What's New in Avaya Aura® Release 6.2 Feature Pack 4

Release 6.2 Feature Pack 4
03-601818
Issue 1
June 2014

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

License types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”, or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each 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
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

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

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

European Union Battery Directive

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

Japan

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

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

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment

(VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

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

If this is a Class B device:

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

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document provides an overview of the new and enhanced features of the following Avaya Aura® 6.2 Feature Pack 4 components:

- Avaya Aura® Communication Manager 6.3.6
- Avaya Aura® Call Center Elite 6.3.6
- Avaya Aura® Session Manager 6.3.8
- Avaya Aura® System Manager 6.3.8
- Avaya Aura® Presence Services 6.2.4
- Application Enablement Services 6.3.3

Intended audience

This document is for the following audience:

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

Related resources

Documentation

The following table lists the documents related to the components of Avaya Aura® Release 6.2 Feature Pack 4. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Implementation			
18-604394	*Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394	Describes the procedures to install System Platform, license and authentication files, and Communication Manager 6.3.6.	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 6.3.6, 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 6.3.6.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
—	Administering Avaya Aura® System Manager	Describes the procedures for configuring System Manager Release 6.3.8 and the Avaya Aura® applications and systems	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Document number	Title	Description	Audience
		managed by System Manager.	
—	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 by using System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
555-245-207	Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware devices that can be incorporated in a Communication Manager telephony configuration.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Maintenance and Troubleshooting			
03-300431	Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers	Provides commands to monitor, test, and maintain hardware components of Avaya servers and gateways.	Solution Architects, Implementation Engineers, Sales Engineers,

Document number	Title	Description	Audience
			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 **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 4 components, select 6.3.x.
5. Click **Enter**.

   Note:

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

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

Training

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

Course code	Course title
Avaya Aura® core implementation	
1A00234E	Avaya Aura® Fundamental Technology
4U00040E	Avaya Aura® Session Manager and System Manager Implementation
4U00030E	Avaya Aura® Communication Manager & CM Messaging Implementation
10U00030E	Avaya Aura® Application Enablement Services Implementation
8U00170E	Avaya Aura® Presence Services Implement and Support
AVA00838H00	Avaya Media Servers and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop Labs
Avaya Aura® core support	
5U00050E	Session Manager and System Manager Support
5U00060E	ACSS - Avaya Aura® Communication Manager and CM Messaging Support
4U00115I 4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.x to R6.x)
1A00236E	Avaya Aura® Session Manager and System Manager Fundamentals
Avaya Aura® core administration and maintenance	
9U00160E	Avaya Aura® Session Manager for System Administrators
1A00236E	Avaya Aura® Session Manager and System Manager Fundamentals
5U00051E	Avaya Aura® Communication Manager Administration
5M00050A	Avaya Aura® Communication Manager Messaging Embedded Administration, Maintenance & Troubleshooting

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support web site, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, 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.

Note:

Videos are not available for all products.

Avaya Aura® 6.2 Feature Pack 4 components

Product component	Release version
Communication Manager	6.3.6
Communication Manager Messaging	6.3.6
Session Manager	6.3.8
System Manager	6.3.8
Branch Gateway	6.3.6
Presence Services	6.2.4
Application Enablement Services	6.3.3
Call Center Elite	6.3.6
System Platform	6.3.4

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

The Avaya Aura® Suite licensing offers a flexible ordering approach to address solution-oriented options for Avaya Aura® customers. Suite licenses bundle select Avaya Aura® features to provide a simpler approach for partners to order the best enterprise solution for their customer. Suite licenses can be mixed within any enterprise so key features can be supplied to those users that need them the most.

As new collaboration options are introduced, existing Suite bundles might be modified. Effective from 1 June 2014, Avaya Agile Communication Environment™ (ACE) entitlements will no longer be part of any Foundation, Mobility or Collaboration bundles. Orders placed prior to that date will still include ACE, and any existing customers will maintain the entitlements. The Avaya Agile Communication Environment™ entitlements are still available to any customer as an a la carte option. For more information, contact your Avaya Partner or Avaya Account Representative.

Chapter 3: What's new in Communication Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® Communication Manager 6.3.6.

Avaya one-X® Communicator Display and Log to show E164+

Communication Manager 6.3.6 adds a plus sign (+) instead of the international access code digit to the incoming or connected ISDN number when the number appears on the designated Avaya one-X® Communicator endpoint. The endpoint displays the number in the E.164 format, with a leading plus sign (+). For example, an incoming call from 0004969910 appears as +4969 on the display and is stored in the same format in the call log. Thus, a user can re-dial the number from the call log directly, without having to add the location access codes, for example, 0 or 9 for external calls and 00 or 011 for international calls.

Communication Manager applies the following rules to add the plus sign (+):

Numbering type	Prefix
E.164/national	Local E.164 country code associated with the ISDN trunk group location
E.164/subscriber	City/Area code and local E.164 country code associated with the ISDN trunk group location
Private or unknown	Unchanged

To enable this feature, set the following fields on the Location Parameter screen to a value other than **no**:

- **Replace International Access Code with '+'**
- **Convert ISDN Public Numbers to International for Display**

Note:

SIP stations are excluded because Communication Manager does not control the display of SIP stations. To add the plus sign (+) for incoming or connected ISDN calls to SIP stations, administer the SIP Signaling Group and SIP Trunk Group screens.

Inter-gateway Alternate Routing for SIP Endpoints

Inter-gateway Alternate Routing (IGAR) provides voice connectivity using a public service provider (PSTN) if not enough bandwidth is available on the private network. If the Corporate Data Network cannot handle the call, the bearer connection is routed over the Public Voice Network.

In previous releases, IGAR does not work with SIP endpoints. Starting with this release, you can use IGAR when calling to or from a SIP endpoint that is registered to a Session Manager.

The IGAR triggers include:

- The inter-branch bandwidth limit is reached.
- IGAR is “always on” for branches with low-bandwidth connectivity.

The source and destination of the call must be associated with the same Communication Manager. Video calls are automatically downgraded to audio if IGAR is triggered.

Use Cases

- Case #1: Vijay in Bangalore and Michael in London both have SIP endpoints and are served by Communication Manager. At peak hours, bandwidth between Bangalore and London is insufficient to carry audio calls with proper quality. With IGAR, Communication Manager automatically sends the audio media over the PSTN, ensuring excellent audio for the call.
- Case #2:

  An enterprise has a small branch gateway in Reykjavik with all SIP endpoints registered to an Avaya Aura® data center in Stockholm. The low-cost data connection to Iceland has insufficient bandwidth to carry more than a few audio calls. With IGAR, every call to or from Reykjavik is carried over a low-cost PSTN connection using the “always on” option.

DSP resource reduction for Avaya one-X® Communicator SIP endpoints

In the Telecommuter mode, the Avaya one-X® Communicator SIP endpoints use up to four DSP resources for every call: 2 DSP resources for each leg of the call. This design prevents

SIP glare conditions and call setup delays because the SIP endpoint and Communication Manager, both act as controllers.

The enhancement for Avaya one-X® Communicator SIP endpoints operating in the Telecommuter mode addresses the conditions where the endpoint can shuffle the telecommuter callback number to the called party when the Direct Media feature is ON. Therefore, the use of DSP resources on the MedPro board is reduced.

If the Avaya one-X® Communicator endpoint supports shuffling and Communication Manager direct media feature is enabled, the SIP telecommuter endpoint processes the new call flows. For example, endpoints A and B send invites to each other simultaneously, and A receives the invite from B before the response to the invite sent earlier. With the shuffling support feature, the new invites are not rejected. Call flows for Hold, transfer, conference, and any kind of re-invites or glare conditions are processed by the endpoint.

If the Avaya one-X® Communicator SIP endpoint does not support shuffling and the **Direct Media** setting on Communication Manager is OFF, the endpoint processes the old call flows and rejects any new invite.

Video SRTP and TLS support with Scopia 8.3

TLS and SRTP encryption is supported between Session Manager and Scopia® solution products, providing higher security within mixed Scopia® solution and Avaya Aura® environments. This support is available with the upcoming Scopia 8.3 service pack.

The MCU, a device used to bridge videoconferencing connections, can encrypt communications with endpoints to create secure connections with H.235-based encryption for H.323 endpoints and SRTP and TLS encryption for SIP endpoints.

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. 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.

For more information about administering SRTP for video signaling, see *Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504*.

Limit Number of Concurrent Calls for SIP endpoints

The Limit Number of Concurrent Calls (LNCC) feature causes a multi-call appearance endpoint to behave as a single line appearance endpoint. When the LNCC feature is enabled and the user is active/busy on one call appearance, subsequent incoming calls receive a busy signal and are tagged as missed calls.

LNCC already works on all H.323 and DCP endpoints. With this release, the LNCC feature extends to any SIP endpoint that supports call appearances.

A user controls this feature using a feature button or feature access code (FAC). Normal operation allows two incoming calls. The user must enable LNCC to allow only one call.

LNCC allows:

- outgoing calls, incoming priority calls, and emergency callback for SIP stations.
- outgoing calls, incoming priority calls, emergency callback, and crisis alert for H.323 and DCP stations.

LNCC works with the Dual Registration and Multiple Device Access features. The user applies LNCC at the user level, and all devices associated with the user inherit the LNCC feature.

For example:

- Most of the time, Steve wants to be active on only one call at a time, so he activates LNCC.
- Andy calls Steve, and they talk for 15 minutes.
- During their conversation, Cindy calls Steve. Because LNCC is active, Cindy’s call goes right to coverage.
- Cindy does not leave a message, but Steve’s endpoint still records her call as a missed call. Steve calls Cindy after he finishes his conversation with Andy.

EC500 Call Suppression enhancement

This enhancement is an extension of the SIP dual mode feature introduced in Communication Manager Release 6.3.0. In Communication Manager Release 6.3.6, this feature extends to Client Enablement Services (CES) users as well and is also known as EC500 Call Suppression.

When a call is made to a SIP extension that uses a dual-mode mobile client and has a CES profile associated with it, the SIP extension receives two calls: a SIP call and a cellular call. The SIP extension shows an incoming SIP call for initial one to two seconds. Before the user accepts the call, the SIP extension receives a cellular call from Communication Manager.

With the introduction of EC500 Call Suppression feature, the dual-mode client applications, such as Avaya Aura Communicator for Android, receive only a single incoming call on the mobile phone for that particular extension. EC500 Call Suppression ensures that users receive an alert either by a VoIP call or a cellular call, but never both.

When we register the dual-mode client, Communication Manager determines that the client is logged in and can answer the call, and therefore, does not fork the call to the cellular extension through GSM network. When the dual-mode client moves out of the Wi-Fi zone, Communication Manager waits for a response from the client. If Communication Manager receives a response within four seconds, the call is not forked to the EC500 extension. If Communication Manager does not receive a response from the dual-mode client within four seconds, Communication Manager forks the call to the mobile phone through the GSM network. Communication Manager forks the call to the EC500 extension even if the dual-mode client is logged off.

The following scenarios show the real-time application of EC500 Call Suppression. These scenarios require remote access.

- You are commuting and have configured the application to use the EC500 service. Also, you do not have Wi-Fi or cellular data access to Avaya Aura®. In this case, the EC500 service redirects all incoming calls on the deskphone to the mobile phone network.
- After you reach home, you can connect to the home Wi-Fi network and use the VoIP service. You continue to receive all incoming calls directed to the deskphone on the mobile phone by using the home Wi-Fi network over SIP. In this case, the server suppresses the EC500 cellular call to the mobile phone based on the use of VoIP.
- If you register the mobile phone to a Wi-Fi network and move outside the network, the mobile phone connects automatically to the cellular data network. You continue to receive incoming calls to the deskphone on Avaya Aura Communicator for Android using SIP. In this case, the server processes that the application is using the VoIP service and suppresses the EC500 cellular call to the mobile phone.

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

T.38 fax during audio

With the T.38 fax during audio feature, Communication Manager supports the transition of an existing SIP audio call to a fax call.

In the T.38 mode, gateway DSP devices or G650 VoIP boards convert T.30 signals into T.38 packets and send the converted packets to a peer. If the fax endpoint on the far end supports T.30 signaling, the peer converts the packets back into T.30 signals and pass them to the fax endpoint. However, if the fax endpoint supports the T.38 protocol, the peer passes on the packets directly to the fax endpoint.

T.38 is the preferred industry standard fax protocol. H.323 and SIP trunks support the T.38 protocol. Communication Manager uses the T.38 protocol for fax transmission over IP network facilities. Communication Manager cannot initiate or receive a fax call directly. Communication Manager can only support the transition of an existing audio call to a fax call.

During an audio call, Communication Manager performs one of the following operations when a request for establishing a fax call is received:

- If T.38 is administered, Communication Manager accepts the fax call and disconnects the audio call.
- If T.38 is not administered, Communication Manager rejects the fax call.

Communication Manager does not support a fax call and an audio call simultaneously. The gateway at the near end converts the analog fax streams into T.38-defined data packets. The gateway at the far end converts the T.38-defined signals into analog fax streams and transmits the streams to the receiving analog device.

For more information about T.38 fax enhancement, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205

Team button enhancements

A Team button is a button that has two generic functions: a display function and an execution function.

With the display function, a member of the team (monitoring station) can observe the station state of another team member (monitored station). The station state of the monitored station is a combination of active calls and ringing calls on the station.

With the execution function, a member of the team can use a Team button as a Speed Dial button or Pick-Up button. Depending on the state of the monitored station, a user can:

- establish a call directly to the monitored station.
- pick up a ringing call from the monitored station.

This release introduces the following enhancements to the Team button:

- **Direct Transfer**: Transfer an active call by pressing the Team button. The call automatically is put on hold and the transfer-destination (monitored station) is called. The user does not need to press the transfer button.
- **Transfer Upon Hangup**: Complete a transfer operation by hanging up the phone without the need to press the **Transfer Complete** button.
- **Override the Monitored Station’s Forwarding**: The Monitoring Station can override the redirection of the monitored station. If the monitored station does not answer within a certain amount of time, the system redirects the call according to the redirection policy of the monitoring station.

Feature operation and control are the same for H.323 and SIP. COR and station flags that control the new functionality are now applicable for SIP Team buttons.

The Team button is supported on 1XC 6.2 and 96X1 SIP 6.2.4.

Scopia 8.3 interoperability

The Scopia 8.3 solution provides the following features:

- **Avaya Scopia XT brand**: the following Scopia products have moved under the Avaya brand:
  - Scopia Elite MCU 6000
  - Scopia Management
  - Scopia Management
  - Scopia Desktop Client
  - Scopia Mobile
  - Scopia XT4200 and 5000
  - Scopia XTE240
- **Netsense, H.264 HiP, and SVC with FEC**: supported across the board with our Elite 6000 MCU and the latest XT series as well as the mobile and desktop clients
- **New Gallery Layout**: for a shared view of live video and content on a single video stream now supported by our Elite 6000 MCU
- **Scopia Desktop**: provides new methods for data sharing with improved presentation quality, especially in low quality network conditions
- **H.264 Hip and XTD virtualization**: for small-to-medium-sized (SMB) offerings. Also available for IP Office users
- **Enhanced reporting**: available on Scopia Management
- **XT meeting control GUI**: for enhanced room meeting experience

SIP undelivered call notification

The SIP undelivered call notification feature provides a notification about an undelivered call to the endpoint. The endpoint log this call entry in the missed call log.

Communication Manager sends the undelivered call notification when a call is made directly to an endpoint but is not delivered to it. The following features trigger this notification:

- All call appearances are busy
- Limit Number of Concurrent Calls is enabled and the endpoint is busy
- Call Forward Busy or Call Forward All is enabled
- Enhanced Call Forward (ECF) unconditional or ECF busy is enabled
- Cover All Calls is enabled

This feature does not require any administration on Communication Manager or Session Manager and is available to the users by default. However, the **Enable Layer 3 test** field must be set to `y` on the signaling group between Communication Manager and Session Manager so that Communication Manager can understand the capabilities of Session Manager.

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

Support for increase in number of digits in call logs

Communication Manager displays up to 21 digits of the calling-party number on a DCP, an H.323, or a SIP endpoint. Earlier, Communication Manager displayed up to 17 digits of the calling-party number.

Endpoints store all 21 digits in the missed call log or the answered call log, as appropriate. This feature applies to direct calls to the endpoint and to calls that are redirected to an endpoint due to Call Coverage, Call Forwarding, or a Bridge Call Appearance.

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

Administrable Timers for One–X Mobile VM Detection

Use the Configuration Set screen to define call treatment options for One-X Mobile calls. With FP4, three new configuration set options are available beyond the normal 99, to control feature behavior: **onex**, **mobile-onex**, and **callback-onex**.

Note:

In the One-X mobile environment, you can edit the values of only the **Cellular voice mail detection** , **Confirmed Answer**, and **Call log notify** fields. All other fields are read-only.

Enhanced support for SIP Contact Centers on failed outgoing ISDN calls

When a Voice Portal agent makes a call to a PSTN user and the call is routed over an ISDN trunk and if the PSTN disconnects the call before the called party can answer, the PSTN might send an indication to Communication Manager to delay the call drop until the PSTN completes playing an announcement or tone to the caller. The delay in call drop keeps the Voice Portal agent busy while the announcement or tone is being played to the caller, even though the agent cannot actually hear the announcement or tone.

With Communication Manager Release 6.3.6, you can use the **Interworking of ISDN Clearing with In-Band Tones** field on the **SIP Trunk** form to communicate the reason of the call drop to the caller.

After knowing that the called party will not answer the call, the caller or the Voice Portal agent can decide whether to end the call immediately or wait for the announcement or tone to complete.

If you set the **Interworking of ISDN Clearing with In-Band Tones** field to **drop-with-sip-error**, Communication Manager sends the reason for the call being dropped by the called party.

If you set the **Interworking of ISDN Clearing with In-Band Tones** field to **keep-channel-active**, the call drop is delayed till the complete announcement or tone is being played to the caller.

Full Communication Manager release string in MST trace

Earlier, MST traces included the Communication Manager release strings only for major and minor releases, for example, 6.2, 6.3, and 7.0. From Communication Manager Release 6.3.6, MST files also capture internal release strings along with major and minor release string. This enhancement helps in identifying the currently activated patch ID on the system when a particular trace is captured.

The MST file contains the complete Communication Manager Release string, including the Service Pack number. When you run the list trace command, the messages in the trace buffer display the complete Communication Manager string.

The format in which the release string appears is *Major.Minor.ServicePack.SpecialRelease-ServicePackID-InternalBuildNumber*. For example, for Communication Manager Feature Pack 4, the MST trace will show the following string: `6.3.2.0.124-xxxxx`, where xxxxx represents the Service Pack ID.

Online/Offline Call Journal (Call History) for H.323 endpoints

Previously, the H.323 phones were responsible for maintaining the call logs. As long as the users were logged in to the phone, the phone backed up all call logs. After the user logged out and logged back in, the phone pulled the previously stored call logs. However, these logs did not contain incoming calls that took place while the user was logged out. This behavior led to confusion as all the registered devices did not show the same call logs if the user was logged in to some devices and not others.

From Communication Manager Release 6.3.6, call logs include the incoming calls even when the device is in the logged-out state. This support is available to the latest H.323 endpoints.Communication Manager stores up to 10 entries for the most recent calls for the user. When the user logs back in, Communication Manager sends these log entries to the phone. The H.323 phone reconciles the call logs it receives from Communication Manager with the logs it restores from the backup server. The H.323 phone backs up the merged call logs in the central backup file for later retrieval. The H.323 phones back up the call logs to an HTTP server and load whenever a user logs in.

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

Password complexity enhancement

Starting Release 6.3.6, the new password policy allows customers to have a more secured password with the flexibility of using different character combinations in usernames. :

The password policies apply to settings that use the Linux Pluggable Authentication Modules (PAM) for authentication on the virtual machine on which Communication Manager runs. PAM provides dynamic authorization for applications and services in a Linux system. This feature does not impact password authentication used by phones and trunks.

Linux allows all-digit usernames, but Communication Manager previously required at least the first character of a username to be a letter. With the new policy, customers can have usernames with all-digits, all-letters, or any combination.

The password complexity options can be configured on the **Login Account Policy** page in Communication Manager System Management Interface.

The available username and password configuration options:

- All-digit usernames are allowed.
- Minimum password length.
- Required numbers of digits, lowercase letters, uppercase letters, and special characters.
- Number of old passwords that cannot be reused.
- Number of sequentially repeated characters allowed.
- Number of characters in the new password that must differ from the old password.
- Password must contain at least one uppercase character, a lower case character, a special symbol, and a number.
- Check against dictionary words.

VMware enhancements

With Communication Manager Release 6.3.6, you can:

- Deploy Communication Manager on VMware vSphere ESXi 5.5.
- Configure IPv6 to specify the IPv6-compliant IP addresses.

For information about VMware software requirements and IPv6 configuration, see *Deploying Avaya Aura® Communication Manager on VMware® in Virtualized Environment*.

Security enhancements

With the Communication Manager Release 6.3.6 security service patch, you can receive and validate the certificate that uses the SHA-2 signing algorithm and 2048 bit RSA keys. Using Communication Manager System Management Interface, you can import the third-party trusted certificate that uses the SHA-2 signing algorithm.

Note:

To obtain the security service pack details, go to the Avaya Support website at http://support.avaya.com.

For information about certificates, see *Avaya Aura® Communication Manager Security Design*, 03-601973 and *Administering Avaya Aura® Communication Manager*, 03-300509.

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 4: What’s new in Session Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® Session Manager Release 6.3.8.

Security enhancements: Removal of Default Certificates

Starting with Session Manager Release 6.3.8, default certificates are no longer supported for new installations. Default certificates, also known as demo certificates, are non-unique identity certificates which were automatically installed on newly shipped Session Manager servers. Default certificates are not secure and do not meet current NIST standards (SHA–256 hashing and 2048–bit RSA keys).

New Session Manager servers no longer use the default certificates that were Avaya SIP Product CA issued. New customer networks can request an Identity Certificate from the System Manager Trust Management that is signed by the System Manager Certificate Authority.

For upgrades, Session Manager preserves the previous certificate. If a demo certificate was in use in the previous release, the certificate is preserved through the upgrade.

Existing customers who either need to replace a Session Manager server or want to add a Session Manager to an existing network of Session Managers can download old certificates. However, Avaya recommends that customers use the newer certificates as soon as possible.

To manage certificates:

- Use the new Identity Certificate issued by System Manager (default).
- Use third-party ID certificates.

Security enhancements: NIST Support

The National Institute of Standards and Technology (NIST) develops cryptographic standards for the United States government. NIST recommends that starting in 2014, the digital signatures of Identity Certificates use the SHA–2 signing algorithm and 2048–bit encryption keys. NIST requires at least 2048 bit keys. Customers have the option to create larger keys, such as 4096.

Starting with Release 6.3.8, Session Manager:

- uses SHA–256 and 2048–bit RSA keys for signing new Identity Certificates by default.
- uses SHA–512 for passwords.

A new Connection filter, **Non-Compliant NIST TLS Only:**, helps users identify non-NIST compliant connections. The filter appears on the Security Module Status page. New fields on the page include:

- **Cert Sign**
- **Key Exch**
- **Encryption**
- **MAC**
- **TLS Version**

These fields display the following status for NIST SP800–131a compliance:

- **Acceptable**
- **Deprecated**
- **Disallowed**
- **Not Approved**
- **Restricted**
- **Unknown**

Transport Layer Security

Session Manager Release 6.3.8 supports Transport Layer Security (TLS) 1.2.

TLS 1.2 provides:

- a higher level of security than earlier versions to protect users from known attacks.
- flexibility for defining cryptography algorithms.

The TLS protocol provides three essential services to all applications running above it: encryption, authentication, and data integrity.

By default, Session Manager uses TLS 1.2. If the other end of the connection cannot use TLS 1.2, Session Manager reverts to TLS 1.0.

You can view the TLS version on the Connection Status page in the **Transport** field.

Session Manager Scale increases

For Avaya Common Servers Release 1, HP supplies the HP ProLiant DL360 G7 servers and Dell provides the Dell™ PowerEdge™ R610 servers.

For Avaya Common Servers Release 2, HP supplies the HP ProLiant DL360p G8 servers and Dell supplies the Dell™ PowerEdge™ R620 servers.

Using an Avaya Common Servers R2 server, you can significantly increase the capacity of a single Session Manager. A VMware footprint identifies the capacities of the R2 server.

A distinction no longer exists between SIP users and SIP devices. Instead, only SIP devices are used for determining Session Manager capacities. Capacities decrease in scenarios where a device has a larger impact than a typical device. For example, Call Center Agents subscribe to an additional package.

Session Manager on Common Server R1 supports:

- 10,000 SIP users during normal operations
- a maximum of 12,000 SIP users in a failover scenario
- 100 sessions per second (360K per hour)
- 90K simultaneous sessions

Session Manager on a Common R2 Server supports:

- 21,500 SIP devices during normal operations
- a maximum of 25,000 SIP devices in a failover scenario
- 150 sessions per second (540K sessions per hour)
- 160K simultaneous sessions

A Session Manager configuration supports up to 12 interconnected Session Managers.

Up to 125K SIP users or 150K SIP devices are supported by any N+M sparing Session Manager configuration consisting of Common Server R2 or comparably sized VMware servers. The customer must adequately distribute devices across primary and secondary servers to accommodate the configuration. For example, the typical Session Manager solution with N+1 sparing supports 150K SIP devices across 7 Session Managers for a single Session Manager failure. Similarly, a dual data center (N+N) supports 150K SIP devices across 12 Session Managers (6 in each data center).

Online/Offline Call Journal (Call History) for SIP endpoints

Previously, SIP endpoints maintained the logs locally while the endpoints were logged in. When a SIP user logged in from a different device, in addition to the calls received in the logged-out state, the old call logs stored in a different device were not visible.

Starting with Session Manager Release 6.3.8, the call log of a device includes incoming calls when the device is not logged in. In addition, if a call cannot be delivered to an endpoint due to the Limit the Number of Concurrent Calls (LNCC) feature, the calls is also logged. For SIP endpoints, the primary Session Manager stores all call logs and downloads the logs to the endpoint during login. The endpoint maintains the logs locally when the device is logged in.

Call logs are only stored on the primary Session Manager of the user. There is no redundancy for storing call logs. The primary Session Manager stores the call logs in the User Data Storage database.

You enable **Call History logging** on the Session Manager Communication Profile for the user by enabling **Enable Centralized Call History**. The default is **off**. The maximum number of call logs per Communication Profile is 100.

Related topics:

User Data Storage and Call History Management GUI changes on page 36

User Data Storage and Call History Management GUI changes

A new column, **User Data Storage Status**, displays on the Session Manager Dashboard page. The status indicates the state of the User Data Storage connection and the server. The **User Data Storage Status** displays dashes (**--**) for Session Managers running releases earlier than 6.3.8.

Selecting a Session Manager instance and clicking on the associated **User Data Storage Status** link displays the **User Data Storage Status** screen. Using this screen, you can manage, monitor, backup, and restore User Data Storage data on the configured Session Managers.

System Manager Web Services

See the description for *System Manager Web Services* in the *What’s new for System Manager* chapter.

Role Based Access Control (RBAC) for Routing Web Services

The SMEM/NRP resource type now includes Routing Web Services access. By default, the following built-in System Manager roles have access to the Web Service:

- System Administrator
- Security Administrator
- Session Manager Administrator
- Routing Administrator

Enhanced Session Manager Application Sequencing

Starting with Session ManagerRelease 6.3.8, implicit sequencing definitions can be applied to SIP users.

Avaya recommends that customers segregate the Implicit User applications from the Explicit User applications. SIP users are administered as Explicit Users. Non-SIP users are administered as Implicit Users. Unless the enterprise SIP users and non-SIP users have completely different number prefixes, customers might see inadvertent Implicit User applications invocation for the SIP users. To avoid such issues, the implicit sequencing definition for SIP users feature is disabled by default.

New SIP Entity types

Session Manager Release 6.3.8 supports **Collaboration Environment** and **Media Server** as SIP Entity types.

The new types appear in the **Type** drop-down menu when a user creates a new SIP Entity on the SIP Entities page.

SIP Phone Configuration template

Starting with Avaya Aura® 6.2 Feature Pack 4, Avaya supports pre- or post-configuration of phone settings and button assignments. Administrators can centrally configure SIP phone settings from System Manager that were previously only accessible from the SIP phone device. Administrators can standardize specific SIP phone button configurations and terminology without having to rely on employees to make the phone configuration changes or having to dispatch a technician to make the changes local to the SIP device. Settings include:

- Button Label fields on SIP Phones defined by the administrator.
- Favorite Key check box to enable specific buttons to appear on the device home page.
- New Phone Settings, such as Call Setting Options, Screen and Sound Options, and Language/Region Settings.

You can change the Phone Settings and Button Assignments by using the:

- UPM Communication Manager Endpoint Profile Endpoint Editor screen.
- Communication Manager Manage Endpoint screen.

Using the 96x1/1XC phone GUI, you can change the button label and the **favorite** status of the button. You cannot change the button type.

The following are the supported use cases for the SIP Phone pre-configuration template:

- Create a new custom template from an Avaya-provided default template.
- Apply a template to a new user.
- Apply a template to an existing user.
- Modify endpoint settings for an existing user.
- Modify endpoint settings for a group of existing users.
- User can make an update that overrides the template settings.
- Remove a template.

The following use cases are *not* supported at this time:

- Apply a template to a group of existing users.
- Update a template and propagate the changes to all users ad devices assigned to that template.

Phone Settings:

- 14+ parameters are available to set or change.
- SIP endpoints:
    - remove phone settings the endpoint does not use or understand.

- remove badly formatted settings.

- replace any missing settings with default values.

- All AST phone buttons are configurable with personal labels, and most buttons can be configured as favorite buttons.

This feature supports the 96x1 endpoints, including the 9611 and 9641. Default phone templates already exist in the System Manager database. Users can create custom templates using the default templates.

Team Button enhancements

See the description for *Team Button enhancements* in the *What's new for Communication Manager* chapter.

Limit Number of Concurrent Calls for SIP endpoints

See the description for *Limit number of concurrent calls* in the *What's new for Communication Manager* chapter.

Inter-gateway Alternate Routing for SIP Endpoints

Inter-gateway Alternate Routing (IGAR) provides voice connectivity using a public service provider (PSTN) if not enough bandwidth is available on the private network. If the Corporate Data Network cannot handle the call, the bearer connection is routed over the Public Voice Network.

In previous releases, IGAR does not work with SIP endpoints. Starting with this release, you can use IGAR when calling to or from a SIP endpoint that is registered to a Session Manager.

The IGAR triggers include:

- The inter-branch bandwidth limit is reached.
- IGAR is “always on” for branches with low-bandwidth connectivity.

The source and destination of the call must be associated with the same Communication Manager. Video calls are automatically downgraded to audio if IGAR is triggered.

Use Cases

- Case #1: Vijay in Bangalore and Michael in London both have SIP endpoints and are served by Communication Manager. At peak hours, bandwidth between Bangalore and London is insufficient to carry audio calls with proper quality. With IGAR, Communication Manager automatically sends the audio media over the PSTN, ensuring excellent audio for the call.
- Case #2:

  An enterprise has a small branch gateway in Reykjavik with all SIP endpoints registered to an Avaya Aura® data center in Stockholm. The low-cost data connection to Iceland has insufficient bandwidth to carry more than a few audio calls. With IGAR, every call to or from Reykjavik is carried over a low-cost PSTN connection using the “always on” option.

VMware support enhancement

Starting Release 6.3.8, you can deploy Session Manager on VMware vSphere ESXi 5.5.

For more information about VMware software requirements, see *Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment* .

Chapter 5: What's new in System Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® System Manager in Release 6.3.8.

Common console enhancements

For enhanced user experience, System Manager Release 6.3.8 provides the following common console changes:

- Provides the **Settings** icon (🔧) to navigate to **Help**, **About**, and **Change Password** links.
- Provides the feature to add a corporate logo on the web console.
- User Preference: You can add a page as your preference by using the plus sign (+) in the top-right corner. The web console displays the link to the page to System Manager. You can delete the user preferences.
- Quick Navigator: You can type the name of the link that you want to search. The web console displays all related links with the search text in the top-right corner of the page. You can click a link to navigate to the specific page.
- The look and feel of the UCM webpages matches with System Manager webpages.

Bulk import and export enhancements

System Manager supports:

- Granular export with user attribute filtering options
- More than one communication profile set
- User provisioning rule name for a user
- Changing login name by using bulk user import using XML and Excel
- Import and export of all attributes of Communication Manager station communication profile by using the Excel file

- Import and export of the Collaboration Environment communication profile by using the Excel file
- Import and export of the CallPilot communication profile by using the Excel file
- Import and export of the Presence communication profile by using the Excel file

Directory synchronization enhancements

LDAP synchronization and authentication with Active Directory 2012.

Scheduler enhancements

System Manager supports:

- Scheduling of the sequential jobs
- Rerunning of the failed jobs
- Rescheduling the failed jobs

Security enhancements

System Manager supports:

- Generation of SHA-2 algorithm-based certificates
- Generation of certificates by using 2048 key size
- Subject Alternative Name for certificate generation. Enables Subject Alternative Name values in the URI format for all System Manager-CA issued identity certificates.

VMware enhancements

With System Manager Release 6.3.8, you can deploy System Manager on VMware vSphere ESXi 5.5.

WebLM enhancements

- Centralized licensing on VMware in Virtualized Environment on System Manager WebLM
- WebLM generates a warning when a system administrator installs a new license file without the non-capacity feature that was present in the existing license file. The system prompts the administrator to confirm or cancel the license file installation. If the administrator chooses to continue, WebLM proceeds with the new license file installation after logging the warning event.

  The log includes details of the license installation, the user name of the person installing the license, and the status whether the administrator confirmed or cancelled the warning. This enhancement applies to the standalone WebLM and System Manager WebLM.

  For example, the customer might have a non-capacity feature, such as ASAI on Communication Manager (FEAT_CM_ASAI_PCKG), in the installed Communication Manager license file on WebLM. When this customer tries to install a new license file without this feature, the customer gets a warning message. The message is to confirm whether the customer intentionally dropped this feature from the license file.

Reports

Avaya Aura® System Manager supports the Reports feature for communication objects. System Manager 6.3.8 added about 350 predefined List and Display Communication Manager configuration reports.

Use Reports to:

- Generate Communication Manager object reports in various formats such as CSV, PDF, and HTML.
- Create and manage reports.
- Edit report parameters.
- Rerun reports.
- Customize the contents of 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 custom user.

Discover survivable servers

Create profile and discover SRS and SCS servers

Use the **Create Profiles and Discover SRS/SCS** option to automatically discover survivable remote servers (SRS) and survivable core servers (SCS) from the main Communication Manager. System Manager uses the **`list survivable-processor`** command to discover the SRS and SCS servers that are associated with the main Communication Manager. The servers that are discovered are stored in **Inventory** > **Manage Elements**.

Additionally, the SRS and SCS servers are automatically added in the System Manager inventory. The Communication Manager servers are automatically identified as survivable servers in **Inventory**.

Software Management

Software Management, a centralized upgrade solution, provides an automatic upgrade of Communication Manager and associated devices, such as Gateways, TN boards, and media modules from a single view. The centralized upgrade process minimizes repetitive tasks and reduces the error rate.

The Software Inventory page consists of a collective inventory of different devices arranged in a hierarchy.

When more than one element is selected within a hierarchy, the system creates one scheduler job for the upgrade. Each hierarchy can have only one job scheduled. The system determines the sequence in which the elements must be upgraded. The devices might include:

- Communication Manager
- Communication Manager Messaging
- Utility Server
- Branch Session Manager
- Gateways
- TN Boards
- Media modules

If one of the devices fails to upgrade within the hierarchy, the system might proceed or process the job as failed based on the compatibility of the failed device with the subsequent device.

Important:

> You cannot select Communication Manager 5.2.1 and System Platform-based Communication Manager 6.x together. You can upgrade either Communication Manager 5.2.1 systems together or all System Platform-based Communication Manager 6.x systems.

You can perform the following operations by using Software Inventory:

- Get Inventory.
- Analyze software.
- Download.
- Perform a preupgrade check.
- Reset or backup Communication Manager.
- Sequence upgrades.
- Upgrade the following:
    - System Platform-based Communication Manager 6.x
    - Communication Manager 5.2.1
    - All devices and components that run on Communication Manager
- Commit, rollback, or cancel the template upgrade.

Important:

> Note that you cannot perform updates by using the **Software Management** > **Software Inventory** link.
>
> However, you can perform the following operations by using **Manage Software** > **Communication Manager**:
>
> - Update Communication Manager, SAMP firmware, and MPC firmware.
> - Upgrade Communication Manager 5.x to 5.2.1.
>
>   **Note:**
>
>   Install System Platform on the supported server before you upgrade Communication Manager.
> - Upgrade Gateways, TN boards, and media modules.

Avaya Enterprise Short Messaging element

System Manager supports Avaya Enterprise Short Messaging as an element and provides the alarm management service.

NRP sync feature

By using the NRP synchronization feature, users with H.323 phones can move between offices and have appropriate E911 routing for their location.

For the NRP sync feature, ensure that the authoritative Communication Manager **IP Network Region** information is configured in the Session Manager routing table. A Communication Manager server is authoritative for a location if the location contains media gateways and SIP endpoints that are administered on that Communication Manager server.

Therefore, if you make any change to the **IP Network Map** for the **IP Network Region** that are controlled by Communication Manager, the updates are automatically detected. These updates are replicated to the corresponding **Location** entries in the Session Manager routing table.

Simplified Communication Manager upgrades

Avaya Aura® System Manager Release 6.3.8 Software Management has enhanced infrastructure to simplify and automate Avaya Aura® Communication Manager upgrades.

Customers and business partners can avail the following benefits while performing Communication Manager upgrades:

- Fully automated upgrade from Communication Manager Release 6.0, 6.1, and 6.2 to 6.3.6 by using Software Management. System Platform and the Communication Manager template and patches are automatically upgraded from System Manager.
- Partially automated upgrade from Communication Manager Release 5.2.1 to 6.3.6. System Platform is not automatically installed as part of the upgrade. Only the Communication Manager template and patches are automatically upgraded from System Manager when you install System Platform on the supported server.

- Preupgrade checks to ensure that the Communication Manager hardware and IP network environment support the Communication Manager upgrade. This function increases, the rate of successful upgrade.
- Job sequencing and job chaining of all Communication Manager component upgrades, which minimizes the wait time and delay between different upgrade tasks. For example, upgrades of media modules, TN Boards, and gateways that are associated with the upgraded Communication Manager. The result is a faster Communication Manager upgrade.
- Eliminated or reduced human intervention during the upgrade of Communication Manager and associated elements, reducing the potential for errors.
- Starting and monitoring upgrades that centrally reduces or eliminates the need for onsite visits
- Scheduling of Communication Manager upgrades during off-hour maintenance windows, with System Manager performing the entire upgrade.

Communication Manager templates

Using System Manager Software Management, you can upgrade the following Communication Manager templates:

- Duplex CM Main/Survivable Core with SAL and Communication Manager.
- Simplex CM Main/Survivable with SAL,Communication Manager, Communication Manager Messaging, and Utility Services.
- Simplex Survivable Remote with SAL, Communication Manager, Branch Session Manager, and Utility Services.
- Embedded CM Main with SAL, Communication Manager, Communication Manager Messaging, and Utility Services.
- Embedded Survivable Remote with SAL, Communication Manager, Branch Session Manager, and Utility Services.

You can use the templates in both the fully automated process and the partially automated process. However, in the partially automated process:

- You cannot upgrade System Platform from Software Management. This upgrade rule is applicable for upgrade from Communication Manager 5.2.1 to Communication Manager 6.3.6 on S8800, S8510, and the 8300D.
- To automatically upgrade the Communication Manager template and patches from System Manager, you must install System Platform. This rule is applicable for upgrade from Communication Manager 5.2.1 to Communication Manager 6.3.6 on S8800, S8510, and the 8300D.

For more information about the two processes, see Simplified Communication Manager upgrades on page 46.

Supported servers

For full and partial automated upgrades, you can perform upgrades on the following Avaya Aura® Communication Manager servers:

- Servers that support upgrade of Communication Manager 6.0, 6.1, and 6.2 to Release 6.3.6:
    - S8510 with increased 8GB memory and HDD
    - S8800 with increased 8GB memory and HDD
    - S8300D
    - Common Server R1 Dell R610, HP DL 360 G7
    - Common Server R2 Dell R620, HP DL 360p G8
- Servers that support upgrade of Communication Manager 5.2.1 to Release 6.3.6:
    - S8510 with increased 8GB memory and HDD
    - S8800
    - S8300D

Software Management infrastructure enhancements

Avaya Aura® System Manager provides the following infrastructure enhancements to simplify the Communication Manager upgrade process and to support other Avaya Aura® applications in future releases of System Manager:

- System Manager collects all the needed upgraded information from the administrator at the beginning of the upgrade process workflow. Communication Manager and other Avaya Aura® applications then do not need to continually interact with System Manager during a Communication Manager upgrade.
- Where possible, steps that are part of the System Platform and Communication Manager templates upgrade are automated.
- The Element Inventory page in Software Management shows all Communication Manager instances, gateways, media modules, TN boards, and System Platform server information in a single hierarchical view. In previous versions of Software Management,

all elements were on separate tabs. Administrators can now select the Communication Manager instances and associated elements to be upgraded.

- The Element Inventory page provides a list of common element information in a single table structure, for example, hardware, platforms, release, and versions.

System Manager also provides the following new features:

- New SNMP Access Profile configuration area : To centrally configure access credentials for an SMNP discovery. This feature is added to the System Manager web console and is now a part of the Software Management discovery and inventory process.
- Preupgrade checks: To ensure that all aspects of the upgrade environment are correct. The checks are as follows:

  - RAID battery check
  - Hardware compatibility check
  - Required files download check
  - CDOM credentials check
  - Disk space check
  - Sufficient memory check
  - Version compatibility check
  - Version compatibility check
  - Bandwidth is sufficient check
- Rollback and Failure Scenario feature options: To run **Auto Rollback** for the Communication Manager template that has a System Platform error during the upgrade process.

  A Manual **Rollback** / **Commit** option is available if the **Auto Commit** option is not selected during the upgrade. The **Rollback** / **Commit** feature applies to Communication Manager 6.x Release upgrades.
- Simultaneous upgrade: For System Manager Software Management to simultaneously upgrade a maximum of five Communication Manager and all associated elements.

Chapter 6: What's new in Presence Services

This chapter provides an overview of the new and enhanced features for Avaya Aura® Presence Services Release 6.2.4.

Support for the Do Not Disturb presence state

Presence Services 6.2.4 supports the Do Not Disturb (DND) presence state.

If a user enables DND:

- Watchers of the user can see the presence state as DND.
- The Presence server archives all incoming IMs and delivers the archived IMs to the user after the user deactivates DND.
- The Presence server redirects all incoming calls to the coverage path of the user.

High Availability

Presence Services 6.2.4 supports High Availability (HA) in a clustered setup. With HA, each user configured in a cluster can be assigned a primary and a backup Presence server.

Enabling HA for an N-node cluster requires N+1 Presence servers with N primary servers and 1 backup server. The value of N can range from 1 to 8.

For more information, see *Deploying Avaya Aura® Presence Services* and *Deploying Avaya Aura® Presence Services on VMware® in Virtualized Environment*.

Inter-Domain Presence Services to Presence Services federation

Presence Services 6.2.4 supports federation between non-clustered single Presence Services instances that are on separate Avaya Aura® systems and use different domains. For more information, see *Administering Avaya Aura® Presence Services*.

IBM® Domino® Calendar integration

Presence Services 6.2.4 supports Domino Calendar that integrates with the IBM® Domino® Enterprise deployment. The Presence server collects and publishes the Calendar and Out of Office information for Domino Mailboxes and uses this information to determine the presence state of users.

Presence Services 6.2.4 supports Domino Server 8.5.3.

For more information, see *Administering Avaya Aura® Presence Services*.

Multiple Domain support

Presence Services 6.2.4 supports multiple presence domains on a single Presence Services system. This feature enables the exchange of presence information between different domains. For more information, see *Administering Avaya Aura® Presence Services*.

SHA2 support

Presence Services 6.2.4 accepts Root Certificate Authority (CA) certificates and generates server certificates by using the SHA256 signature algorithm with a 2048 bit key.

Support for increased H.323 and SIP user capacity

Presence Services 6.2.4 supports up to 16,000 H.323 and SIP users on a single node and up to 125,000 SIP and H.323 users with a cluster of 8 nodes.

Support for the Lync integration in a clustered deployment

Presence Services 6.2.4 supports the federation of a clustered Presence Services deployment with Lync Server 2013. With this feature, the Presence Services cluster can exchange data with the Lync Edge system.

Support for Presence Services cluster deployment on VMware

Presence Services 6.2.4 supports the deployment of a Presence Services cluster on VMware and support up to eight Presence Services nodes in Virtual Environment.

VMware enhancements

With Presence Services Release 6.2.4, you can deploy Presence Services on VMware vSphere ESXi 5.5. For more information about VMware software requirements, see *Deploying Avaya Aura® Presence Services on VMware® in Virtualized Environment*.

Chapter 7: What’s new in Application Enablement Services

This chapter provides an overview of the new features and enhancements for Application Enablement Services (AES) Release 6.3.3.

Virtual IP Address for Geographic Redundancy High Availability

Earlier, AE Services 5.2 supported Fast Reboot High Availability (FRHA) and AE Services 6.2 supported Machine Preserving High Availability (MPHA).

AE Services 6.3.3 supports Geographic Redundancy High Availability (GRHA). With GRHA the limitations of cross over cables and dependence on System Platform is removed and the only prerequisite is the quality of the LAN or WAN between the data centres. AE Services 6.3.3 offers two options of GRHA:

- System Platform deployment with AES MPHA at one or both sites if preferred or otherwise a non HA AES
- VMware deployment

Earlier, the client application used two different IP addresses - one IP to connect to the primary AE Services GRHA server and another IP to connect to the secondary AE Services GRHA server. The client application was responsible to determine which AE Services GRHA server was active, and to connect to the active server using the appropriate IP address.

With AE Services 6.3.3, the client application uses one IP address to connect to either of the AE Services GRHA servers. If the primary AE Services GRHA server stops working, the virtual IP address is automatically assigned to the secondary AE Services GRHA server. You can configure the virtual IP address from the **High Availability Configuration** page in the **Eth0 Virtual IP Address** field.

The use of the virtual IP address has significant advantages:

- The client application can use the same IP address to connect to the active AE Services GRHA server. The client application does not have to maintain two different AE Services server IP addresses.
- If the virtual IP address is also used for the Switch Connectivity and Media Connectivity, any Device Media Call Control (DMCC) associations that are currently in place at the time of a GRHA fail-over will be automatically recovered by the new active AE Services server. The associations include: DMCC client sessions, DMCC devices and device monitors, DMCC station registrations, DMCC call associations, and DMCC system registrations.

✱ **Note:**

For GRHA, the active and standby servers are synchronized every minute. Thus, if there is an unplanned fail-over, any new associations or other changes made within the last minute may not be synchronized. In that case, these last-minute changes will not be recovered by the new active server.

For more information about Virtual IP Address for Geographic Redundancy High Availability, see *Avaya Aura® Application Enablement Services Administration and Maintenance*.

VMware enhancement

AE Services 6.3.3 adds the following for VMware:

- Support for the AE Services vApplication for VMware version 5.5.
- Support for the AE Services Geographic Redundancy High Availability (GRHA) feature on VMware.

For more information about GRHA, see *Avaya Aura® Application Enablement Services Administration and Maintenance*.

Improved support for contact center events

In AE Services 6.3.3 and ASAI Link release 7, the number of digits in the address of the Calling Party Number and the Connected Number is increased to 21. The number of digits for ASAI Link release 1 to 6 is still limited from 1 to 15 digits.

With this enhancement, the maximum limit the **Minimum Length** field, **Maximum Length** field, **Delete Length** field on Add Dial Plan-default page and Add Dial Plan – Switch Administration page is increased to 21 digits.

For more information about Add Dial Plan-default page and Add Dial Plan – Switch Administration page, see *Avaya Aura® Application Enablement Services Administration and Maintenance*.

Improved consistency between station call logs and CTI applications

In AE Services 6.3.3 and later, with the combination of Avaya Aura® Feature Pack 4 and ASAI Link version 7, the ASAI Call Redirected event, the ASAI Busy/Unavailable event, and the Reorder/Denial event now include the optional information elements mentioned in the table.

Element	Description
Calling Party Number IE	The extension number of the calling party
Redirecting Number IE	The extension number of the station from which the call is redirected
Redirection Number IE	The extension number to which the call is redirected
Cause IE	The reason why the call is redirected
Party ID IE	The party ID of the calling party

AE Services 6.3.3 with the support of ASAI Link Version 7 or later provides the following enhancements for CTI events.

- CVLAN enhancement: The CVLAN client library supports new optional IE values added to the ASAI Redirected event report event.
- TSAPI enhancement: The TSAPI Link supports the new optional IE values added in the ASAI Call Redirected event reports. The system uses the IE values to set CSTA Diverted event parameter values. The TSAPI service and TSAPI clients support a new private data version 12. The ATT Diverted Event now includes number of the calling party.
- JTAPI enhancement: The JTAPI Service negotiates private data version 4-12 when connecting to TSAPI Service Link administered with ASAI Link Version 7 or later. When the CSTA Diverted event from the TSAPI Service sends the confirmation, the JTAPI middleware converts the CSTA Diverted event into the equivalent JTAPI LucentV12DivertedEvent.
- DMCC enhancement: The DMCC Call Control Service negotiates private data version 12 while connecting to TSAPI or JTAPI administered with ASAI Link Version 7 or later. When the CSTA-1 Diverted event from the TSAPI Service sends the confirmation, the DMCC service converts the CSTA-1 Diverted event into the equivalent CSTA-3 Diverted event. The DMCC service forwards the CSTA-3 Diverted event to the appropriate DMCC clients.

For more information about TSAPI links, see *Avaya Aura® Application Enablement Services Administration and Maintenance*.

Chapter 8: What's new in Call Center Elite

This chapter provides an overview of the new and enhanced features of Call Center Elite Release 6.3.6.

Improved reporting of SIP trunks

SIP agent deskphones must have dedicated SIP trunk groups for:

- Call traffic with service providers and other Communication Manager servers.
- Call signaling with Session Manager.

Furthermore, Call Management System (CMS) or Avaya IQ must not measure Off-PBX Station (OPS) SIP trunk groups that carry signaling data because signaling data is inconsistent with the format of call traffic data. Sharing of SIP trunk groups and measuring of signaling data can lead to loss of call traffic data and reporting errors.

To prevent data loss and reporting errors, Communication Manager, starting with this release, does not send station signaling-related messages to CMS or Avaya IQ. Furthermore, if CMS or Avaya IQ measure OPS SIP trunk groups, Communication Manager logs a `measured SIP OPS` denial event.

For more information, see *Administering Avaya Aura® Call Center Elite* and *Using Avaya 96X1 SIP Agent Deskphones with Avaya Aura® Call Center Elite*.

New fields to match agent and skill partitions

Businesses that provide hosted contact center services can increase their cost advantage by sharing resources with multiple tenants. For example, service providers can share the maximum skill capacity of 8000 skills on a single Communication Manager instance with multiple tenants. However, sharing of resources presents problems related to voice and data security. For example, delivery of calls to unintended tenants is a breach in security.

With the Match Agent and Skill Partitions feature, administrators can ensure that calls for one tenant do not flow to another tenant. Communication Manager prevents the assignment of skills with Tenant Numbers (TNs) for which agents must not receive calls.

To apply administrative restrictions, this feature provides the following optional fields on the Agent LoginID screen:

- **Check skill TN to match LoginID TN**: Administer this field to ensure that Communication Manager delivers calls based on TN assignments. Thus, agents within a tenant partition receive calls for skills in the same tenant partition.
- **Include Tenant Calling Permissions**: Administer this field for extended intertenant call delivery where agents can receive calls for more than one TN.

  If you grant tenant calling permissions to an agent, you can assign skills with TNs for which the agent can receive calls.

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

Tenant number capacity increase

Businesses that provide hosted contact center services can increase cost advantage by sharing resources with multiple tenants. In this release, the tenant number capacity on a single Communication Manager instance is increased from 100 to 250 tenants.

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

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

Note:

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

Signing up for PCNs and PSNs

About this task

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