Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailid=000012112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE: HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACQUIRES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTND 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 as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) 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

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of 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.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment.
Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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

Virtualization
The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each instance of a product must be separately licensed and ordered. For example, if the end user or customer or Avaya Channel Partner would like to install two instances of the same type of products, then two products of that type must be ordered.

Third Party Components
"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/ Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEGLA LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider
THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEGLA LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws
You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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 Help Desk at +1-800-043-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities
Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

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

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

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(s) 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.

AVAYA

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.

Java is a registered trademark of Oracle and/or its affiliates.
## Contents

### Chapter 1: New in this release

- Product branding.................................................................................................................. 7
- Other changes......................................................................................................................... 7

### Chapter 2: New features

- Account and password security............................................................................................ 9
- Accounting record changes..................................................................................................... 10
- AS 5300 UC Client configurable number of logons.............................................................. 11
- AS 5300 UC Client new DSCP driver installation for Windows XP........................................ 12
- AS 5300 UC Client Sign on updates...................................................................................... 12
  - AS 5300 UC Client Sign on updates—CAC........................................................................ 13
- AS 5300 UC Client Standard Skin Answer Video................................................................. 13
- AS 5300 UC Client Standard Skin MLPP support................................................................. 13
- ASAC and TDM enhancements.............................................................................................. 13
- Avaya Media Server changes............................................................................................... 14
  - Packaged Application configuration.................................................................................. 14
- Call Forward Variants VSC activation................................................................................... 14
- Click To Call Enable MKI...................................................................................................... 15
- Client Collaboration enhancements...................................................................................... 15
- Codec support....................................................................................................................... 15
- Custom Network Domains..................................................................................................... 16
- Database changes.................................................................................................................. 17
- Destination Code Controls.................................................................................................... 17
- Element Manager enhancements.......................................................................................... 17
- Emergency calls without authentication............................................................................... 18
- Emergency calls when E911 Manager is deployed............................................................. 18
- Enable Dual Stack Support Preference option.................................................................. 18
- General Dynamics vIPer phone support............................................................................. 19
- General user interface changes............................................................................................ 19
- Hardware support.................................................................................................................. 20
- IP Phone tab in Personal Agent............................................................................................ 20
- IPv6 enhancements............................................................................................................... 20
  - IPv6 support for UC Client............................................................................................... 21
- Network settings changes..................................................................................................... 21
- Network Time Protocol Symmetric Keys............................................................................ 21
- Paired MFSS for failover....................................................................................................... 22
- Password expiry during active call...................................................................................... 22
- Precedence domain changes............................................................................................... 22
- Reorder tone.......................................................................................................................... 22
- Secure Shell and Common Access Card integration........................................................... 23
- SIP Profiles for UC Clients................................................................................................. 23
Chapter 1: New in this release

This document details what's new in Avaya Aura® Application Server 5300 Release Delta, NN42040-201 for Avaya Aura® Application Server 5300 Release 3.0.

For information on the new features, OAM, and other changes, see

- New features on page 9
- OAM Impacts on page 27
- Other changes on page 31

Product branding

The following product and application name changes apply in Application Server 5300 Release 3.0:

<table>
<thead>
<tr>
<th>Product or application name in Application Server 5300 Release 3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS 5300 Element Manager. Formerly System Manager.</td>
</tr>
<tr>
<td>AS 5300 Element Manager Console. Formerly System Management Console.</td>
</tr>
</tbody>
</table>

Other changes

This document is new for Application Server 5300 Release 3.0.

Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2017</td>
<td>Updated the legal page for Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>July 2015</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0 Service Pack 11.</td>
</tr>
<tr>
<td>December 2014</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0 Service Pack 10.</td>
</tr>
</tbody>
</table>

Comments on this document? infodev@avaya.com
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2014</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0 Service Pack 9.</td>
</tr>
<tr>
<td>July 2013</td>
<td>Standard 01.06. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>March 2013</td>
<td>Standard 01.05. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>February 2013</td>
<td>Standard 01.04. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>December 2012</td>
<td>Standard 01.03. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td></td>
<td>Updated the following section: <a href="#">OCS/MOC/Office Client support</a> on page 32.</td>
</tr>
<tr>
<td>September 2012</td>
<td>Standard 01.02. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td></td>
<td>Added the following section: <a href="#">OCS/MOC/Office Client support</a> on page 32.</td>
</tr>
<tr>
<td>June 2012</td>
<td>Standard 01.01. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
</tbody>
</table>
Chapter 2: New features

The following sections describe the new features for Avaya Aura® Application Server 5300 Release 3.0.

Navigation

• Account and password security on page 10
• Accounting record changes on page 11
• AS 5300 UC Client configurable number of logons on page 12
• AS 5300 UC Client new DSCP driver installation for Windows XP on page 12
• AS 5300 UC Client Sign on updates on page 12
• AS 5300 UC Client Standard Skin Answer Video on page 13
• AS 5300 UC Client Standard Skin MLPP support on page 13
• ASAC and TDM enhancements on page 13
• Avaya Media Server changes on page 14
• Call Forward Variants VSC activation on page 14
• Click To Call Enable MKI on page 15
• Client Collaboration enhancements on page 15
• Codec support on page 15
• Custom Network Domains on page 16
• Database changes on page 17
• Destination Code Controls on page 17
• Element Manager enhancements on page 17
• Emergency calls without authentication on page 18
• Emergency calls when E911 Manager is deployed on page 18
• Enable Dual Stack Support Preference option on page 18
• General Dynamics vIPer phone support on page 18
• General user interface changes on page 19
• Hardware support on page 20
• IP Phone tab in Personal Agent on page 20
• IPv6 enhancements on page 20
Account and password security

Avaya Aura® Application Server 5300 Release 3.0 provides options to require greater password complexity, and enhances password aging options and login rules.

Subscriber password changes

Subscriber password policies are enhanced, and several new policies are added. The following policies are available:

- Minimum Length of the Password
- Minimum Number of Digits in Password
- Minimum Number of Lowercase Characters
- Minimum Number of Uppercase Characters
- Minimum Number of Special Characters
- Maximum Consecutive Characters in Password
- Minimum Number of Characters Different from Previous Password
- Password History to restrict reuse of passwords
- User ID Permitted Checking in Password
- Check for Dictionary Words in Password
Subscriber passwords are also protected by domain password policies, including initial password reset, subscriber lockout on failed login, per-user maximum password life, and password expiry notification. A Subscriber Audit feature checks for and disables inactive accounts.

**Provisioning Client administrator and AS 5300 Session Manager Console administrator changes**

Admin password policies are enhanced, and several new policies are added. The following policies are available:

- Minimum Password Length
- Minimum Lowercase Characters
- Minimum Uppercase Characters
- Minimum Digits
- Minimum Special Characters
- Maximum Consecutive Characters
- Minimum Characters Different From Previous Password
- Password History
- User ID or Reversed User ID Permitted in Password
- Check for Dictionary Words in Password
- Maximum Password Life (per-user)
- Minimum Password Life
- Expiry Notification

A tab called Password Policies is added to the on the Add tab of the Admin portlet. On this tab, you can override system Password Policies on a user-by-user basis. Currently, you can override the Maximum Password Life policy.

Admin passwords are also protected by Login Rules; a new Login Rule is added to disable accounts which are inactive for a configurable period of time. An Admin Audit feature checks for and disables inactive accounts.

**References**

For more information see the following documents:

- *Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040–112*
- *Avaya Aura® Application Server 5300 Personal Agent User Guide, NN42040–105*
- *Avaya Aura® Application Server 5300 Security, NN42040–601*

---

**Accounting record changes**

The IPDR records and fields for Connect Egress and Connect Ingress accounting events have been updated to include DCC related changes.
References
For more information, see the following document:
- Avaya Aura® Application Server 5300 Accounting Records Reference, NN42040-501

AS 5300 UC Client configurable number of logons
The AS 5300 UC Client system security administrator configures the number of consecutive logon attempts possible. The number of consecutive failed logons allowed is between two and five and the default value is three.

References
For more information, see the following document:
- Avaya Aura® Application Server 5300 UC Client User Guide, NN42040-107

AS 5300 UC Client new DSCP driver installation for Windows XP
You must install the new DSCP driver while installing the AS 5300 UC Client for Windows XP operating system.

References
For more information, see the following document:

AS 5300 UC Client Sign on updates
Automatically sign me in at Startup, Remember my password and Sign me in automatically options apply only for UC Clients that are not configured for high security.

References
For more information, see the following document:
AS 5300 UC Client Sign on updates—CAC

AS 5300 UC Client configured for high security might require you to insert the Common Access Card (CAC) and provide your card's personal identification number (PIN).

References
For more information, see the following documents:


AS 5300 UC Client Standard Skin Answer Video

The Answer Video button is now added in the standard skin (theme) AS 5300 UC Client. Previously, this option was supported only in AS 5300 UC Client in the classic skin (theme).

References
For more information, see the following document:

- Avaya Aura® Application Server 5300 UC Client User Guide (NN42040–107)

AS 5300 UC Client Standard Skin MLPP support

This feature provides support for the Multilevel Precedence and Preemption (MLPP) feature in the standard skin (theme) of the Avaya Aura® Application Server 5300 UC Client. In previous releases, the AS 5300 UC Client supported MLPP only in the classic skin.

References
For more information, see the following documents:

- Avaya Aura® Application Server 5300 Overview (NN42040–100)
- Avaya Aura® Application Server 5300 UC Client User Guide (NN42040–107)

ASAC and TDM enhancements

The AS 5300 Session Manager reports the real-time values of Assured Service Admission Control (ASAC) allocated resource (ASAC counts) to an ASAC Operational Measurements (OM) Group.

The system now monitors ARTS configuration, and raises alarms and logs if the system detects invalid ARTS configuration for any ASAC node.
The system generates accounting data (IPDR) records containing the trunk ID and channel ID of calls that connect to a Time Division Multiplex (TDM) network.

**References**
For more information, see the following documents:

- *Avaya Aura® Application Server 5300 Accounting Records Reference, NN42040–501*
- *Avaya Aura® Application Server 5300 Alarms and Logs Reference, NN42040–701*
- *Avaya Aura® Application Server 5300 Operational Measurements Reference, NN42040–702*

---

**Avaya Media Server changes**

Changes to Avaya Media Server (MS) include:

- Remove support for Jasper.
- Avaya MS backup and restore uses Linux procedures.
- In the AS 5300 Element Manager Console, added IPv6 media address support for Avaya MS.

---

**Packaged Application configuration**

Configure packaged applications to ensure that users can access and use packaged applications according to business requirements. The following features are available:

- AdHoc Conferencing
- Announcements
- Instant Message Chat
- Meet Me Conferencing
- Music on Hold
- Recorder configuration
- Unified Communications

**References**
For more information, see the following document:

- *Avaya Aura® Application Server 5300 Configuration, NN42040-500.*

---

**Call Forward Variants VSC activation**

This feature enables subscribers to activate Call Forward (CFWD) Variants using a VSC.
References
For more information, see the following documents:
• Avaya Aura® Application Server 5300 Overview, NN42040–100.

Click To Call Enable MKI
A new check box Enable MKI is added to Click To Call.

References
For more information, see the following document:

Client Collaboration enhancements
Application Server 5300 does not support provisioning of Client Collaboration feature for Federal Service packages.

References
For more information, see the following document:
• Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040–112.

Codec support
The system supports the following codecs, which you can configure for each SIP Profile through AS 5300 Session Manager:
• audio
  - Clearmode
  - Codec5
  - G722
  - G722.1
  - G723
  - G728
New features

- G729
- PCMA
- PCMU
- telephone-event
- v150fw
- x-ccd

• video
  - H.261
  - H.263
  - H.263–1998
  - H.263–2000
  - H.264
  - H.264–SVC
  - mp4v-es
  - x-nnvc

Support for the DivX codec has been removed in this release.

References
For more information, see the following documents:

• Avaya Aura® Application Server 5300 Overview, NN42040–100
• Avaya Aura® Application Server 5300 UC Client User Guide, NN42040–107
• Avaya Aura® Application Server 5300 Configuration, NN42040–500

Custom Network Domains
Avaya Aura® Application Server 5300 supports user-defined network domains apart from the system-defined DSN, UC, or CUC domains. You should create a custom network domain only if you are unable to use any of the system-defined network domains. You can define a maximum of five network domains.

References
For more information, see the following document:

• Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040-112.
Database changes

The following changes were made regarding the database:

- All the specific instances of the database application "Oracle" were changed to the generic term "DB".
- Alternate procedures were added to start and stop the database.

Reference

For more information, see the following documents:

- Avaya Aura® Application Server 5300 Administration - NN42040-600.
- Avaya Aura® Application Server 5300 Troubleshooting and Fault Management - NN42040-700.

Destination Code Controls

Destination Code Controls (DCC) allows you to control the calls to specific locations that have been temporarily designated as ‘difficult to reach’. DCC controls the traffic to such regions and allows only precedence traffic to be passed to the destination. Using DCC, you can configure the percentage of calls that should be blocked to such destinations.

References

For more information, see the following documents:

- Avaya Aura® Application Server 5300 Overview, NN42040–100
- Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040–112
- Avaya Aura® Application Server 5300 Terminology, NN42040-103

Element Manager enhancements

The AS 5300 Element Manager configuration parameters have been updated to support TLSAuth and EMAadminAudit.

References

For more information, see the following document:

- Avaya Aura® Application Server 5300 Configuration, NN42040-500
Emergency calls without authentication

This feature enables subscribers to place emergency calls without authentication on 11xx series phones. The UC Client does not support this option.

**References**

For more information, see the following documents:

- Avaya Aura® Application Server 5300 Features Reference, NN42040–118.
- Avaya Aura® Application Server 5300 Using the Avaya 1120E IP Deskphone with SIP Software 4.2, 18-604104.
- Avaya Aura® Application Server 5300 Using the Avaya 1140E IP Deskphone with SIP Software 4.2, 18-604105

Emergency calls when E911 Manager is deployed

Integration of E911 Manager into deployment allows dynamic determination of the real physical location information of an emergency caller. Even if the location selected by user at the login time was incorrect, the call will be routed to the appropriate nearest PSAP, based on the location determined by E911 Manager.

This feature is not supported for subscribers without authentication on 11xx series phones.

For more information, see the following documents:

- Avaya Aura® Application Server 5300 Overview, NN42040-100
- Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040-112
- Avaya Aura® Application Server 5300 Features Reference, NN42040–118
- Avaya Aura® Application Server 5300 Planning and Engineering, NN42040-200
- Avaya Aura® Application Server 5300 Configuration, NN42040-500
- Avaya Aura® Application Server 5300 Alarms and Logs Reference, NN42040-701
- Avaya Aura® Application Server 5300 Operational Measurements Reference, NN42040-702

Enable Dual Stack Support Preference option

A new option is available to enable the dual stack support preference option.

**References**

For more information, see the following document:

General Dynamics vIPer phone support

Application Server 5300 Release 3.0 supports vIPer phones from the vendor General Dynamics. The Sectéra® vIPer phone is a SIP desktop phone that meets the UCR 2008 Change 1 requirements for a secure IP Phone.

References

For more information, see the following documents:

- Avaya Aura® Application Server 5300 Overview, NN42040–100
- Avaya Aura® Application Server 5300 Planning and Engineering, NN42040–200

General user interface changes

All user interfaces for Application Server 5300 and Avaya Media Server been updated for this release, including parameter changes.

The following user interfaces have been updated:

- All installation, upgrade, and downgrade programs
- Avaya Aura® Application Server 5300 Personal Agent
- Avaya Aura® Application Server 5300 UC Client
- Provisioning Client
- AS 5300 Element Manager Console
- Avaya Media Server Element Manager

References

For more information, see the following documents:

- Avaya Aura® Application Server 5300 Personal Agent User Guide, NN42040–105
- Avaya Aura® Application Server 5300 UC Client User Guide, NN42040–107
- Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040–112
- Avaya Aura® Application Server 5300 Configuration, NN42040–500
- Avaya Aura® Application Server 5300 Administration, NN42040–600
- Avaya Aura® Application Server 5300 Security, NN42040–601
- Avaya Aura® Application Server 5300 Meet Me Conferencing Quick Reference, NN44474–102
- Avaya Aura® Application Server 5300 Unified Communications Quick Reference, NN44474–103
- the Avaya customer-facing Method of Procedure (MOP) documents
Hardware support

Application Server 5300 Release 3.0 adds support for the HP ProLiant DL360 G7 server.

Existing systems continue to use the IBM x3550 servers. If additional servers are required, existing systems can add either IBM x3550 or HP ProLiant DL360 G7 servers.

The new server is supported as an AS 5300 server or an Avaya Media Server.

New systems use HP ProLiant DL360 G7 servers.

References

For more information, see the following documents:

- Avaya Aura® Application Server 5300 Overview, NN42040–100
- Avaya Aura® Application Server 5300 Planning and Engineering, NN42040–200
- Avaya Media Server Planning and Engineering, NN44471-200

IP Phone tab in Personal Agent

IP Phone tab under User Preferences in Personal Agent was designed to be used with UNISTIM phones only. Since UNISTIM phones are no longer supported, the IP Phone tab is removed from the Personal Agent.

IPv6 enhancements

IPv6 is enhanced in several aspects:

- AS 5300 Session Manager configuration is moved to AS 5300 Element Manager Console, preserving the AS 5300 Session Manager IPv6 address on undeploy.
- License key checks moved from AS 5300 Session Manager to AS 5300 Element Manager. License key checks are now enforced when a user enters an IPv6 address in the AS 5300 Element Manager. The IPv6 in platform is not license keyed.
- AS 5300 Session Manager can communicate with AudioCodes Gateway (M3000, M800), Edge Border Controllers (EBC), and Foreign Domains over IPv6 and IPv4.
- IPv6 address support (start/stop/monitor) moved to Network Interface (NIF).
- Enhancements to Platform IPv6 configuration scripts.
- Support added for backup and restore of IPv6 platform network data.
IPv6 support for UC Client

Application Server 5300 UC Client supports IPv6 for signaling and media options.

References

For more information, see the following document:

• Avaya Aura® Application Server 5300 Planning and Engineering, NN42040-200.

Network settings changes

The network settings dialog box have been updated to include media preference option through IPv6. The media preference option applies only if the Dual Stack feature is available.

References

For more information, see Avaya Aura® Application Server 5300 UC Client User Guide, NN42040-107.

Network Time Protocol Symmetric Keys

Application Server 5300 Release 3.0 offers enhanced authentication protection for Network Time Protocol (NTP) through the use of symmetric keys. Symmetric keys are used to protect NTP communication between external NTP servers and the AS 5300 Element Manager.

For more information, see the following documents:

References

• Avaya Aura® Application Server 5300 Overview, NN42040–100.
• Avaya Aura® Application Server 5300 Planning and Engineering, NN42040–201.
• Avaya Aura® Application Server 5300 Security, NN42040–601
Paired MFSS for failover

You can configure an MFSS as a pair for the local SS, for failover purposes. This is possible only if there is zero or one local SS profile on your system and will not be allowed for a second SS profile added to the system.

You can have only one MFSS paired with the local SS. If you try to select a second MFSS as paired, the system displays a message indicating that an MFSS pair already exists in the system and asks for an override confirmation to replace the existing paired MFSS.

References
For more information, see the following document:

- Avaya Aura® Application Server 5300 Configuration, NN42040-500.

Password expiry during active call

The Personal Agent and AS 5300 UC Client use a single password to access the application. If this password expires or changes during an active call, the call does not get disconnected during re-registration.

References
For more information, see the following documents:

- Avaya Aura® Application Server 5300 Overview, NN42040–100.

Precedence domain changes

The precedence domains have been changed in the messages pertaining to MLPP. MLPP supports the new network domains 'UC' and 'CUC', in addition to 'DSN'.

References
For more information, see the following document:

- Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040-112.

Reorder tone

The SIP access authentication process is updated to include a reorder tone. The caller receives a reorder tone, if the proxy authentication fails three times consecutively.
Secure Shell and Common Access Card integration

Administrators use Secure Shell (SSH) for remote access and administration of the Linux servers. The Application Server 5300 comes with OpenSSH installed. OpenSSH is an open-source application, which does not support two-factor authentication.

To provide two-factor authentication and Common Access Card (CAC) integration, Application Server 5300 also supports Attachmate Reflection for Secure IT as an optional configuration. Attachmate Reflection is not included with Application Server 5300. The purchase, installation and maintenance of Attachmate software are the customer’s responsibility. To install Attachmate Reflection for Secure IT, remove OpenSSH during system installation and commissioning.

References
For more information, see the following documents:

- 106.1.5 AS 5300 DoD Attachmate Administration.

SIP Profiles for UC Clients

Two new SIP Endpoint Protocol Profiles are added to support UC Client:

- avayaucc8—This profile is used for UC Client version 8.x
- avayaucc—This profile is used for any version of UC Client for which there is no SIP Profile specific to the UC Client version.

References
For more information about SIP Profiles, see the following documents:

- Avaya Aura® Application Server 5300 Overview, NN42040–100.
- Avaya Aura® Application Server 5300 Features Reference, NN42040–118.
- Avaya Aura® Application Server 5300 Configuration, NN42040–500.

TR87 Client Control

TR87 Client Control allows a soft client to monitor and control the actions of a hard client.
New features

References
For more information, see the following document:

• Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040–112.

Treatments
Treatments or announcements related to the following features have been added:

• Destination Code Controls (DCC)

References
For more information, see the following document:

• Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040–112

Trusted certificates
Application Server 5300 UC Client configured for high security allows access only to sites with trusted certificates.

References
For more information, see the following document:


User Agent field changes
The User Agent fields in the accounting records have been updated to include 'Avaya UCC' instead of 'Avaya PCC'.

References
For more information, see the following document:

• Avaya Aura® Application Server 5300 Accounting Records Reference, NN42040-501
V.150.1 support

The system supports V.150.1 for secure calls between General Dynamics vIPer Phone and Audiocodes Gateway or Integrated Analog Devices (IAD).

References

For more information, see the following document:

• Avaya Aura® Application Server 5300 Planning and Engineering, NN42040-200.

Video bandwidth changes

The Active call window has been updated to include the option of changing the video bandwidth during an active video call. This can be done using both standard and classic interface.

References

For more information, see the following document:

• Avaya Aura® Application Server 5300 UC Client User Guide, NN42040-107

Video codecs for System Profile

The video codecs H.261 and H.263++ have been added to the System Profile Video portlet in Provisioning Client.

References

For more information, see the following document:

• Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040–112.

XMPP Gateway Configuration process is updated

Configuration of XMPP data is moved from Personal Agent to Provisioning Client. In Personal Agent, the user has the ability to see the XMPP name provisioned by the system administrator. The XMPP configuration is structured in System Profiles and User Profiles to separate the XMPP domain and the XMPP name configuration for the user. There is a set of XMPP FQDNs that is associated with Session Manager. Also, migrating multiple users from one XMPP domain to another becomes easy.
References
For more information about XMPP Gateway Configuration, see the following documents:

- Avaya Aura® Application Server 5300 Overview, NN42040–100
- Avaya Aura® Application Server 5300 Personal Agent User Guide, NN42040–105
- Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040–112
- Avaya Aura® Application Server 5300 Features Reference, NN42040–118
Chapter 3: OAM Impacts

The following section describes the Operation, Administration, and Maintenance (OAM) impacts for Application Server 5300.

Navigation

• Alarms and logs on page 27
• Operational measurements on page 30

Application Server 5300 Alarms and logs

The following new Application Server 5300 alarms are added.

Table 1: New alarms

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAC 808</td>
<td>Raised on SS and indicates that ASAC rejects the call due to missing or incorrect CCA-ID.</td>
</tr>
<tr>
<td>ASAC 809</td>
<td>Raised on the terminating subscriber’s home LSC and indicates that the call was rejected by ASAC on SS due to missing or incorrect CCA-ID.</td>
</tr>
<tr>
<td>DBMN 102</td>
<td>Raised when database access is not available for the EM database monitor.</td>
</tr>
<tr>
<td>DBMN 729</td>
<td>Raised when the database replication software that keeps the primary and secondary databases in sync detects that databases are not in a synchronized state, indicating 20 errors in incoming batches.</td>
</tr>
<tr>
<td>DBMN 730</td>
<td>Raised when the database replication software that keeps the primary and secondary databases in sync detects that databases are not in a synchronized state, indicating 20 errors in outgoing batches.</td>
</tr>
<tr>
<td>DBMN 201</td>
<td>Raised when the database server process is not available.</td>
</tr>
<tr>
<td>DBMN 202</td>
<td>Raised when the database replication process is not available.</td>
</tr>
<tr>
<td>DCC 800</td>
<td>Raised when there is at least one DCC entry enabled in Provisioning Manager.</td>
</tr>
<tr>
<td>EMRG806</td>
<td>Raised when the connection with E911 Manager is not stable.</td>
</tr>
<tr>
<td>ICRT 808</td>
<td>Raised when a certificate has been added to the Truststore.</td>
</tr>
</tbody>
</table>

Table continues…
The following Application Server 5300 alarms are modified.

Table 2: Changed alarms

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBCM 203</td>
<td>Raised when there is no free space for DB Instance.</td>
</tr>
<tr>
<td>DOS 400</td>
<td>Raised when source IPs locked out due to distributed DoS attack.</td>
</tr>
<tr>
<td>LKEY 765</td>
<td>Raised when License key has been expired.</td>
</tr>
<tr>
<td>LKEY 466</td>
<td>Raised when pending license key has been expired.</td>
</tr>
<tr>
<td>NCAS 103</td>
<td>Raised when NCAS link IP address modified.</td>
</tr>
<tr>
<td>NECM 103</td>
<td>Raised when rogue network element instance has connected.</td>
</tr>
<tr>
<td>OVLD 404</td>
<td>Raised when the memory is exhausted.</td>
</tr>
<tr>
<td>RECS 209</td>
<td>Raised when it is unable to open file.</td>
</tr>
<tr>
<td>RECS 227</td>
<td>Raised when it is unable to rename file.</td>
</tr>
<tr>
<td>RECS 213</td>
<td>Raised when it is unable to write to file.</td>
</tr>
<tr>
<td>SRVR 201</td>
<td>Raised when RES Network interface is unavailable.</td>
</tr>
<tr>
<td>MVAL 102</td>
<td>Raised when Endpoint Protocol Profiles need better refinement.</td>
</tr>
<tr>
<td>QOS 801</td>
<td>Raised when the value of the DSCP parameter has been changed.</td>
</tr>
</tbody>
</table>

The following new Application Server 5300 logs are added.

Table 3: New logs

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAC 806</td>
<td>Indicates that the SS received an INVITE from one of the LSCs it serves, and the INVITE contains an unrecognized network domain in the resource-priority header.</td>
</tr>
<tr>
<td>Group</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ASAC 807</td>
<td>Indicates that the SS received an INVITE from one of the LSCs it serves, and the INVITE contains a known network domain but with an invalid value for the r-priority field.</td>
</tr>
<tr>
<td>DCC 802</td>
<td>Indicates that the DCC entry is activated.</td>
</tr>
<tr>
<td>DCC 803</td>
<td>Indicates that the parameters of the DCC entry are changed.</td>
</tr>
<tr>
<td>DCC 804</td>
<td>Generated when a DCC entry is renamed and parameters are potentially changed.</td>
</tr>
<tr>
<td>DCC 805</td>
<td>Generated when a DCC entry is disabled.</td>
</tr>
<tr>
<td>DCC 806</td>
<td>Generated when a DCC entry is renamed and disabled.</td>
</tr>
<tr>
<td>DCC 807</td>
<td>Generated when a DCC entry is deleted.</td>
</tr>
<tr>
<td>EMRG707</td>
<td>Generated when an emergency caller has associated the ELIN number received previously from E911 Manager node, but no provisioned ANI is found per this.</td>
</tr>
<tr>
<td>JPL 201</td>
<td>Log4j warn logs are proxied from hibernate access layer to this log.</td>
</tr>
<tr>
<td>JPL 202</td>
<td>Log4j info logs are proxied from hibernate access layer to this log.</td>
</tr>
<tr>
<td>OMIS 650</td>
<td>Generated when EM Admin Audit has started.</td>
</tr>
<tr>
<td>OMIS 651</td>
<td>Generated when one or more admins that have been inactive for too long are detected by the EM Admin Audit. Note that when a user is reported as inactive in the current audit, it will not be reported in next audit.</td>
</tr>
<tr>
<td>OMIS 652</td>
<td>Indicates that the current EM Admin Audit is complete.</td>
</tr>
<tr>
<td>OMIS 653</td>
<td>Indicates the next time the EM Admin Audit will run</td>
</tr>
<tr>
<td>OMIS 654</td>
<td>Indicates that the EM Admin Audit has been activated by the configuration parameter.</td>
</tr>
<tr>
<td>OMIS 655</td>
<td>Indicates that the EM Admin Audit has been deactivated by the configuration parameter.</td>
</tr>
<tr>
<td>SPIS 650</td>
<td>Indicates that Subscriber Audit is started.</td>
</tr>
<tr>
<td>SPIS 651</td>
<td>Generated when there are one or some users whose expiring/expired passwords are detected by Password Expiry Audit. Please note, once an user with expired password is reported in current audit, it will not be reported in next audit.</td>
</tr>
<tr>
<td>SPIS 652</td>
<td>Indicates that current Subscriber Audit running finished.</td>
</tr>
<tr>
<td>SPIS 653</td>
<td>Indicates when Subscriber Audit runs next time.</td>
</tr>
<tr>
<td>SPIS 654</td>
<td>Indicates that Subscriber Audit is activated by the configuration parameter.</td>
</tr>
<tr>
<td>SPIS 655</td>
<td>Indicates that Password Expiry Audit is deactivated by the configuration parameter.</td>
</tr>
<tr>
<td>SPIS 656</td>
<td>Generated when Subscriber Account Audit finds there is one or some accounts which has no activity in Account Inactivity Intervel. This user's account is then disabled by the system. Please note, once an user's account is disabled, it will not be reported in next audit.</td>
</tr>
<tr>
<td>SPIS 660</td>
<td>Indicates that the Prov Admin Audit has started.</td>
</tr>
<tr>
<td>SPIS 661</td>
<td>Generated when Subscriber Account Audit finds there is one or some accounts which has no activity in Account Inactivity Intervel. This user's account is then disabled by the system. Please note, once an user's account is disabled, it will not be reported in next audit.</td>
</tr>
</tbody>
</table>

*Table continues...*
The following Application Server 5300 logs are modified.

**Table 4: Changed logs**

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L4J 201</td>
<td>Log4j warn logs are proxied to this log.</td>
</tr>
<tr>
<td>L4J 202</td>
<td>Log4j warn logs are proxied to this log.</td>
</tr>
</tbody>
</table>

**References**

For more information, see the following document:

- **Avaya Aura® Application Server 5300 Alarms and Logs Reference, NN42040–701.**

---

**Operational measurements**

Application Server 5300 Release 3.0 contains the following operational measurement (OM) changes:

- Added the ASAC OM group details
- Added the TDM OM group details
- Added the DCC OM group details
- Added the E911MNGR OM group details
- Updated the AdvancedAuth OM group details

**References**

For more information, see the following document:

- **Avaya Aura® Application Server 5300 Operational Measurements Reference, NN42040–702**
Chapter 4: Other changes

This section describes other changes to Application Server 5300.

Navigation
- Database changes on page 17
- Avaya Media Server service integration on page 31
- OCS/MOC/Office Client support on page 32
- Supported features on page 32
- Tomcat and Jetspeed replaces JBoss on page 33

Database changes

The following changes were made regarding the database:

- All the specific instances of the database application "Oracle" were changed to the generic term "DB".
- Alternate procedures were added to start and stop the database.

Reference

For more information, see the following documents:

- Avaya Aura® Application Server 5300 Administration - NN42040-600.
- Avaya Aura® Application Server 5300 Troubleshooting and Fault Management - NN42040-700.

Avaya Media Server service integration

In Avaya Aura® Application Server 5300 Release 3.0, functionality formerly available through the Avaya Media Server (MS) Element Manager is available through the Media Server network element in AS 5300 Element Manager, including

- Avaya MS Application Restrictions
- Avaya MS audio CODEC management
• Avaya MS configuration parameters (config parms)
• Avaya MS database replication
• Avaya MS IP Traffic configuration
• Avaya MS key management
• Avaya MS lock management
• Avaya MS media port configuration
• Avaya MS Media management, including media for Treatment and Music on Hold.
• Avaya MS Media Security
• Avaya MS Network Element configuration
• Avaya MS server and cluster configuration
• Avaya MS QoS DSCP configuration

References
For more information, see the following documents:
• Avaya Aura® Application Server 5300 Overview, NN42040–100
• Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040–112
• Avaya Aura® Application Server 5300 Configuration, NN42040–500

OCS/MOC/Office Client support
Application Server 5300 Release 3.0 supports the Avaya Aura® AS 5300 Office Client.

Supported features
The list of features supported by the system has changed in Application Server 5300 Release 3.0.

Reference
For more information, see the following documents:
• Avaya Aura® Application Server 5300 Overview, NN42040-100.
• Avaya Aura® Application Server 5300 Features Reference, NN42040-118.
Tomcat and Jetspeed replaces JBoss

Tomcat Web Server replaces JBoss Application server as the servlet container, and Jetspeed 2 (which supports JSR 286) has replaced JBoss (which supports JSR 168) as the portal for portlets.

References
For more information, see the following documents:
• Avaya Aura® Application Server 5300 Configuration, NN42040–500.
• Avaya Aura® Application Server 5300 Security, NN42040–601.

Migrating to RHEL 6.6 and Java 8

Application Server 5300 Release 3.0 uses the RHEL 6.6 operating system and is compliant to the Red Hat Enterprise Linux 6 Security Technical Implementation Guide.

The system administration steps for the RHEL 6.6 based platform are the same as the administration steps for the older platform.

Application Server 5300 Release 3.0 uses Java 8 as the default library for both server and client. Administrators can log in to the Element Manager console by using Java 8 installed on the system.

References
For more information, see the Application Server 5300 Method of Procedure (MOP) documents.