What's New in Avaya Aura® Communication Manager, Communication Manager Messaging, and Session Manager Release 6.2

Release 6.2
03-601818
Issue 6
July 2012

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the following Web site: http://www.avaya.com/support.

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 Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Product Safety Standards

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

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

This product may contain Class 1 laser devices.

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:

Note:

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

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

Equipment With Direct Inward Dialing ("DID"):

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

Proper Answer Supervision is when:

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

Permissible exceptions are:

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

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

Automatic Dialers:

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

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

Toll Restriction and least Cost Routing Equipment:

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

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

For equipment approved prior to July 23, 2001:

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

For equipment approved after July 23, 2001:

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

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

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

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX.

The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

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

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

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

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

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

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

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

Installation and Repairs

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

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

FCC Part 68 Supplier's Declarations of Conformity

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

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

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

Canadian Conformity Information

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

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

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

European Union Declarations of Conformity

CE

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

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

European Union Battery Directive

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

Japan

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

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

If this is a Class A device:

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

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

If this is a Class B device:

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

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: About this document

Overview

This document provides an overview of the new and enhanced features for Avaya Aura® Communication Manager, Avaya Aura® Communication Manager Messaging, and Avaya Aura® Session Manager.

Audience

This document is for the following audiences:

- Avaya Contractors
- Avaya Employees
- Channel Associates
- Remote Support
- Sales Representatives
- Sales Support
- On-Site Support
- Avaya Business Partners

Using this document

Use this document to obtain a high-level information on the new and enhanced features for the current release of Avaya Aura® Communication Manager, Avaya Aura® Communication Manager Messaging, and Avaya Aura® Session Manager. For information on the required feature, see the index or table of contents to locate the page number where the information is described.

Downloading this book and updates

About this task

You can download the latest version of this documentation from the Avaya Support website at http://support.avaya.com. You must have access to the Internet and a copy of Adobe Reader installed on your personal computer. Avaya makes all possible efforts to ensure that the information in this book is complete and accurate. However, information can change after we publish this documentation. Therefore, the Avaya Support website might also contain new product information and updates to the information in this book. You can also download these updates from the Avaya Support website.

To download the latest version of this documentation:

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. At the top of the page, click the **SEARCH AVAYA SUPPORT** text box.
3. In the Search text box, type the documentation number `03-601818` and click the arrow button.
4. In the resulting list, locate the latest version of this document.
5. Click the document title to view the document in PDF format.

Related resources

For more information on any of the features in this document, see:

- *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.
- *Avaya Aura® Communication Manager Screen Reference*, 03-602878.
- *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.
- *Avaya Aura® Session Manager*, 03-603324.
- *Implementing Avaya Aura® Communication Manager*, 03-603558.
- *Administering Avaya Aura® Communication Manager*, 03-300509.

- *Upgrading Avaya Aura® Communication Manager*, 03-603560.
- *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

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.

Trademarks

Sending comments

Avaya welcomes your comments on this book. You can send your comments to: infodev@avaya.com. In the comment section, mention the name and number of this document, What's New in Avaya Aura® Communication Manager, Avaya Aura® Communication Manager Messaging, and Avaya Aura® Session Manager, 03-300684.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. On the Avaya Support website at http://support.avaya.com, search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to help answer questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Chapter 2: What's new in Communication Manager

This chapter presents an overview of the new features and enhancements for Avaya Aura® Communication Manager 6.2, which runs on the S8300D, S8510, S8800, HP ProLiant DL360 G7, and Dell™ PowerEdge™ R610 servers.

SIP to H.323 Direct Media

Communication Manager uses the SIP to H.323 Direct Media feature to directly connect SIP stations or SIP trunks to H.323 stations, without using a media resource and shuffling the call.

When a call connects, the Direct Media feature signals a direct talk path from a SIP station or a SIP trunk to an H.323 station. The Direct Media feature can be activated on the Signaling Group screen, in the **Initial IP-IP Direct Media** field. To establish a direct path during a call setup, SIP stations and H.323 stations must use the same IP version, IPv4 or IPv6.

The benefits of using the SIP to H.323 Direct Media feature are:

- Elimination of the SIP to H.323 call shuffling after the call connects
- Elimination of clipping on the talk path
- Decrease in the number of signaling messages for each SIP to H.323 call
- Early detection of the media path in the call flow and use of fewer media processor resources to configure the system
- Reduction in the processing time of each SIP-H.323 call, and increase in the SIP Busy Hour Call Completions (BHCC) capacity

For more information on the **Initial IP-IP Direct Media** field, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

SIP INFO out-of-band DTMF digit processing

The out-of-band option sends all outgoing DTMF messages as SIP INFO messages. When the out-of-band option is activated, Communication Manager sends SIP INFO messages over a SIP signaling group.

The out-of-band option is interoperable with H.323 networks. This option connects an Avaya non-SIP endpoint or trunk to a voicemail system on the H.323 network. The voicemail system is connected to Communication Manager and Avaya Aura® Session Manager through SIP.

For more information on the out-of-band option, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

International CPN Prefix

To convert the incoming and outgoing ISDN numbers to international format and to support international ISDN number configurations, CPN prefixes are added to the calling numbers, based on the location from where the call has originated.

The **International Access Code** field is associated with the location of the trunk on which the calling number arrives. The **International Access Code** field is administered on the Locations Parameter screen. If the **International Access Code** field is blank, Communication Manager fetches the international CPN prefix from the Feature Related System Parameter screen and adds the CPN prefix to the calling party number.

If the existing administrator option, **Passed Prefixed CPN: ASAI**, is activated, the ASAI client displays the calling party number with the CPN prefix. If deactivated, the ASAI client displays the calling party number without the CPN prefix.

For more information on the **International Access Code** field, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

For information on the International CPN Prefix feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Look Ahead Routing for 404 and 407 SIP Messages

When any far-end returns SIP call failure errors such as 407 (Not Found) or 404 (Proxy Authentication required), Communication Manager initiates look ahead routing (LAR), if LAR is set up correctly for the routing pattern.

Signaling group usage for SIP signaling groups

You can administer a procr near-end for SIP signaling groups the same way you administer procr near-end for H.323 signaling groups. The near-end procr set up for signaling groups works with the survivable remote, the survivable core, or the main server.

VDN option for DID/Tie/ISDN/SIP intercept treatment

The Vector Directory Number (VDN) option of the **DID/Tie/ISDN/SIP Intercept Treatment** field is now available to route incoming invalid calls to the specified VDN.

For information on the **DID/Tie/ISDN/SIP Intercept Treatment** field, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

Call preservation for Communication Manager

A Failover Group is a group of two active Session Manager instances interconnected to ensure high availability of Session Manager services. A route pattern mechanism and a failover group domain mapping mechanism are used for call preservation during a network outage. You can administer up to nine failover domains in the Failover Group Domain Mapping (failover-grp-domain-map) table.

For preferred domain names, you can define the primary and the inverse failover groups and match them with Session Manager administration.

For more information, on call preservation administration, see *Call Preservation Administration Case Study*.

Related topics:

Session Manager call preservation for contact centers on page 29

Connection Preserving Migration of SIP trunks on H.248 gateways

The Connection Preserving Migration (CPM) feature preserves existing bearer (voice) connections when a branch gateway migrates from one Communication Manager server to another because of network or server failure. However, users on connection-preserved calls

cannot use features such as Hold, Conference, or Transfer. During Avaya's complementary recovery strategies, CPM extends the time period for recovery operations and functions. CPM is also supported for SIP trunks on H.248 media gateways. CPM keeps the SIP trunks on Local Survivable Processor (LSP) or Enterprise Survivability Server (ESS) in-service after the media gateway has migrated to another Communication Manager server.

Exceptions

1. Calls that do not use branch gateway resources and are shuffled to Direct-IP are not preserved.
2. SIP signaling states are not preserved for re-constructed calls. The signaling connection for the SIP call is lost as the media gateway moves over to LSP. Therefore, for re-constructed calls, the switch software does not retain signaling call states.
3. Calls that pass directly through Session Manager and not through Communication Manager are not preserved as a part of CPM call.

For more information on connection preserving migration, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Conference Factory URI

Conference Factory URI feature enables seamless integration of Session Manager with conference capabilities of conference products, such as Avaya Aura® Conferencing, Meeting Exchange, Communication Manager, and SIP endpoints, including Avaya Desktop Video Device. This feature provides enhanced experience for participants in conferences and enables richer collaboration when using voice, video, and text conference systems.

For more information, see *Administering Avaya Aura® Session Manager*, 03-603324.

Service Observing Next Call Listen Only Access Code

The Service Observing Next Call Listen Only Access Code feature is used in a call center environment where a service observer needs to monitor the observed entity. The observed entity is not notified of call monitoring, which means that there is no warning tone played and no delay when the service observer joins the call.

The service observer cannot join an active call by using this service observing feature, but can join and observe the next call. The observer can monitor calls that are routed to:

- An extension, a Vector Directory Number (VDN) on system call vectoring
- An agent who is using systems with expert agent selection

⚠ Warning:

Listening to the call of another user can be subject to federal, state, or local laws, rules, or regulations. You might need to obtain the consent of one or both of the parties on the call. Ensure that you know, and comply with, all applicable laws, rules, and regulations when you use this feature. Provision of the service observing warning tone while observing may be required in some cases. Use of the “Next Call” FAC or button will not apply warning tone even if it is enabled for other forms of service observing and should not be used when observing calls that require the warning tone. In some cases the playing of an announcement before the call is put in queue stating that the call may be subject to monitoring will meet the legal requirements.

For more information on the Service Observing feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Microsoft Office Communicator integration

The integration of Microsoft Office Communicator (MOC) with Communication Manager supports bridging or answering two calls simultaneously: an active call on a desk phone and an active call on an off-PBX destination, such as a mobile phone. MOC is integrated with Communication Manager by activating the **MOC Control** field on the Class of Service screen. Off-PBX Telephony Integration and Mobility (OPTIM) applications, such as CSP, EC500, PBFMC, SPFMC, and Avaya one-X® Client Enablement Services, support this feature.

With the integration of MOC, although a call to the off-PBX phone appears to be on hold to the MOC client and the desk phone, the call can be attended on both, the off-PBX phone and the desk phone. Once the off-PBX station disconnects the call, Communication Manager disconnects the call at the off-PBX phone as well as the desk phone. However, if the same call is bridged to the off-PBX phone from the desk phone, you need to manually disconnect the call at the off-PBX phone as well as the desk phone.

For more information on administering office telephones for Extension to Cellular, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Support for Internet codec G722.2

To support high-quality audio over low-bandwidth links and also to support 96x1-series SIP Release 6.2 codec, Communication Manager provides signaling support for the G.722.2 wideband codec. The G.722.2 codec uses a 16 KHz sampling frequency and an adaptive and variable bit rate, ranging from 6.6 Kbps to 23.85 Kbps. The G.722.2 codec does not support media resources, such as Medpro and branch gateways. Communication Manager uses the G.722.2 codec to enable SIP and H.323 endpoints for direct IP calls.

For information on Administering IP Codec set, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Group Paging

SIP phones support the Group Paging feature. SIP phones not only originate a group page but also become a part of the paging group.

For information on the Group Paging feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Service Pack and Dot Release Guardian

Avaya Service Pack and Dot Release Guardian is a patent pending technology that protects and controls the authorized use of Communication Manager service packs and dot releases by inserting the support end date (SED) in the license file and comparing it with the publication date of the service pack or dot release. The application of service packs and dot release upgrades require Avaya support entitlements. With this technology, a service pack or a dot release can be used if the publication date of the service pack or the dot release is on or before the SED in the Communication Manager license file.

For more information on Service Pack and Dot Release Guardian, see *Implementing Avaya Aura® Communication Manager*, 03-603558.

Type 3 License Allocation Algorithm

Communication Manager implements Type 3 License Allocation Algorithm during registration and unregistration. Based on the content of the license file, Type 3 License Allocation Algorithm provides multiple Type 3 feature entries for the same product ID with different releases. An available license can be used for a registered endpoint if the release number of the license is identical to the release number of the registered endpoint or a later version of the registered endpoint.

Communication Manager uses Type 3 License Allocation Algorithm to:

- Check the available capacity of the license for the same release and product ID of the registering endpoint, and uses the license based on the available capacity
- Search for available licenses of incremental releases for the product ID if adequate capacity is unavailable

- Search for any release of an available license if licenses with specific releases for the product ID are unavailable
- Release the available license at the time of unregistration

Type 3 License Allocation Algorithm is used to register licenses of multiple releases with endpoints of multiple releases. Type 3 License Allocation Algorithm provides the benefit of optimum usage of licenses and easy upgrade of the licenses for endpoints.

Type 3 License Allocation Algorithm uses the lowest-priced license for registration and releases the highest-priced license at the time of unregistration.

Main and survivable server split registration prevention

The split registration prevention feature, which ensures that gateways and telephones in a network region register to the same server, is now available for preventing split registration between the main server and the survivable core server. Earlier, this feature was only available for preventing split registration between the main server and the survivable remote servers.

The split registration prevention feature can be administered through the **Force Phones and Gateways to Active Survivable Servers** field on the IP Options System Parameters screen.

You can now administer the mg recovery rule to immediate. The functioning of immediate rule depends on the type of server the gateways are registered to. If the following conditions are met, gateways can re-register to the main server once the network stability period expires.

- The survivable server is a survivable core server.
- There are gateways registered with the main server.

The default duration of the network stability period is three minutes. You can change the duration on the mg-recovery-rule screen. If all gateways are registered with the survivable core server, the network regions assigned to the survivable server are disabled. If the survivable server is a survivable remote server, the network regions are disabled even if there are some telephones and gateways registered with the main server.

For more information on split registration, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Patch management for Communication Manager

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

- Communication Manager dot release
- Security
- Kernel

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

Hardware

Supported servers

Communication Manager runs on the following servers:

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

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

Only the S8300D server, HP DL360 G7, and Dell R610 are currently being sold. If you have an S8800 or S8510 server, you might need to add the necessary memory and hardware to upgrade to Communication Manager Release 6.2.

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

New telephones

Communication Manager now provides native support for the following telephones:

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

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

- Fixed feature buttons, such as Hold, Conference, Transfer, Message waiting lamp, Drop and Redial
- Message button
- Customized button labels
- Forty Unicode, Eurofont, or Kanafont character display message support
- Speakerphone functionality, including Group Listen
- Support for the same set of Communication Manager call processing features that are supported by the 1416 digital deskphones

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

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

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

Upgrades

This release of Communication Manager includes several upgrade procedures. The supported upgrade paths are listed in Upgrade paths on page 22.

For upgrade procedures, see *Upgrading Avaya Aura® Communication Manager*, 03-603560.

Upgrade paths

The following table provides the supported upgrade paths from various releases of Communication Manager to Release 6.2.

Note:

You cannot upgrade some servers to Release 4.0.5 or Release 5.2.1 directly. You must upgrade to Release 4.0.5 or Release 5.2.1 on a supported server, respectively, before you complete the upgrade to Release 6.2.

Release	Requirement
Release 1.x.x (DEFINITY R)	Restore translations to a HP DL360 G7 or Dell R610 server on Release 6.2.
Release 2.x (DEFINITY SI)	Restore translations to an S8300D, HP DL360 G7, or Dell R610 server on Release 6.2.
Release 3.x.x (DEFINITY CSI)	Restore translations to an S8300D, HP DL360 G7, or Dell R610 server on Release 6.2.
Release 1.x.x (S8300A)	Upgrade the hardware to an intermediate server (S8300B or S8300C) on Release 4.0.5 and then upgrade the hardware to S8300D Server on Release 6.2.
Release 1.x.x (S8700)	Upgrade to Release 4.0.5 before you upgrade to Release 6.2 on HP DL360 G7 or Dell R610.
Release 2.x.x (S8300A)	Upgrade the hardware to an intermediate server (S8300B or S8300C) on Release 4.0.5 and then upgrade the hardware to S8300D Server on Release 6.2.
Release 2.x.x (S8500A, S8700, S8710 wDAL1)	Upgrade to Release 4.0.5 with memory upgrade before you upgrade to Release 6.2 on HP DL360 G7 or Dell R610. For S8710, upgrade to Release 5.2.1 before you upgrade to Release 6.2 on HP DL360 G7 or Dell R610, You do not require to upgrade the memory.
Release 2.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 3.x.x (S8500A, S8700, S8710/S8720 wDAL1)	Upgrade to Release 4.0.5 and then upgrade to a HP DL360 G7 or Dell R610 server on Release 6.2.
Release 3.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 4.x.x (S8500A, S8700, S8710/S8720 wDAL1)	Upgrade to Release 4.0.5 and then upgrade to a HP DL360 G7 or Dell R610 server on Release 6.2.

Release	Requirement
Release 4.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 5.0.x	Upgrade to Release 5.2.1 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 5.1.x	Upgrade to Release 5.2.1 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 5.2.1	Install a preupgrade service pack before you upgrade to Release 6.2.
Release 6.0.x	Upgrade software-only to Release 6.2.

Special applications

Special applications, also known as green features, meet special requirements of customers. Communication Manager now supports many of these special applications at no additional cost and on the same license. You can log in as a super-user and activate these applications. Although these applications are available for use, they are not extensively tested.

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

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

Chapter 3: What's new in Communication Manager Messaging

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

Communication Manager Messaging Embedded runs on the S8300D, S8510, S8800, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.

50-digit and variable length extensions

Communication Manager Messaging supports variable length mailbox extensions and extensions up to 50 digits long. The option to create the variable length extensions is available on the Switch Link screen. The variable length extension makes it easy to administer your messaging environment by allowing one-to-one mapping of real extension with mailbox numbers.

For more information, see *Avaya Aura® Communication Manager Messaging Documentation CD*, 18-603645, and *Implementing Avaya Aura® Communication Manager Messaging*, 18-603644.

Automatic Message Forwarding to SMTP

In Communication Manager Messaging, you can have messages forwarded to:

- Microsoft Exchange
- An external SMTP account such as Yahoo! or Gmail
- Another user

By default, to prevent unwanted automatic traffic, message forwarding is disabled.

You can enable this feature by activating the **Enable automatic msg fwding** field. You must also enable it on the subscriber mailboxes.

For procedures to enable Auto Msg Fwding to SMTP, see *Avaya Aura® Communication Manager Messaging Documentation CD*, 18-603645.

Patch management for Communication Manager Messaging

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

- Communication Manager Messaging dot release
- Security
- Kernel

You can download the latest patches from the Avaya Support Web site. For information on the latest patches, see *Avaya Aura®Communication Manager Release Notes*.

LDAP and SMTP networking

Communication Manager Messaging supports LDAP and SMTP networking. As a result, Communication Manager Messaging fully supports 50-digit and variable-length mailboxes.

To interact with Avaya Messaging products, such as Aura Messaging or Modular Messaging, Communication Manager Messaging does not depend on Message Networking. However, if a Communication Manager Messaging instance supporting mailboxes of more than 10 digits interacts with an earlier release of Communication Manager Messaging or Intuity Audix, it must still use Message Networking.

Both, LDAP and SMTP, are open, standard protocols. LDAP is used to transmit directory updates, whereas SMTP is used to transmit messages.

For more information on LDAP and SMTP networking, see *Avaya Aura® Communication Manager Messaging Documentation CD*, 18-603645.

SIP INFO method

Communication Manager Messaging supports DTMF transport, both inbound and outbound, by using the SIP INFO method.

The SIP INFO method transmits mid-session signaling information, such as DTMF tones along the SIP signaling path in a reliable way. The SIP INFO method uses the underlying SIP reliability. Sequenced delivery of information ensures that data packets are delivered with minimal data loss. The transmission of tones is completed during a call and is independent of the RTP.

The SIP INFO method is not used to change the state of a SIP call.

For more information on SIP INFO method, see *Implementing Avaya Aura® Communication Manager Messaging*, 18-603644.

Migration paths

Communication Manager Messaging supports the following migration paths:

- Communication Manager Messaging 4.0.5 to Communication Manager Messaging 6.2
- Communication Manager Messaging 5.2.1 to Communication Manager Messaging 6.2
- *Intuity Audix* 5.1 to Communication Manager Messaging 6.2
- *Intuity Audix* 4.4 to Communication Manager Messaging 6.2
- *Intuity Audix* LX 1.1 to Communication Manager Messaging 6.2
- *Intuity Audix* LX 2.0 to Communication Manager Messaging 6.2

For more information on migration paths, see the following documents:

- Migration from *Intuity Audix* LX R2.0 to *Avaya Aura®Communication Manager Messaging* R6.2, 18-603650
- Migration from *Intuity Audix* LX R1.1 to *Avaya Aura®Communication Manager Messaging* R6.2, 18-603649
- Migration from *Intuity Audix* R5.1 to *Avaya Aura®Communication Manager Messaging* R6.2, 18-603648
- Migration from *Intuity Audix* R4.4 to *Avaya Aura®Communication Manager Messaging* R6.2, 18-603646

Communication Manager Messaging 6.0 and 6.0.1 support upgrades to Communication Manager Messaging release 6.2. For upgrading procedures, see *Upgrading Avaya Aura*® *Communication Manager*, 03-603560.

Chapter 4: What's new in Session Manager

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

Session Manager call preservation for contact centers

Call preservation enables a contact center call to remain active when there is a failure of core Session Manager or failure of a connection to Session Manager. Call preservation ensures that ongoing SIP sessions or call transactions, such as conference, transfer, or hold, continue without interruption or outage.

Session Manager, Communication Manager, G860, AudioCodes Mediant 3000, and Avaya Aura® Experience Portal collaborate to preserve calls in the queue. The call preservation feature does not apply to SIP telephones. These telephones use a different failover mechanism.

For more information, on call preservation administration, see *Call Preservation Administration Case Study*.

Related topics:

Call preservation for Communication Manager on page 15

Session Manager Network Connect Service

Session Manager Network Connect Service (NCS) provides routing services to VoIP endpoints based on Communication Server 1000 (CS1000), similar to the services provided by Nortel Network Routing Service. Session Manager NCS provides network redirection services for UNIStim phones for several CS1000 network features, such as geographic redundancy, virtual office, branch office, or Survivable Remote Gateway.

For more information, see *Administering Avaya Aura® Session Manager*, 03-603324.

Conference Factory URI

Conference Factory URI feature enables seamless integration of Session Manager with conference capabilities of conference products, such as Avaya Aura® Conferencing, Meeting Exchange, Communication Manager, and SIP endpoints, including Avaya Desktop Video Device. This feature provides enhanced experience for participants in conferences and enables richer collaboration when using voice, video, and text conference systems.

For more information, see *Administering Avaya Aura® Session Manager*, 03-603324.

Network-wide bandwidth management

Network-wide bandwidth management provides enhanced support for centralized video and voice call admission control with bandwidth sharing and Avaya Aura® Conferencing Solution interoperability for media server CAC and mid-call video downspeeding.

For more information, see *Administering Avaya Aura® Session Manager*, 03-603324.

Avaya Aura® solution scalability enhancements

The number of Session Managers available for scalability has increased to 10. This release supports up to 100,000 SIP endpoints to register with the Session Manager core.

Support for Cisco endpoints

Session Manager now supports the unsolicited Notify standard supported by Cisco endpoints. Session Manager detects the Cisco endpoints and automatically sends the unsolicited Notify messages.

Support for Solution for Midsize Enterprise and RPM-level patching

During the installation of Avaya Aura® Solution for Midsize Enterprise (ME), the system hides most of the Session Manager installation steps so that you can avoid redundant steps, such as confirming password, and complete the ME installation faster. The ASG password scheme is available for Session Manager, survivable remote servers, survivable core servers, and ME configurations. You need to use the System Platform ASG process for ASG access to Session Manager on the survivable remote server or ME.

The RPM-based patching mechanism is available for Session Manager on the survivable core server, the survivable remote server, and ME. To patch Session Manager on a survivable core server or an ME, System Platform provides tools by which RPMs can be easily delivered to Session Manager. Also, System Platform provides tools to run a kernel patch, especially a security patch, on Session Manager on a survivable remote server or an ME.

Note that the System Platform-based watchdog for Session Manager on the survivable remote server and ME is identical to the watchdog that runs for Session Manager on the survivable core server.

Index

T

U

V

W