, the call established is encrypted or un-encrypted. Thus, regardless of which media encryption is supported, both audio and video calls are connected. In this mode, SIP endpoints accept and negotiate RTP-only offers, SRTP-only offers, and RTP or SRTP best effort offers.
- **SRTP required**: If the call-originating endpoint supports SRTP, the receiving endpoint must acknowledge and support audio and video encryption using SRTP. If the other endpoint does not support SRTP, the video call is not established. SRTP must also work for audio-only calls. If the receiving endpoint cannot support the audio encryption, then the call is not connected.

Rules for SRTP in video signaling

- Communication Manager supports SRTP for video call flows only when the call-originating and the receiving endpoints are SIP-registered and the IP-codec-set administration on Communication Manager is SRTP.

  Note:

  SRTP for video does not work for H.323 signaling. H.323-registered endpoints always send video RTP. SIP-H.323 interworking with video encryption is not supported and video is blocked in this case. However, if the Best effort SRTP mode is selected,

Communication Manager allows video RTP to pass through in SIP to H.323 interworking.

- If an H.323 video endpoint originates an RTP call and the originating and the terminating endpoints send an RTP call, the system supports the audio and video calls only if the endpoints send RTP for both audio and video.
- If an H.323 video endpoint originates an SRTP call, the system does not support encrypted video calls.
- If an H.323 video endpoint sends audio as SRTP and video as RTP, the system supports audio and video calls.
- If a SIP video endpoint originates an RTP call and the terminating H.323 video endpoint sends RTP for audio and video, the system supports audio and video calls only if both the streams are RTP.
- If a SIP video endpoint originates SDES/CAPNEG SRTP call and the terminating endpoint is an H.323 video endpoint, the audio call is SRTP and the video is blocked.

Hardware

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.

DSP cards supported for G450

The G450 main board has four slots for VoIP engines. You can install up to two MP160 (Media Processor 160). An MP160 provides 160 channels for voice transport. Alternatively, if no standard voice is required, a maximum of 120 channels of V.150.1 call traffic is supported. A combination of voice calls and V.150.1 calls is supported as per the Avaya configuration guidelines.

Note:

The G450 supports up to 320 active channels for voice transport. You can install up to two MP160 modules, or a combination of Media Processor modules with a total of up to 320 channels for voice transport, for example, one MP160 and two MP80s.

Combination of cards	MP80	MP20	MP160
Combination 1	-	-	1 or 2
Combination 2	-	1 or 2	1
Combination 3	1 or 2	-	1
Combination 4	1	1	1

Special applications

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

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

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

Chapter 5: What's new in Session Manager

This chapter presents an overview of the new and enhanced features for Avaya Aura® Session Manager Release 6.3.4.

Define number ranges in Session Manager Dial-plan

In this release, Session Manager provides an enhanced Dial-plan administration feature. You can specify number ranges in the Session Manager Dial-plan to account for DID numbers that are not in blocks of 10, 100, or 1000.

You can enter a range that is a subset or superset of an existing range or pattern. The smaller range is called a sub-range. Sub-ranges have the following limitations within the same location and domain:

- Two sub-ranges must not match each other.
- A sub-range must not match a pattern.
- A sub-range must not cross the starting or end of another range.

Example

If the specified range is 5000:5499, you can specify the sub-ranges as:

- 5002:5011
- 5000:5499 and 5492:5499, where the end of sub-range and range match.
- 5000 (single entry) and 5000:5009, where the beginning of sub-range and range match.

The sub-range 5300:5555 is not valid because the sub-range crosses the end of the range.

To enable the Dial Plan Range feature in an enterprise system, all Session Manager installations need to be of version 6.3.4 and later.

For more information about the Dial Plan Range feature, see *Administering Avaya Aura® Session Manager Release 6.3*.

Session Manager support for Avaya SBCE Remote Worker

Using the Remote Worker feature, remote users can access the enterprise communication network through the public Internet and without VPN connectivity

For the Remote Worker configuration, Session Manager supports the following SIP endpoints.

- 96x1
- Avaya one-X® Communicator SIP
- Avaya one-X® Mobile SIP
- Flare Experience
- Avaya A175 Desktop Video Device
- B179 Conference Phone
- VDI Communicator

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

Session Manager firewall rule administration and maintenance enhancement

The Session Manager SIP firewall configuration feature provides an improved user interface to administer and manage SIP Firewall rule sets. You can assign the SIP Firewall rule sets to the selected Session Manager and Branch Session Manager instances. In this release, Session Manager SIP firewall provides the following enhancements:

- Simplify on-going maintenance of rule sets and rule settings, including automatic upgrade of default settings.
- Create named SIP Firewall rule sets specific to the Session Manager system.
- View the status of SIP Firewalls across all Session Manager systems, including the specific rule set that is deployed to each Session Manager and Branch Session Manager in the network.
- View SIP Firewall rule match counts for all Session Manager systems in the network.

Session Manager also runs a periodic audit to ensure that SIP Firewall is in a healthy and functioning state. Based on this audit, Session Manager:

- retrieves the state of the SIP Firewall (for example, empty, loading, running).
- resets the rule set to the default rule set and generates an event under the following conditions:
  - If the SIP Firewall Rule Set is found to be in the not assigned state (empty state).
  - If the SIP Firewall Rule Set has been in a loading state for more than five minutes (or for a complete maintenance cycle).

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

Flexible footprint for Session Manager on VMware

In this release, Session Manager offers a flexible footprint for a server configuration, based on the specific number of users supported for a customer deployment.

You can re-configure a Session Manager instance running on VMware to support one of the following user capacities:

- Up to 500 SIP users on a sunny day and up to 1000 users on a rainy day
- Up to 1000 SIP users on a sunny day and up to 2000 users on a rainy day
- Up to 2400 SIP users on a sunny day and up to 3000 users on a rainy day
- Up to 3500 SIP users on a sunny day and up to 4000 users on a rainy day
- Up to 4500 SIP users on a sunny day and up to 5000 users on a rainy day
- Up to 7000 SIP users on a sunny day and up to 8000 users on a rainy day
- Up to 10000 SIP users on a sunny day and up to 12000 users on a rainy day

For more information about configuring hardware resources for different user footprints, see *Session Manager using VMware® in the Virtualized Environment Deployment Guide*.

Session Manager CDR enhancements

Session Manager now generates Call Detail Recording (CDR) records for station to station calls, for reporting and billing. This is in addition to current trunk call CDR capabilities.

Session Manager provides the following CDR data file formats :

- The existing Session Manager 6.3 CDR flat file format. This format continues without any changes and allows customers to use their existing Session Manager CDR adjuncts without changes or updates.
- The new Session Manager 6.3.4 CDR flat file format. This format adds new data on the existing Session Manager 6.3.2 format. The most notable additions are as follows:
  - user to user (formally called as station to station) calls
  - incomplete calls
  - Tenant ID (where applicable)
- The new Session Manager 6.3.4 XML format. This new CDR format provides enhanced call records and enables CDR adjuncts to easily adopt any future changes in the CDR formats.

The new CDR formats provide enhanced call records and enable CDR adjuncts to easily adopt any changes in future CDR formats.

For more information about Call Detail Recording, see the chapter Call Detail Recording (CDR) in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Pluggable SIP adaptation modules

In SIP network configurations involving different elements, one of the major problems is interoperability among different SIP elements. The inherent flexibility of the SIP protocol leads to different SIP dialects and inconsistent implementations. To solve this problem, Session Manager provides a capability, called SIP adaptation modules, to selectively modify signaling messages, based on the interfacing SIP entity. Session Manager provides a number of adaptation modules to meet the broader and general inconsistencies or nuances of particular SIP elements.

These modules are also referred as the system Adaptation Modules, because these modules are packaged within the Session Manager software releases.

With Session Manager 6.3.4, Avaya has opened this interface so that Avaya Professional Services (APS) can develop adaptation modules.

Using this capability:

- APS can build custom adaptation modules to meet specific customer needs.
- Avaya can release these adaptation modules, independent of standard Session Manager software release cycles.

Inter Tenant Communication Control

Using the Inter Tenant Communication Control (ITCC) feature, customers can share the Avaya Aura® infrastructure across multiple user communities to reduce people, capital and operating costs. In a single Avaya Aura® infrastructure, ITCC provides segmented virtual systems to specific user communities. With ITCC, the system places restrictions on the communication between the segmented communities or, across tenant boundaries. The ITCC feature allows the user-to-user calls within the tenant boundaries. Any call targeted by a user to another user who is part of another tenant or to an external number, needs to be routed through a carrier SIP element. The system uses the user-to-Session Manager routing logic to route requests across tenant boundaries. This procedure of routing the requests also applies to other non-SIP methods that are routed based on the contents of the R-URI.

In addition to the routing requirements, the ITCC feature places restrictions on Contact Management.

In Session Manager, there are two types of contacts: an enterprise contact or internal contact and a private contact or external contact.

When the ITCC feature is enabled:

- A search request returns only the contacts that belong to the same tenant partition.
- Only contacts within the same tenant partitions are stored as internal contacts.
- A contact from a different tenant partition is stored as an external contact.
- Users in one tenant cannot see the presence state of or send IM messages to users in any other tenant unless they are added as external contacts.

Chapter 6: What is new in System Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® System Manager in Release 6.3.4.

Multi Tenancy

Using the Multi Tenancy feature, customers, also known as tenants, can share the same instance of the application, while allowing the tenants to manage users to fit the customer needs as if the application runs on a dedicated environment.

You can manage Multi Tenancy from System Manager Web Console. System Manager supports the following capabilities:

- View, create, edit, copy, and delete the tenant.
- View, create, edit, and delete tenant administrators for a tenant.
- View, create, edit, and delete the organization hierarchy of the tenant.
- View the tenant hierarchy on the Tenant Management page and User Management page.
- View the tenant associated with a user.
- Create and edit the user associated with a tenant from the User Management page.

System Manager provides a tenant administration dashboard that requires administrator credentials.

By default, the Multi Tenancy feature is disabled. You have to manually enable the Multi Tenancy feature. After enabling the Multi Tenancy feature, you cannot disable the feature.

User provisioning rule

The administrator can create rules called user provisioning rules. When the administrator creates a user by using the user provisioning rule, the system displays the default values, the communication addresses, and the communication profiles that are defined in the rule. The administrator need to provide minimal user information.

The administrator can provision the user by using the user provisioning rules from System Manager Web Console, Web services, directory synchronization, and bulk import services. You can assign only one user provisioning rule to a user.

System Manager supports creating, editing, duplicating, and deleting the user provisioning rule. You can use the User Profile Management user interface to associate the user provisioning rule with users while creating and editing users.

Virtualized Environment footprint flexibility

Virtualized Environment applications provide a fixed profile based on the maximum capacity requirements. Based on the number of supported users, System Manager offers a flexible footprint profile for customers who do not require the maximum capacity.

The customer can configure VMware CPU and RAM of the System Manager virtual machine based on the following capacity size categories:

- Profile 1 is the default profile that supports 35000 to 250,000 users.
- Profile 2 supports up to 35000 users.

The System Manager Multi Tenancy feature does not support Profile 2.

Backup integrity check

System Manager supports backup integrity check. This feature restricts the restoration of corrupted or tampered backup files on System Manager.

Common Servers Release 2.0 support

System Manager supports Release 6.3.4 deployments and upgrades on Common Servers Release 2 on System Platform.

Common Servers Release 2.0 includes HP ProLiant DL360p G8 and Dell™ PowerEdge™ R620.

Avaya does not sell Common Servers Release 1.0 anymore. However, you can use the Release 1.0 servers for software-only upgrades of System Manager.

Communication profile password complexity

For enhanced security of the system, the network administrator enforces the password strength policy for communication profile password complexity. The password must meet the standards.

By default, the system disables the communication profile password complexity feature. The administrator must enable this feature by using User Management.

Common console enhancements

For enhanced user experience, System Manager Release 6.3.4 provides the following common console changes:

- Color scheme changed to match with the look of Flare.
- Tabs moved from Left to Right.
- Descriptions for each link under User, Elements, and Services on the Login page are available as hover text making the page look clean.

Bulk import and export enhancements

Using System Manager, you can carry out:

- Bulk import of user information from an Excel and an XML file.
- Bulk export of user information to an Excel and an XML file.

  For import and export operations, use only the Excel template that System Manager supports. Microsoft Office Excel 2007 and later support bulk import and export in the .xlsx format. Do not change the Excel template format. The import or export operation might fail if you change the details of the headers in the Excel template.
- Bulk import and export of user information by using the System Manager Web Console.
- Tenant-based user provisioning.

Directory synchronization enhancements

System Manager supports the following directory synchronization enhancements:

- Bi-directional synchronization of the phone number and the mailbox number.
- Synchronization of the user provisioning rule data from the LDAP directory server to System Manager. You can map multiple LDAP attributes to the user provisioning rule.
- Synchronization of CS 1000 extensions and Communication Manager extensions from System Manager to LDAP directory server.

Support for the Collaboration Environment 2.0 element

System Manager supports Collaboration Environment 2.0 as an element and provides the following services:

- Central Authentication (SSO)
- Central Authorization (RBAC)
- Trust management (Certificate Management)
- Discovery and inventory
- Audit Log Collection
- Security Log Collection
- User Provisioning
- Alarm Management
- Serviceability Agent

Reports

System Manager supports the Reports feature.

Use Reports to:

- Generate Communication Manager object reports in various formats such as CSV, PDF, and HTML.
- Create and manage reports.
- Customize the contents of a report.
- Use a default or a custom template to create a report.
- Save reports in the System Manager server.
- View and delete reports that are stored in System Manager.
- Save reports to a local computer.
- Email reports to one or more addresses. You can configure an email server to send reports.

You can assign permissions for reports and generate reports for specific tenants.

Field-level RBAC

System Manager supports field-level RBAC for Communication Manager objects. You can assign permissions for the following Communication Manager objects:

Communication Manager object	Field
Endpoints	• Name • Security Code • IP Softphone • IP Video Softphone • EC500 State • EC500 Button • Coverage Path 1 • Coverage Path 2 • Tenant Number • Extension Number • Type • Port • Name • Lock Messages • Hunt-to Station

Communication Manager object	Field
	• BCC • TN • Location • Loss Group • Speakerphone • Display Language • Survivable GK Node • Survivable COR • Survivable Trunk Dest • Message Lamp Ext • Mute Button Enabled • Media Complex Ext • Short/Prefixed Registration Allowed • LWC Reception • LWC Activation • LWC Log External Calls • CDR Privacy • Redirect Notification • Per Button Ring Control • Bridged Call Alerting • Active Station Ringing • H.320 Conversion • 4Service Link Mode • Multimedia Mode • MWI Served User Type • AUDIX Name • IP Hoteling • Auto Select Any Idle Appearance • Coverage Msg Retrieval • Auto Answer • Data Restriction • Idle Appearance Preference • Bridged Idle Line Preference

Communication Manager object	Field
	• EMU Login Allowed • Per Station CPN Send Calling No • Audile Message Waiting • Display Client Redirection • Select Last Used Appearance • Coverage After Forwarding • Multimedia Early Answer • Direct IP-IP Audio Connections • Always Use • IP Audio Hairpinning • Remote Softphone Emergency Calls • Emergency Location Ext • Conf/Trans on Primary Appearance • Bridged Appearance Origination Restriction • Call Appearance Display Format • IP Phone Group ID • Hot Line Destination – Abbreviated Dialing List Number • Hot Line Destination – Dial Code • Feature Button Assignments 1 - 3 • Button types displayed to the Administrator
Service Hours Table	• Description • Use time adjustments from location
Holiday Table	• Name
Hunt Group	• Group Name • Group Extension • Group Type • TN • COR • Security Code • ISDN/SIP Caller Display • ACD • Queue

Communication Manager object	Field
	• Vector • Coverage Path • Night Service Destination • NM Early Answer • Local Agent Preference • LWC Reception • Audix Name • Message Center • Ignore Call Forwarding • Re-hunt On No Answer (rings)
Announcements	• Annc Name • Annc Type • COR • TN • Queue • Rate • Protected • Group/Board

Note:

Field-level RBAC is applicable only for the Edit operation.

Field-level RBAC is not applicable when you add Communication Manager objects.

Multi Tenancy for Communication Manager objects

With the Multi Tenancy feature, Communication Manager provides telecommunication services to multiple, independent groups of users through a single Communication Manager server. Each tenant appears to have a dedicated Communication Manager server, though in reality, the tenants share the same Communication Manager server.

As an administrator, you can gain access to one or more tenant partitions in System Manager, and you can administer tenant numbers for several Communication Manager objects. You can

segregate tenants through the tenant numbers. The following Communication Manager objects support the Multi Tenancy feature:

- Agents
- Announcements
- VDN
- Endpoints
- Term Extension Group
- Trunk Group
- Hunt Group

When a user is added to a tenant, the **Tenant Number** field is autopopulated for these Communication Manager objects.

The Communication Manager Objects page displays specific Communication Manager objects based on the tenant permissions and the Communication Manager permissions you specify.

Note:

For a particular Communication Manager instance, you must not assign the same tenant number for more than one tenant.

After the tenant administrator selects the site and the tenant from the Tenant Management Web console, the Communication Manager objects page displays a drop down with the tenant site combination. Depending on the tenant and site a user selects, the tenant range and tenant permissions take effect.

Multi Tenancy and tenant partitioning in Communication Manager

The native tenant partitioning feature of Communication Manager provides multiple services to independent groups of users through a single Communication Manager server. In addition to the tenant capabilities offered by Communication Manager, Communication Manager 6.3.2 offers two new features:

- Segmenting call processing and feature processing by the Inter-Tenant Communications Control (ITCC) feature.
- Tenant management of users and system administrators through System Manager.

System Manager Inter-tenant Communication Control (ITCC) enables Communication Manager to segregate features for each customer. System Manager tenants are shared across multiple adopters. Communication Manager is one of the adopters. Based on the roles and permissions assigned on the Communication Manager instances in a tenant, the Communication Manager objects are segregated for the tenant.

Chapter 7: What’s new in Branch Gateway

This chapter provides an overview of new features for Avaya Branch Gateway Release 6.3.1.

H.248 Registration Source Port

You can define the source port range that the gateway uses when registering with Communication ManagerCommunication Manager by using the following CLI commands:

- set registration source-port-range
- show registration source-port-range
- set registration default source-port-range

If you do not specify a range, the gateway selects a port within the default range of 1024 to 65535.

For more information about the CLI commands, see *CLI Reference Avaya Branch Gateway G450*, 03-602056 or *CLI Reference Avaya Branch Gateway G430*, 03-603234

Accessing diagnostic logs

This feature enables customers to securely capture diagnostic logs on the H.248 gateways. These diagnostic logs are sent to Avaya Support Representatives for troubleshooting and Root Cause Analysis (RCA). The diagnostic information is not intended for customers but captured so that Avaya Support Representatives can analyze the information and investigate the problem.

The following commands can be used to obtain diagnostic logs:

- show all logs
- show event-log
- system show reset-log
- show dev log file

For more information about CLI commands, see *CLI Reference Avaya Branch Gateway G450*, 03-602056 or *CLI Reference Avaya Branch Gateway G430*, 03-603234.

Chapter 8: What's new in Presence Services

This chapter provides an overview of the new and enhanced features for Avaya Aura® Presence Services 6.2.2.

Access Control List enhancements

Presence Services 6.2 enhances the support for Accept, Deny, and Revoke. You can set the ACL options by using Avaya Aura® System Manager Web Console.

Avaya Common Server

Presence Services Release 6.2 supports the next generation common servers, Dell™ PowerEdge™ R620 and HP ProLiant DL360p G8. Common servers are the rack-mountable servers that are based on the Intel Xeon ES2600 series processors, also called a Sandy Bridge.

For more information about the Dell™ PowerEdge™ R620 and HP ProLiant DL360p G8 servers, see the *Installing the Dell™ PowerEdge™ R620 Server* and *Installing the HP ProLiant DL360p G8 Server* guides on the Avaya Support website at, https://support.avaya.com.

Failover improvements

Presence Services 6.2 improves failover notifications in the following scenarios:

- When Presence Services restarts.
- When the TCP connection to Session Manager is not working.

Increased support for H.323 and SIP users

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.

Inter-Tenant Communication Control

Presence Services 6.2 supports Inter-Tenant Communication Control. For more information about Inter-Tenant Communication Control, see *Administering Avaya Aura® System Manager*.

Microsoft Exchange Calendar

Presence Services 6.2 supports Exchange Calendar that integrates with the Microsoft (MS) Exchange Enterprise deployment. Exchange Collector collects and publishes the Calendar and Out of Office Assistant information for Exchange Mailboxes.

Presence Services 6.2 supports the MS Exchange 2010 SP1 version of MS Exchange Mailbox server.

Simple Authentication and Security Layer

Presence Services 6.2 supports the Simple Authentication and Security Layer (SASL) framework for data security and authentication. SASL uses a number of mechanisms for the authentication process, such as EXTERNAL, ANONYMOUS, and DIGEST-MD5. Presence Services uses the DIGEST-MD5 mechanism to authenticate XMPP clients. In the DIGEST-MD5 mechanism, the system accepts the MD5 hash value instead of a user name and a password to authenticate the clients. The MD5 hash value is a hexadecimal number.

VE Footprint flexibility

Presence Services 6.2 supports VE Footprint flexibility for 1000, 2400, 5000, and 10,000 users. Use the following set of resources on the ESXi host before deployment:

CPU and memory requirements		
Maximum number of users	**CPU cores**	**Memory size**
1000	4	8 GB
2000	4	8 GB
2400	6	8 GB
3000	6	12 GB
4000	6	16 GB
5000	8	20 GB
6000	8	24 GB
7000	8	28 GB
8000	8	32 GB
9000	8	32 GB
10,000	8	32 GB
11,000	12	32 GB
12,000	12	32 GB

Avaya Security Gateway authentication

Presence Services Release 6.2 supports the Avaya Security Gateway (ASG) authentication for a secured Avaya Services access. The ASG authentication feature modifies the login credentials for a system. After you install Presence Services 6.2.2, the system sets up the following usernames:

- cust. The default password for the cust username is cust01. Use the cust credentials to log in to the XCP Controller Web interface.
- root. The default password for the root username is root01.

Improved presence behavior for legacy phones

Presence Services 6.2 supports publishing an away state for legacy phones. Legacy phones are the endpoints that are hosted by Avaya Aura® Communication Manager. Presence Services publishes an away state when a legacy phone is in an idle state for configurable amount of time.

In addition, Presence Services Release 6.2 supports publishing an offline state when a legacy phone logs out of the system. Presence Services also supports disabling the presence behavior of legacy phone for users with soft-clients or SIP phones that are capable of publishing their own presence states. For more information about presence states, see the *Administering Avaya Aura® Presence Services* guide.

Presence Services parameter change scripts

Presence Services Release 6.2 extends the support for the Presence Services parameter change scripts for the Virtualized Environment and Software-only deployments. Earlier, Presence Services supported the parameter change scripts only for the System Platform deployments.

Chapter 9: 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).

Geo Redundant High Availability

AE Services 6.3.1 with Avaya Aura® Contact Center 6.4 introduces the Geo Redundant High Availability feature, which is a high availability solution that works across two data centers with a pair of servers connected over a routable network. When the standby AE Services server is activated, AE Services will start providing service approximately a minute after the connectivity failure to the active server was detected. Geo Redundant High Availability is not state preserving. As a result, only the configuration data is copied from the active AE Services server to the standby server.

Using the AE Services Management Console, you can

- administer the preferred node. If a preferred node is administered, that node will become active when connectivity between the two data centers is reestablished. If a preferred node is not administered, the current active AE Services server remains active.
- manually start and stop Geo Redundant High Availability
- synchronize the active and standby servers

Note:

Data synchronization occurs automatically every two minutes.

- manually switch to the standby server (interchange)
- suspend and unsuspend Geo Redundant High Availability
- ping targets to gauge the health of the network and determine which AE Services server should be active

Three levels of licensing are available for Geo Redundant High Availability:

- Small
- Medium
- Large

Note:

Geo Redundant High Availability is only supported on the AE Services 6.3.1 on System Platform 6.3.1 offer. The AE Services server in each data center must be protected against hardware failure using System Platform's Machine Preserving High Availability (MPHA) mode.

Virtualized Environment Footprint Flexibility

In Release 6.3.1, the Avaya Application Enablement Services using VMware® in the Avaya Aura® Virtualized Environment offer allows you to configure the CPU and RAM of the virtual machine based on the number of available VMware licenses and the number of users to be supported. The AE Services 6.3.1 OVA template is built with a minimum resource consisting of 1 CPU and 2 GB of memory without CPU and memory reservation. CPU and memory reservation are required if you want to reach the advertised capacities (number of users and BHCC).

AE Services 6.3.1 supports the following footprint matrix.

Footprint	Microsoft Office Communicator /Microsoft Lync/ Sametime	Avaya Aura Contact Center (Agent)	DMCC (non-server media)	TSAPI, DLG, CVLAN
1 CPU 2GB	10K/6K BHCC	1K/20K	1K/9K BHCC (concurrent 10)	1K msg/s
2 CPU 2GB	12K/12K BHCC	2.5K/50K	2.4K/18K BHCC (concurrent 20)	1K msg/s
4 CPU 4GB	20K/24K BHCC	5K/100K	4K/36K BHCC (concurrent 20)	2K msg/s

Endpoint registration enhancements

In AE Services 6.3.1, DMCC, TSAPI, and JTAPI applications can receive endpoint registration state events that indicate when an H.323 and SIP endpoint has registered to and unregistered from a monitored station. These applications may also query for the H.323 and SIP endpoints registered at a station extension.

These new capabilities require Communication Manager 6.3 with Feature Pack 3 (that is, Communication Manager 6.3.2) or later.

AE Services 6.3.1 provides the following enhancements for endpoint registration events/query:

- **DMCC enhancements**

  DMCC can monitor the following updated events for each H.323 and SIP endpoint:

  - **EndpointRegisteredEvent**. There can be up to four events for a given station (three H.323 endpoints and one SIP endpoint).
  - **EndpointUnregisteredEvent**. There can be up to four events for a given station (three H.323 endpoints and one SIP endpoint).

  Using the **EndpointRegistrationInforRequest**, DMCC can retrieve information on all endpoints registered to a given station on Communication Manager. The information for up to four endpoints for the station can be in the same response.

- **TSAPI enhancements**

  The following new CSTA Private Status events are available for monitored station extensions with TSAPI:

  - **ATTEndpointRegisteredEvent**
  - **ATTEndpointUnregisteredEvent**

  TSAPI can query a monitored station extension using the new **attQueryEndpointRegistrationInfo()** escape service.

  These new events and query require ASAI Link Version 6 and Private Data Version 11.

- **JTAPI enhancements**

  The following new events are available for LucentV11AddressListeners:

  - **LucentEndpointEvent.ENDPOINT_REGISTERED_EVENT**
  - **LucentEndpointEvent.ENDPOINT_UNREGISTERED_EVENT**

  The following new events are available for AddressObservers:

  - **LucentEndpointRegisteredEv**
  - **LucentEndpointUnregisteredEv**

  JTAPI can query a registered endpoint using the new **TsapiAddress.getRegisteredEndpoints()** command.

  These new events and query require ASAI Link Version 6.

Support for the Avaya Common Server – Dell PowerEdge R620 server

AE Services 6.3.1 supports the Avaya Common Server – Dell™ PowerEdge R620 server.

Support for the Avaya Access Security Gateway (ASG)

AE Services 6.3.1 supports the Avaya Access Security Gateway (ASG), which is a challenge and response authentication mechanism. When the ASG is configured, the craft and sroot accounts will receive a challenge when logging into the AE Services server using SSH and the AE Services Management Console.

Support for the Microsoft Lync Server 2013

AE Services 6.3.1 supports Microsoft Lync Server 2013 and Microsoft Lync 2013 client (the full-featured client for Lync Server 2013). (Lync 2013 Basic client does not support Remote Call Control.)

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

F

G

I

L

M

N

O

P

R

S

T

U

V

W