Avaya Aura® Contact Center and Avaya Aura® Unified Communications Solution Description

Release 7.0.3
Issue 01.06
July 2018

© 2016-2018, Avaya Inc.
All Rights Reserved.

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=C20091120112456651010 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 ACCESSES 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 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 EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License 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 type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

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 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 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 MPEG 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 MPEG 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 Hotline at +1-800-643-2353 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, the Avaya logo, Avaya one-X® Portal, Avaya Aura® Communication Manager, Avaya Aura® Experience Portal, Avaya Aura® Orchestration Designer, Avaya Aura® Session Manager, Avaya Aura® System Manager, and Application Enablement Services are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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.

Contents

Chapter 1: Introduction ... 9
Purpose ... 9
Intended audience ... 9
Related resources ... 9
Avaya Aura® Contact Center Documentation ... 9
Viewing Avaya Mentor videos ... 13
Support ... 14
Chapter 2: Changes in this release ... 15
Feature changes ... 15
Avaya Callback Assist integration ... 15
Agent Desktop integration with Enterprise Web Chat ... 16
Avaya Media Server changes ... 16
Contact Center Manager Administration support for Caché database ... 17
Database restore not required for reinstating Mission Critical High Availability ... 17
Instant Messaging feature supports Microsoft Skype for Business 2015 ... 18
Support for Avaya Call Park and Page Snap-in ... 18
Support for Avaya Real-Time Speech Snap-in ... 18
Support for Avaya Smart Caller ID Inbound Snap-in ... 18
Support for Avaya Smart Caller ID Outbound Snap-in ... 18
Support for Avaya WebRTC Snap-in ... 18
Whisper Coaching ... 19
Other changes ... 19
Avaya Aura® Call Center Elite integration is no longer supported ... 19
Avaya Aura® Midsize Business Template is no longer supported ... 20
Avaya Aura® SIP Enablement Services is no longer supported ... 20
Avaya Aura® Unified Communications Release 5.2 and 6.1 are no longer supported ... 20
Avaya Aura® Unified Communications Release 6.x is no longer supported ... 20
Agent Greeting is no longer supported with Avaya Communication Server 1000 ... 20
Microsoft Windows Server 2008 is no longer supported ... 21
Microsoft Windows XP and Windows Vista are no longer supported ... 21
Multimedia Complement for Elite server type no longer supported ... 21
No Switch Configured Multimedia Only server type is no longer supported ... 21
Security Framework server type no longer supported ... 22
Chapter 3: Solution overview ... 23
SIP-enabled Contact Centers ... 23
Avaya Aura® Unified Communications platform SIP-enabled contact center ... 23
SIP-enabled contact center call flow ... 26
SIP network components ... 27
Contact Center SIP domain ... 29

Components ... 30
Offsite Agent Overview ... 33
Chapter 4: Solution specification ... 35
Maximum agent capacity and call rate values ... 36
Orchestration Designer application Variables and Intrinsics ... 41
Email limits and capacity values ... 42
Contact Center Multimedia disk storage requirements ... 43
Required database files ... 43
Email attachment storage ... 44
Outbound capacity ... 44
Chapter 5: SIP Contact Center configuration requirements ... 46
General requirements ... 46
SIP-enabled Contact Center feature limitations ... 46
Dependent platform and switch compatibility ... 47
Upgrade path ... 47
SIP session expiry parameters ... 47
Digital Signal Processing Considerations ... 47
Voice over Internet Protocol ... 48
PABX Digital Signal Processors ... 49
Avaya Aura® Shuffling ... 50
PABX DSP consumption examples ... 50
Avaya Aura® Unified Communications platform DSP ... 51
Dialed Number Identification Service ... 51
DNIS Options in SIP-enabled contact centers ... 51
Incoming SIP Invite message with DNIS information in the To header ... 52
Incoming SIP Invite message with DNIS information in the History-Info header ... 52
Session Manager systems ... 52
Chapter 6: Licensing ... 53
How to obtain a license for a nodal SIP-enabled solution ... 53
Chapter 7: Avaya Aura® Experience Portal Integration ... 55
Data transfer methods ... 56
Avaya Aura® Experience Portal Orchestration Designer ... 57
Voice XML ... 57
Call Control XML ... 57
SIP-enabled Avaya Aura® Contact Center ... 57
P-Intrinsic SIP Header ... 58
User-to-User Information ... 59
Universal Call Identifier ... 60
Avaya Aura® Contact Center Web Service Open Interfaces ... 60
Web Services Open Interfaces ... 60
Front-end Avaya Aura® Experience Portal self-service using Contact Center Web Service Open Interfaces ... 60
Call flow example using CCMS Web service Open Interfaces ... 62

Front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center..... 63
Call flow example for front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center..... 65
Back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center..... 66
Call flow example using back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center..... 68
Back-end Avaya Aura® Experience Portal using Context Creation and SIP-enabled Contact Center..... 69
Call flow example using back-end Avaya Aura® Experience Portal with the Context Creation sample application..... 71
Avaya DevConnect..... 73
Chapter 8: Mission Critical High Availability overview..... 74
MCHA switchover..... 74
Agent experience during an MCHA switchover..... 75
Administrator experience during an MCHA switchover..... 75
Supervisor experience during an MCHA switchover..... 76
Switchover Handling Script..... 76
Mission Critical High Availability operation..... 78
Mission Critical High Availability campus solutions..... 80
Mission Critical HA with Avaya Aura® platform resiliency..... 80
Mission Critical HA without Avaya Aura® platform resiliency..... 81
Mission Critical HA with Avaya Aura® Unified Communications Virtualized Environment 83
Geographic High Availability solution..... 84
Mission Critical High Availability configuration utilities..... 87
How to reinstate High Availability resiliency after a switchover..... 89
How to reinstate High Availability resiliency after a total network outage..... 90
How to manually switch over to the Remote Geographic Node of a Mission Critical solution..... 91
How to revert to the campus site after running the RGN for a few days..... 92
Avaya Aura® platform campus resiliency..... 94
High Availability campus site..... 94
Communication Manager survivability overview..... 96
Session Manager redundancy overview..... 96
Application Enablement Services Machine Preserving High Availability overview..... 97
Application Enablement Services Geographical Redundancy Preserving High Availability overview..... 98
Avaya Aura® platform geographic resiliency..... 100
Campus site and remote geographic site..... 100
Communication Manager Survivable Core (ESS)..... 101
Session Manager geographical redundancy overview..... 102
Application Enablement Services geographical redundancy overview..... 102
Offsite Agent resiliency..... 103
Chapter 9: Microsoft instant messaging server requirements..... 104
Licensing requirements..... 106

Chapter 10: Avaya Aura® Presence Services requirements..... 107
Avaya Aura® Presence Services overview..... 107
Hardware requirements..... 109
Operating system requirements..... 109
Licensing requirements..... 109
High Availability..... 109

Chapter 1: Introduction

Purpose

This document describes the product or solution architecture, suggested topologies, capacities, and interoperability. This document also describes the features and functional limitations of certain configurations. With this information, sales design specialists can make decisions about designs that meet the business needs of a customer.

Intended audience

This document is intended for anyone who wants to gain a high-level understanding of the product features, functionality, capacities, and limitations within the context of solutions and verified reference configurations.

Related resources

Avaya Aura® Contact Center Documentation

The following table lists the documents related to Avaya Aura® Contact Center. Download the documents from the Avaya Support website at https://support.avaya.com.

Title	Use this document to:	Audience
Overview		
Avaya Aura® Contact Center Overview and Specification	This document contains technical details you need to set up your Contact Center suite. The document contains the background information you need to plan and engineer your system (server preparation information, routing options, licensing configurations, and hardware configuration). The document also	Customers and sales, services, and support personnel

Title	Use this document to:	Audience
	contains background information you require to install all software components that are part of and work with Contact Center. General information about considerations for upgrading your existing suite of Contact Center is also included. This document contains strategies and requirements to plan your network configuration and prepare your servers for Contact Center software installations.	
Avaya Aura® Contact Center and Avaya Aura® Unified Communications Solution Description	This document describes the solution architecture, suggested topologies, and capacities for the Avaya Aura® Unified Communications platform. This document also describes the features and functional limitations of certain configurations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center and Avaya Communication Server 1000 Solution Description	This document describes the solution architecture, suggested topologies, and capacities for the Avaya Communication Server 1000 platform. This document also describes the features and functional limitations of certain configurations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center Documentation Catalog	This document describes available Avaya Aura® Contact Center documentation resources and indicates the type of information in each document.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center Terminology	This document contains definitions for the technical terms specific to Contact Center.	Customers and sales, services, and support personnel
Contact Center Performance Management Data Dictionary	This document contains reference tables that describe the statistics and data in the historical and real-time reports generated in Contact Center.	System administrators and contact center supervisors
Implementing		
Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration	This document contains information and procedures to integrate the Avaya Aura® Unified Communications platform with Contact Center.	Implementation personnel
Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration	This document contains information and procedures to integrate the Avaya Communication Server 1000 platform with Contact Center.	Implementation personnel

Title	Use this document to:	Audience
Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications	This document contains information about Contact Center DVD installation, initial configuration, and verification for the Avaya Aura® Unified Communications platform.	Implementation personnel
Deploying Avaya Aura® Contact Center DVD for Avaya Communication Server 1000	This document contains information about Contact Center DVD installation, initial configuration, and verification for the Avaya Communication Server 1000 platform.	Implementation personnel
Deploying Avaya Aura® Contact Center Software Appliance for Avaya Aura® Unified Communications	This document describes how to deploy the Avaya Aura® Contact Center Software Appliance for the Avaya Aura® Unified Communications platform.	Implementation personnel
Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications	This document contains information for Contact Center preparation, process, initial configuration, and verification of the installation on the Avaya Aura® Unified Communications platform.	Implementation personnel
Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000	This document contains information for Contact Center preparation, process, initial configuration, and verification of the installation on the Avaya Communication Server 1000 platform.	Implementation personnel
Avaya Aura® Contact Center and Proactive Outreach Manager Integration	This document provides conceptual and procedural information on the integration between Avaya Aura® Contact Center (AACC) and Avaya Proactive Outreach Manager (POM); it describes the tasks required for AACC and POM integration.	Implementation personnel
Upgrading and patching Avaya Aura® Contact Center	This document contains information and procedures to upgrade from previous releases to Contact Center, migrating the databases, and information and procedures to download and install service packs.	Implementation personnel and system administrators
Administering		
Avaya Aura® Contact Center Server Administration	This document contains information and procedures for day-today maintenance of all servers in the Contact Center suite, including server maintenance tasks, administrative tasks, managing data, configuring data routing, performing archives, and backing up data. It also describes the	System administrators

Title	Use this document to:	Audience
	optional configuration procedures for server configuration.	
Avaya Aura® Contact Center Client Administration	This document contains information and procedures to configure the users and user access, skillsets, server management, and configuration data in the Contact Center database.	System administrators and contact center supervisors
Using Contact Center Orchestration Designer	This document contains information and procedures to configure script and flow applications in Contact Center Orchestration Designer.	System administrators
Maintaining		
Maintaining Avaya Aura® Contact Center	This document contains routine maintenance procedures such as installing service packs, and maintaining the databases for the Contact Center system.	System administrators and support personnel
Troubleshooting Avaya Aura® Contact Center	This document contains system-wide troubleshooting information and procedures for Contact Center hardware, software, and network.	System administrators and support personnel
Contact Center Event Codes	This document contains a list of errors in the Contact Center suite and recommendations to resolve them. This document is a Microsoft Excel spreadsheet.	System administrators and support personnel
Using		
Using Avaya Aura® Contact Center Reports and Displays	This document contains procedures to generate performance reports, and to monitor and analyze performance data and performance measurements.	System administrators and contact center supervisors
Using Agent Desktop for Avaya Aura® Contact Center	This document provides information and procedures for agents who use the Agent Desktop application to accept, manage, and close contacts of all media types in Contact Center.	Contact center agents and supervisors
Using the Contact Center Agent Browser application	This document provides information and procedures for agents who use the Agent Browser application to log on to Contact Center and perform basic tasks.	Contact center agents

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

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

Chapter 2: Changes in this release

The following sections describe the new features and changes in Avaya Aura® Contact Center Release 7.0.

Feature changes

New features in the Release 7.0 base build

See the following sections for information about new features in the Release 7.0 base build:

- Avaya Callback Assist integration on page 15
- Avaya Media Server changes on page 16
- Contact Center Manager Administration support for Caché database on page 17
- Database restore not required for reinstating Mission Critical High Availability on page 17

New features in Release 7.0 Feature Pack 1

See the following sections for information about new features added by Feature Pack 1:

- Agent Desktop integration with Enterprise Web Chat on page 16
- Instant Messaging feature supports Microsoft Skype for Business 2015 on page 18
- Whisper Coaching on page 19

New features in Release 7.0 Feature Pack 2

See the following sections for information about new features added by Feature Pack 2:

- Support for Avaya Call Park and Page Snap-in on page 18
- Support for Avaya Real-Time Speech Snap-in on page 18
- Support for Avaya Smart Caller ID Inbound Snap-in on page 18
- Support for Avaya Smart Caller ID Outbound Snap-in on page 18
- Support for Avaya WebRTC Snap-in on page 18

Avaya Callback Assist integration

Avaya Aura® Contact Center (AACC) Release 7.0 supports integration of the Avaya Callback Assist (CBA) snap—in application, for SIP-enabled contact centers.

Avaya Callback Assist is an application developed on Avaya Aura® Experience Portal that enables customers calling a contact center to request a call back. For example, a customer can decide that the estimated wait time to speak to an agent is too long. The customer can request a call back, so that when an agent becomes available, the contact center calls the customer.

An Avaya application note describes the integration between SIP-enabled AACC and CBA. Check http://support.avaya.com for the most recent application note on CBA integration with AACC.

Agent Desktop integration with Enterprise Web Chat

Agent Desktop Release 7.0 Feature Pack 1 integrates with Enterprise Web Chat (EWC). Agent Desktop Release 7.0 Feature Pack 1 provides two services for web chat: the Web Communications text chat and EWC. Use EWC if you require a large number of web chat sessions. EWC can support up to 3000 simultaneous Web chat sessions.

Agent Desktop integration with EWC is supported only if Avaya Aura® Contact Center is deployed on Communication Manager with a standalone Multimedia server. EWC is a licensed feature. For Agent Desktop to handle EWC contacts, administrators must enable a setting on the Contact Center Multimedia (CCMM) Administration utility.

Note:

If you migrate from an existing Web Communications chat solution to the EWC chat solution, you must redevelop your custom interfaces to integrate with EWC.

Avaya Media Server changes

Avaya Media Server is now called Avaya Aura® Media Server. Avaya Aura® Contact Center Release 7.0 supports only Avaya Aura® Media Server Release 7.7.

Avaya Aura® Contact Center Release 7.0 no longer requires or uses the Contact Center Services for Avaya Media Server (CCSA) component. Avaya Aura® Contact Center Release 7.0 integrates directly with Avaya Aura® Media Server Release 7.7 using Media Server Markup Language (MSML) based communication.

Avaya Aura® Contact Center and Avaya Aura® Media Server use MSML to control how Route Point calls are anchored and treated. Avaya Aura® Contact Center also uses MSML to control Route Point call features such as Agent Greeting, Barge-in, Observe, Zip Tone, and Whisper Skillset announcements.

In Contact Center Manager Administration (CCMA) *Media Services and Routes* configuration, Avaya Aura® Media Server Release 7.7 instances now provide a new MSML-based service type named ACC_APP_ID. This new ACC_APP_ID service type replaces the CONF service type provided by Avaya Media Server Release 7.6.

The following features, previously configured in Avaya Media Server Element Manager, are now configured in Contact Center Manager Administration (CCMA).

- Barge-in tone
- Observation tone
- Call Force Answer Zip tone
- Custom Zip tones
- Whisper Skillset announcement

Enable or disable Barge-in and Observation tones in CCMA *Global Settings*.

Upload the tone and announcement .WAV files in CCMA *Prompt Management*.

Configure Call Force Answer Zip Tone and Whisper Skillset in CCMA *Call Presentation Classes — Prompt On Answer*.

Avaya Aura® Media Server supports only the following deployment options:

- Co-resident with Avaya Aura® Contact Center on a Windows Server 2012 R2 server
- Standalone on a Red Hat Enterprise Linux 6.x 64–bit server

Avaya Aura® Media Server is also available as an Open Virtual Appliance (OVA) package. You can use this OVA file to create an Avaya Aura® Media Server virtual appliance on a VMware host.

Virtualized Avaya Aura® Media Server supports High Availability (HA).

Contact Center Manager Administration support for Caché database

In Contact Center Release 7.0, Contact Center Manager Administration (CCMA) stores information in a Caché database. Contact Center Release 7.0 stores agent, user, statistical, scheduling, and reporting information in Caché databases. This simplifies Contact Center data management, migration, and maintenance. This also simplifies the resiliency configuration processes.

In Contact Center Release 7.0, Contact Center Manager Administration (CCMA) does not store information using Active Directory Lightweight Directory Services (AD-LDS) or Microsoft Access databases.

Database restore not required for reinstating Mission Critical High Availability

After a managed switchover, administrators do not need to restore the database from the new active server to the standby server to re-instate HA.

A managed switchover is a switchover initiated by the administrator or caused by a Contact Center software service outage.

Instant Messaging feature supports Microsoft Skype for Business 2015

From Release 7.0 Feature Pack 1, the Contact Center Instant Messaging feature integrates with Microsoft Skype for Business 2015. Integration and operation is identical with releases of Microsoft Lync already supported in the Contact Center 7.0 base release.

Support for Avaya Call Park and Page Snap-in

From Release 7.0 Feature Pack 2, Avaya Aura® Contact Center inter-operates with the Avaya Call Park and Page Snap-in. The Avaya Call Park and Page Snap-in provides the ability for calls to be parked on a fixed or dynamic extension while an attendant pages an expert. The call can then be picked up by the paged party.

Support for Avaya Real-Time Speech Snap-in

From Release 7.0 Feature Pack 2, Avaya Aura® Contact Center inter-operates with the Avaya Real-Time Speech Snap-in. The Avaya Real-Time Speech Snap-in provides a method of searching for speech on an answered call and reporting matches in real-time.

Support for Avaya Smart Caller ID Inbound Snap-in

From Release 7.0 Feature Pack 2, Avaya Aura® Contact Center inter-operates with the Avaya Smart Caller ID Inbound Snap-in. The Avaya Smart Caller ID Inbound Snap-in provides a method of providing a called party with additional information about a calling party.

Support for Avaya Smart Caller ID Outbound Snap-in

From Release 7.0 Feature Pack 2, Avaya Aura® Contact Center inter-operates with the Avaya Smart Caller ID Outbound Snap-in. The Avaya Smart Caller ID Outbound Snap-in provides a method of configuring caller ID name and number information for outbound calls based on the original caller ID information, the called number, or a combination of both.

Support for Avaya WebRTC Snap-in

From Release 7.0 Feature Pack 2, Avaya Aura® Contact Center inter-operates with the Avaya WebRTC Snap-in. Avaya WebRTC Snap-in enables click-to-call from web applications, for example from a customer facing website, or an enterprise directory web page.

Whisper Coaching

From Release 7.0 Feature Pack 1, SIP-enabled Contact Centers extend the Supervisor Observe feature to include Whisper Coaching. Using Whisper Coaching, a supervisor can talk to an agent on a skillset call with a customer, without being heard by the customer. In the coaching mode, a supervisor can hear everything that is said on the call. However, the advice that the supervisor provides is audible only to the agent.

Whisper Coaching improves agent training and performance because supervisors can coach the agent by whispering advice to the agent.

Other changes

Changes in the Release 7.0 base build

See the following sections for information about other changes in the Release 7.0 base build:

- Avaya Aura Call Center Elite integration is no longer supported on page 19
- Avaya Aura Midsize Business Template (MBT) is no longer supported on page 20
- Avaya Aura SIP Enablement Services is no longer supported on page 20
- Avaya Aura Unified Communications Release 5.2 and 6.1 are no longer supported on page 20
- Avaya Aura Unified Communications Release 6.x is no longer supported on page 20
- Agent Greeting is no longer supported with CS1000 on page 20
- Microsoft Windows Server 2008 is no longer supported on page 21
- Microsoft Windows XP and Windows Vista are no longer supported on page 21
- Multimedia Complement for Elite server type no longer supported on page 21
- No Switch Configured Multimedia Only server type is no longer supported on page 21
- Security Framework server type no longer supported on page 22

Changes in Release 7.0 Feature Pack 3

See the following sections for information about other changes in Release 7.0 Feature Pack 3:

- Avaya Aura Unified Communications Release 6.x is no longer supported on page 20

Avaya Aura® Call Center Elite integration is no longer supported

Avaya Aura® Contact Center Release 7.0 does not support integration with Avaya Aura® Call Center Elite.

Avaya Aura® Midsize Business Template is no longer supported

Avaya Aura® Contact Center Release 7.0 does not support integration with the Avaya Aura® Midsize Business Template (MBT) voice platform.

Avaya Aura® SIP Enablement Services is no longer supported

Avaya Aura® Contact Center Release 7.0 does not support integration with Avaya Aura® SIP Enablement Services (SES).

Avaya Aura® Unified Communications Release 5.2 and 6.1 are no longer supported

Avaya Aura® Contact Center Release 7.0 does not support Avaya Aura® Unified Communications (UC) Release 5.2 and 6.1.

Avaya Aura® Contact Center Release 7.0 supports integration with Avaya Aura® Unified Communications (UC) Release 6.2 FP4 and Release 7.0.

Avaya Aura® Contact Center Release 7.0 supports integration with Avaya Aura® Solution for Midsize Enterprise Release 6.2 FP4.

Avaya Aura® Unified Communications Release 6.x is no longer supported

Avaya Aura® Contact Center Release 7.0 does not support Avaya Aura® Unified Communications (UC) Release 6.x.

Avaya Aura® Contact Center Release 7.0 supports integration with Avaya Aura® Unified Communications (UC) Release 7.0.x, 7.1.x, and 8.0.

Agent Greeting is no longer supported with Avaya Communication Server 1000

Avaya Aura® Contact Center solutions integrated with an AML-based Avaya Communication Server 1000 switch no longer supports the Agent Greeting feature.

Avaya Aura® Contact Center solutions integrated with a SIP-enabled Avaya Aura® Unified Communications platform continues to support Agent Greeting.

For Avaya Aura® Contact Center Release 7.0, Agent Greeting is no longer an Avaya Aura® Media Server based application. The Agent Greeting application is now deployed on an AACC Tomcat instance. This change has no effect on agents and supervisors using Agent Greeting. For customers migrating to AACC Release 7.0, the Agent Greeting feature is automatically migrated from Avaya Aura® Media Server to the AACC Tomcat instance.

Microsoft Windows Server 2008 is no longer supported

Avaya Aura® Contact Center Release 7.0 is supported only on Microsoft Windows Server 2012 R2. Avaya Aura® Contact Center Release 7.0 is not supported on Microsoft Windows Server 2008 R2. Customers upgrading to Avaya Aura® Contact Center Release 7.0 must migrate to a new Microsoft Windows Server 2012 R2 server.

Microsoft Windows XP and Windows Vista are no longer supported

Avaya Aura® Contact Center and Agent Desktop Release 7.0 do not support Microsoft Windows XP or Microsoft Windows Vista. Avaya Aura® Contact Center and Agent Desktop Release 7.0 support Microsoft Windows 7, 8.1 and 10.

Multimedia Complement for Elite server type no longer supported

Avaya Aura® Contact Center Release 7.0 does not support the Multimedia Complement for Elite server type. Customers with an existing Multimedia Complement for Elite solution can migrate to an Avaya Aura® Contact Center Release 7.0 Voice and Multimedia Contact Server.

No Switch Configured Multimedia Only server type is no longer supported

Avaya Aura® Contact Center Release 7.0 does not support the No Switch Configured - Voice and Multimedia Contact Server with Avaya Media Server installation option. In Avaya Aura® Contact Center Release 7.0, for multimedia-only solutions, install a Voice and Multimedia Contact Server but do not configure the voice-related options.

Security Framework server type no longer supported

Avaya Aura® Contact Center Release 7.0 does not support the Security Framework server type. Customers with an existing Security Framework server can change to a single sign-on (SSO) configuration based on an Avaya Aura® System Manager.

Chapter 3: Solution overview

This section describes an Avaya Aura® Contact Center and Avaya Aura® Unified Communications integrated solution.

SIP-enabled Contact Centers

Avaya Aura® Contact Center supports SIP-enabled contact centers based on the Avaya Aura® Unified Communications platform.

Session Initiation Protocol (SIP) is a signaling protocol widely used to control communication sessions such as voice calls over Internet Protocol (IP). SIP works in the application layer of the Open Systems Interconnection (OSI) communications model. SIP can establish, change, and end Internet telephony calls. SIP is independent of the underlying transport layer. SIP is a text-based protocol. SIP incorporates many elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP) for direct inspection by administrators.

SIP-enabled contact centers with Contact Center Multimedia can support multimedia contact types such as email and Web Communications.

Avaya Aura® Unified Communications platform SIP-enabled contact center

Avaya Aura® Contact Center uses industry-standard SIP and CSTA (TR/87 over SIP) interfaces to communicate with other SIP-enabled devices. Avaya Aura® Contact Center uses a SIP Gateway Manager component to support SIP. SIP Gateway Manager (SGM) is a Contact Center Manager Server component and a standalone SIP element.

The Avaya Aura® Unified Communications platform supports SIP. Integrating Contact Center with the Avaya Aura® Unified Communications platform using SIP infrastructure supports communication between customers and contact center agents. This integration gives Contact Center access to and control of Avaya Aura® Communication Manager telephones. Avaya Aura® benefits from Contact Center skill-based routing, call treatments, reporting, and the graphical Orchestration Designer. Avaya Agent Desktop supports Avaya Aura® Communication Manager telephones, email, and Web chat contact types.

Avaya Aura® Contact Center supports the following Avaya Aura® Unified Communications platform components.

- Avaya Aura® Communication Manager (CM)
- Avaya Aura® Session Manager (SM)
- Avaya Aura® Application Enablement Services (AES)

Avaya Aura® System Platform is a real-time virtualization technology that you can use to deploy unmodified versions of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Aura® Application Enablement Services on a single server.

The following diagram shows a typical SIP-enabled contact center based on an Avaya Aura® Unified Communications platform.

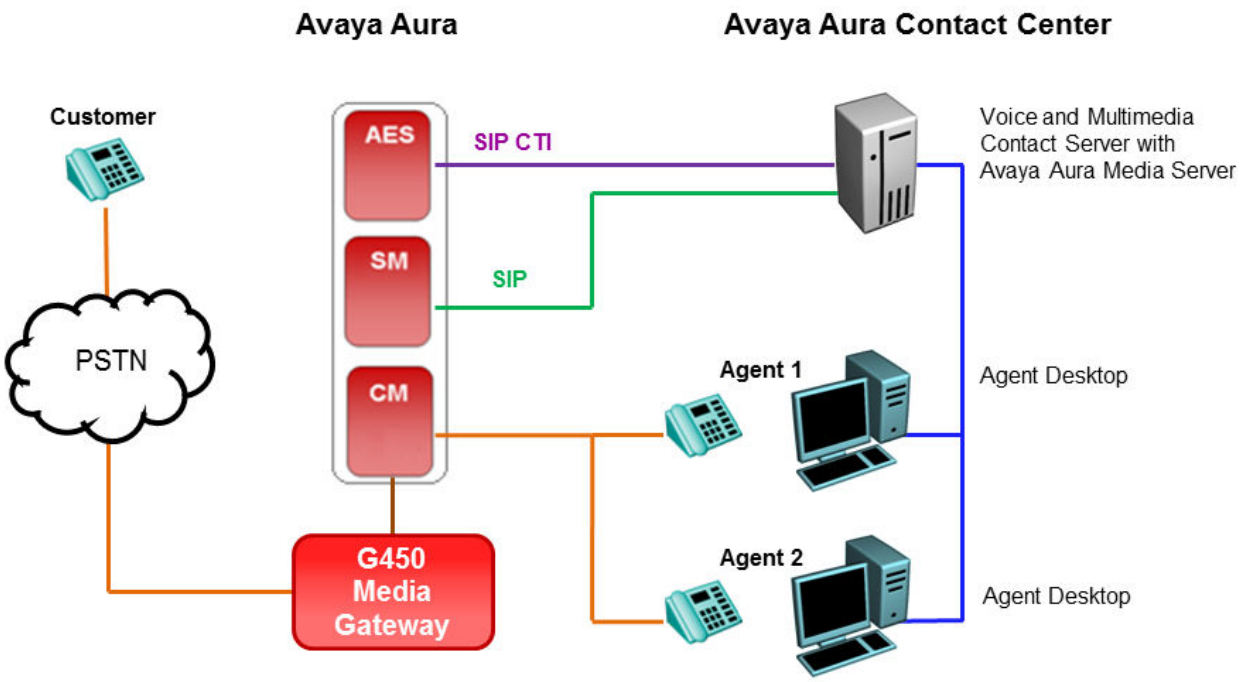


Figure 1: Typical SIP-enabled contact center using the Avaya Aura® Unified Communications platform

For more information about configuring an Avaya Aura® Unified Communications platform-based contact center, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

Avaya Aura® Communication Manager

Avaya Aura® Communication Manager is an IP telephony platform. Communication Manager delivers centralized call control for resilient and distributed networks and supports a wide range of servers, gateways, analog, digital, and IP-based communication devices. Communication Manager has advanced built-in capabilities including mobility applications, call features, and conference calling.

Complete the following configuration items for Communication Manager integration with Avaya Aura® Contact Center.

- Configure the Communication Manager stations for Avaya Aura® Contact Center agents.
- Configure Communication Manager to route calls to and from Avaya Aura® Contact Center using Avaya Aura® Session Manager.
- Configure Communication Manager to communicate with Application Enablement Services for station control and monitoring.

Avaya Aura® System Platform is a real-time virtualization technology that you can use to deploy unmodified versions of Avaya Aura® Communication Manager, Session Manager, and Application Enablement Services on a single server.

Avaya Aura® Application Enablement Services

Avaya Aura® Application Enablement Services (AES) is a collection of enhanced telephony APIs, protocols, and Web services. Application Enablement Services supports access to the call processing, media, and administrative features available in Communication Manager. Application Enablement Services integrates with applications.

The Avaya Device Media and Call Control (DMCC) APIs provided by Application Enablement Services provides applications with access to the basic third-party call control capabilities of Communication Manager.

The AES server uses Transport Layer Security (TLS) communication channels for the SIP CTI connection with Contact Center. TLS is a public key encryption cryptographic protocol, which helps secure a communications channel from danger or loss, and provides privacy and safety. Public key cryptography uses two keys, one public, and one private.

You can obtain a root certificate from your Certificate Authority. A root certificate is an unsigned public key that identifies the Root Certificate Authority (CA). Add the root certificate to the AES server and then use the root certificate to generate a Certificate Signing Request (CSR). Send the CSR and the Common Name (CN) of the AES server to your CA. The CA verifies the identity of the request and issues a signed certificate (a private key) for the AES server.

You must apply the root certificate and the signed client certificate from your Certificate Authority to the AES server. Apply the same root certificate to Contact Center and use the root certificate to create a signed client certificate for the Contact Center side of the secure TLS SIP link. AES and Contact Center can then communicate securely using a TLS SIP connection.

Avaya Aura® Session Manager

Avaya Aura® Contact Center supports integration with Avaya Aura® Session Manager.

Avaya Aura® Session Manager is a SIP routing and integration tool. Session Manager integrates the SIP entities across the entire network within a company. Session Manager provides a core communication service and adds SIP-enabled architecture. Session Manager connects to and acts as a system-wide dial plan for Avaya Aura® Communication Manager using direct SIP connections.

Avaya Aura® System Manager

Avaya Aura® System Manager delivers a collection of shared, secure management services, and a common console across multiple products. You can use System Manager to manage and configure the routing policies for all Session Manager instances in your solution. System Manager communicates with Session Manager using secure links.

SIP-enabled contact center call flow

The following diagram shows how a SIP-enabled contact center processes a typical customer call.

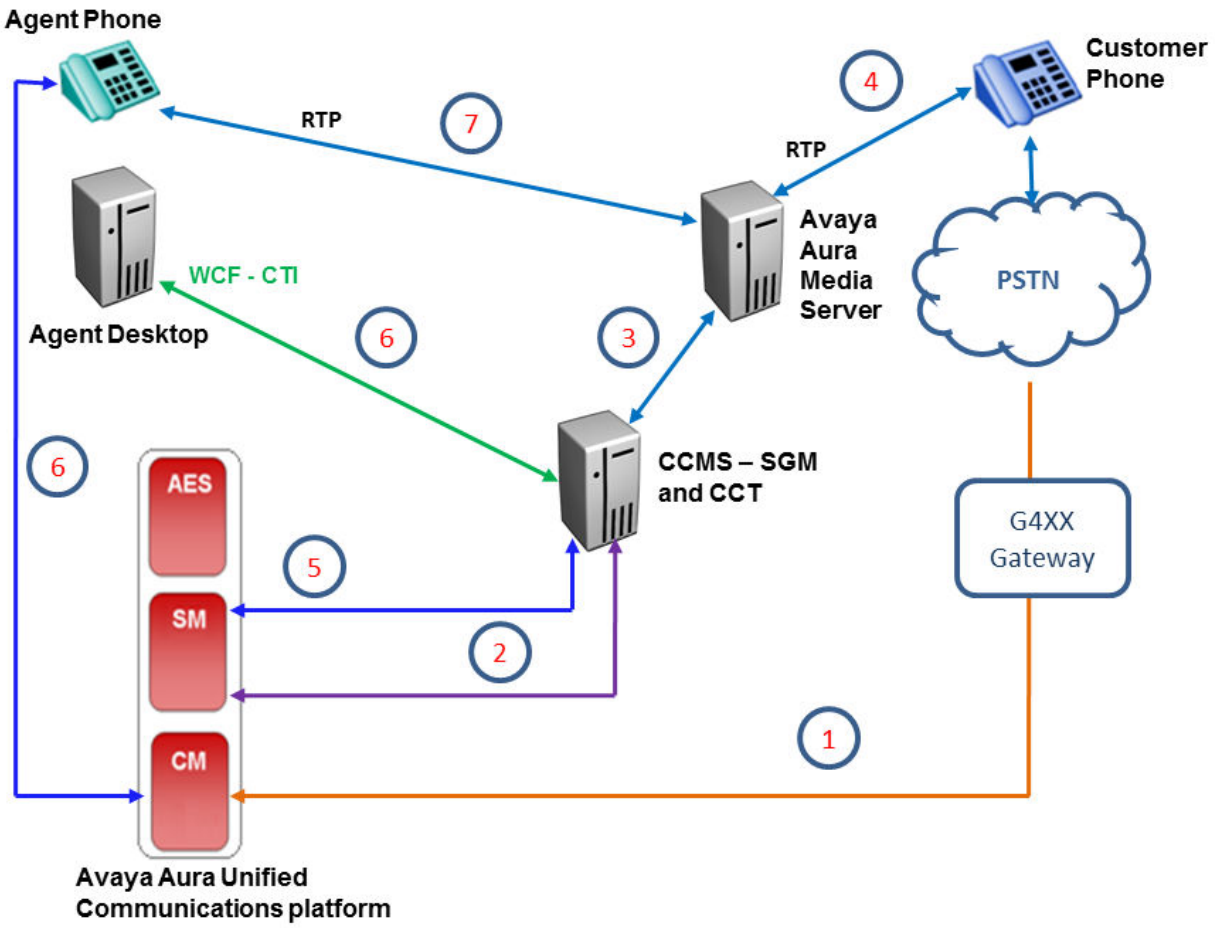


Figure 2: SIP-enabled contact center typical call flow example

The following steps outline how a SIP-enabled contact center processes a typical customer call:

1. A customer calls the contact center. Communication Manager examines the incoming number and routes the call to a signaling group destined for Session Manager.

2. Session Manager routes the call to Avaya Aura® Contact Center based on matching dial patterns, Linux regular expressions, and routing policies, entity links, and SIP entities. Session Manager then sends a SIP INVITE message to Contact Center.
3. When the SIP INVITE message arrives at the Contact Center Manager Server (CCMS), CCMS matches the message with one of the configured Route Point URIs. CCMS then anchors the customer call on an Avaya Aura® Media Server conference port.
4. Avaya Aura® Media Server establishes a Real-Time Transport Protocol (RTP) media and voice path to the customer. CCMS handle the customer's call using this conference port for the duration of the call.
5. When CCMS has identified an agent to handle this call, CCMS sends a SIP INVITE message to Session Manager. When the SIP INVITE message arrives at Session Manager, Session Manager sends the message to the Communication Manager in control of the destination agent H.323 telephone.
6. Communication Manager sends a H.323 request to the agent telephone to indicate that a new call has arrived. The agent telephone rings and Communication Manager sends a SIP 180 Ringing message back to CCMS using the Session Manager. CCMS uses this trigger to inform the Avaya Agent Desktop that a call is alerting on the telephone. In this way, both the agent telephone and the Avaya Agent Desktop software client show the customer call as ringing.
7. At this point, the agent can answer the call using Avaya Agent Desktop or using the telephone.
   - If the agent answers the customer call using the telephone, Communication Manager sends a SIP 200 OK message to the Session Manager and on to the CCMS server. CCMS then notifies the Avaya Agent Desktop client software using Computer Telephony Integration (CTI) that the agent answered the customer call.
   - If the agent answers the customer call using the Avaya Agent Desktop client software, CCMS sends a TR87 AnswerCall request to Communication Manager using Application Enablement Services. This causes the agent telephone to answer the call. Communication Manager sends a SIP 200 OK message through Session Manager to CCMS and, CCMS using CTI notifies the Avaya Agent Desktop client software that the agent answered the customer call.

   Avaya Aura® Media Server establishes a conference between the agent and the customer and the customer and the agent can now communicate.

SIP network components

A SIP network consists of different SIP-specific logical components. The following are some examples of the SIP network components used in a typical SIP-enabled Avaya Aura® Contact Center solution:

SIP Proxy server

A SIP proxy is an intermediary entity that functions as both a server and a client for making requests for other clients. A proxy server interprets and rewrites specific parts of a request message before forwarding the message.

SIP Voice Proxy server

The SIP Voice Proxy server supports inbound and outbound calls, such as routing a call to an agent telephone. In an Avaya Aura® Contact Center solution, the SIP Voice Proxy server is an Avaya Aura® Session Manager.

SIP CTI Proxy server

The SIP CTI Proxy server supports SIP Computer Telephony Integration (CTI) so that Avaya Agent Desktop can acquire and control agent telephones for call control. In an Avaya Aura® Contact Center solution, the SIP CTI Proxy server is an Avaya Aura® Application Enablement Services server.

SIP Endpoint

The SIP communication model realizes many functions in the terminal device. An example of a contact center SIP Endpoint is the Avaya 9640 SIP telephone.

SIP Entity

Avaya Aura® Contact Center registers as a SIP Entity with the SIP Voice Proxy. The SIP Voice Proxy routing policy and the dial pattern route calls to Avaya Aura® Contact Center for agent assistance. SIP Gateway Manager (SGM) is a Contact Center Manager Server component and a standalone SIP element used by Contact Center to communicate with other SIP-enabled devices.

The Contact Center Manager Server SIP Gateway Manager (SGM) handles calls from the SIP Voice Proxy. SIP Gateway Manager is the gateway to the call processing components in the contact center.

SIP User Agent (UA)

The SIP User Agent represents a terminal device in a SIP network. SIP user agents (UA) are endpoints. User Agents are intelligent stateful entities consisting of a SIP user agent client (UAC) and SIP server (UAS). SIP endpoints can end or originate SIP sessions.

A SIP User Agent:

- Terminates (SIP UAS) or originates (SIP UAC) SIP sessions.
- Addressed through logical address of record, such as pat@cc.avaya.com.
- Registers the current position with a central proxy server.

Examples of contact center SIP User Agents:

- Agent, SIP telephone, or SIP client software. A typical agent address is sip: 3794@135.166.107.38
- Supervisor Agents (SIP telephone or SIP client software)
- Avaya Aura® Media Server
- Avaya Aura® Communication Manager

SIP BBUA

A SIP Back-to-Back User Agent (BBUA) is an entity that intercepts and modifies messaging between a UAS and a UAC. A SIP Back-to-Back User Agent provides intelligent call control for the

local party. The Avaya Aura® Contact Center SIP Gateway Manager component functions as a BBUA intercepting the incoming customer calls. SIP Gateway Manager provides call treatments and assistance to customers.

SIP domain

A SIP domain is logical space where SIP devices exist, authenticate, and communicate. In a SIP network a destination address consists of both a user and a domain. A Uniform Resource Identifier (URI) consists of a user name and a domain name. A SIP domain can conceptually represent a service, a company, or a business.

When a SIP application initiates a call, the SIP message looks like this "INVITE 1234@aacc.com". This application wants to call number "1234" in the "aacc" company or domain. The local SIP proxy server processes this SIP message. The local proxy server uses the domain part of the SIP request to determine how to route this message to the destination. If the domain of the SIP message matches with the SIP domain configured on the SIP proxy, the SIP proxy handles the call within the same domain. Otherwise, the SIP proxy forwards the message to a different domain.

The SIP domain name can be the same or different from the Active Directory domain name. The Contact Center SIP domain name usually matches the corresponding Active Directory domain name.

Contact Center SIP domain

The Avaya Aura® Contact Center SIP domain name must match the Avaya Aura® Session Manager SIP domain name. When integrating Avaya Aura® Contact Center and the Avaya Aura® Unified Communications platform, the Avaya Aura® Contact Center "Local SIP Subscriber Domain Name" must match the Avaya Aura® Session Manager SIP "Routing Domain" name configured for contact center.

The Avaya Aura® Contact Center Local SIP Subscriber Domain Name typically matches the local Windows Active Directory domain name.

The following diagram shows a typical SIP domain in an Avaya Aura® Unified Communications platform and Avaya Aura® Contact Center integration.

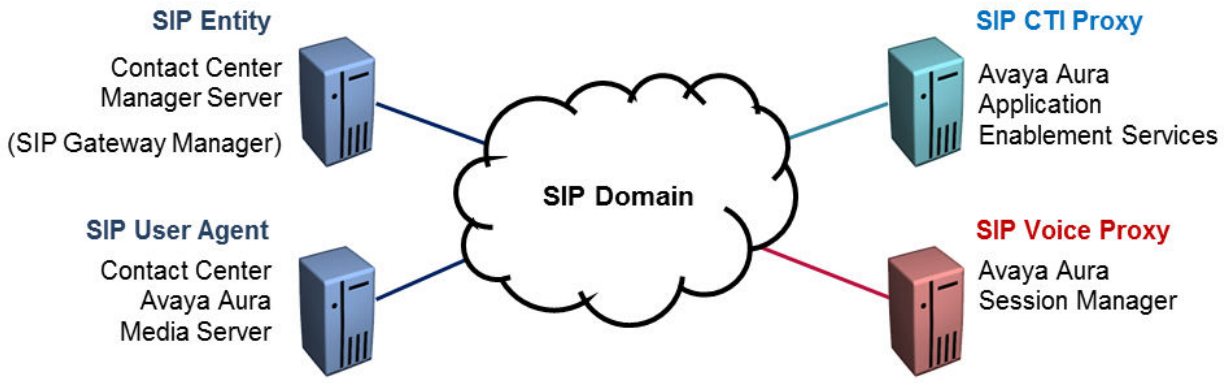


Figure 3: Example of a typical Contact Center SIP domain

In Avaya Aura® Media Server Element Manager (EM), you organize media within a content namespace. The content namespace name must match the contact center SIP domain name. The Avaya Aura® Media Server content namespace must match the “Local SIP Subscriber Domain Name” in Contact Center Manager Server Server Configuration. You must create one locale-specific content group for treatments such as announcements. The locale-specific content group must match the Local SIP Subscriber Locale in Contact Center Manager Server Server Configuration.

Contact Center Services for Avaya Aura® Media Server uses the SIP domain of the RequestURI in the incoming INVITE to fetch prompts and treatments from the content store. The INFO messages Contact Center sends to Avaya Aura® Media Server contain the locale value of the prompts and treatments.

You must configure all agents, supervisor agents, and Avaya Aura® Media Servers, with the same SIP domain name.

Components

Table 1: Avaya Aura® Contact Center for Avaya Aura® Unified Communications platform solution components

Component	Version	Reference Configuration Characteristics
Avaya Aura® Contact Center	7.0.3	Avaya Aura® Contact Center provides context sensitive and skill-based routing for customer voice and multimedia contacts. Avaya Aura® Contact Center also provides routed contact support for email messages, Web communications, voice mail messages, scanned

Component	Version	Reference Configuration Characteristics
		documents, fax messages, SMS text messages, outbound, and Social Networking.
Avaya Aura® Media Server	7.8	Avaya Aura® Media Server is a software-based media processing platform for the Contact Center. Avaya Aura® Media Server provides voice contact routing and conferencing, announcements, and dialogs and Agent-Greeting capabilities in SIP-enabled contact centers.
Avaya Agent Desktop	7.0.3	Agent Desktop is a single-interface client application that contact center agents use to interact with customers. Agents use Agent Desktop to respond to customers through various media, such as phone, email, Web communication, fax messages, voice mail messages, scanned documents, SMS text messages, and instant messages.
Avaya Aura® Unified Communications platform	7.0.x, 7.1.x, 8.0	Avaya Aura® Unified Communications platform is an enterprise grade Private Automatic Branch Exchange (PABX).

Table 2: Avaya Aura® Unified Communications platform components

Component	Version	Reference Configuration Characteristics
Avaya Aura® Communication Manager	7.0.x, 7.1.x, 8.0	Avaya Aura® Communication Manager delivers centralized call control for resilient and distributed networks. Communication Manager supports a wide range of servers, gateways, analog, digital, and IP-based communication devices. Communication Manager has advanced built-in capabilities including mobility applications, call center features, and conference calling.
Avaya Aura® System Manager	7.0.x, 7.1.x, 8.0	Avaya Aura® System Manager delivers a set of shared, secure management services, and a common console across multiple products. Use System Manager to manage and configure the routing policies for the Session Manager in your solution. System Manager communicates with Session Manager using secure links.
Avaya Aura® Session Manager	7.0.x, 7.1.x, 8.0	Avaya Aura® Session Manager is a SIP routing and integration tool. Session Manager integrates all SIP entities across the entire enterprise network within a company. Session Manager

Component	Version	Reference Configuration Characteristics
		offers a core communication service that builds on existing equipment but adds a SIP-based architecture. Session Manager connects to and acts as a system-wide dial plan for Communication Manager using direct SIP connections.
Avaya Aura® Application Enablement Services (AES)	7.0.x, 7.1.x, 8.0	Avaya Aura® Application Enablement Services provides a set of enhanced telephony APIs, protocols, and Web services. These APIs support access to the call processing, media, and administrative features available in Communication Manager. Use these APIs for off-the-shelf and custom integration with communications and business applications. These APIs also provide integration with a broad range of contact centers, Call Recording, and Click-to-Dial applications.

The following Avaya Aura® Contact Center components are part of the initial installation:

Table 3: Avaya Aura® Contact Center components

Component	Version	Reference Configuration Characteristics
Contact Center Manager Server (CCMS)	7.0.3	CCMS is a core Contact Center component that provides the intelligent routing capability for voice and multimedia contacts to the most qualified agent. The most qualified agent is the agent with the appropriate skills and abilities to handle the type of contact. Rules for contact treatment (what happens while the customer waits for a response) and routing (the contact response) can be simple or complex.
Contact Center Manager Administration (CCMA)	7.0.3	CCMA is a browser-based tool for contact center administrators and supervisors to manipulate the data and reporting for the CCMS database. You can use CCMA to configure contact center resources, contact flows, components, and activities. You can also use CCMA to define access levels to data and provide dynamic reporting to fit your enterprise business needs.
Communication Control Toolkit (CCT)	7.0.3	CCT is a client/server application that helps you implement Computer Telephony Integration for installed and browser-based client integrations. In SIP-enabled contact centers, CCT integrates the Contact Center users within the SIP environment to offer features that enrich the customer experience.

Component	Version	Reference Configuration Characteristics
Contact Center Multimedia (CCMM)	7.0.3	CCMM provides support for inbound multimedia contacts. All multimedia contact types are subject to Contact Center routing and prioritization. Administrators can create specific treatments through applications developed in Orchestration Designer. Administrators and supervisors can review a full range of historical reports and real-time displays to track volume and completion statistics.
Orchestration Designer (OD)	7.0.3	OD is a graphical workflow application that you can use to program Avaya Aura® Contact Center applications. OD provides a graphical editor to create Contact Center Task Flow Executor (TFE) flows.
Contact Center License Manager (LM)	7.0.3	LM provides centralized licensing and control of all Contact Center suite components and features across the Contact Center suite.
Contact Center Manager Server Utility (SU)	7.0.3	SU monitors and maintains Contact Center Manager Server activity.

Offsite Agent Overview

The Offsite Agent feature works on the Avaya Aura® Unified Communication platform and requires Communication Manager Telecommuter mode. Offsite Agent extends a Contact Center to an agent's preferred environment, allowing them to handle skillset calls regardless of location. The Offsite Agent feature connects contact center calls to the agent's telephone (home telephone or mobile), without the agent needing special hardware.

For many contact centers, providing the ability for agents to be offsite gives a range of advantages. It can:

- increase employee satisfaction, by offering flexible working hours and zero travel time
- help retain highly skilled employees
- reduce the overhead of having agents working onsite, for example reduction in real estate costs
- improve management of staffing levels at peak times, since offsite agents provide the ability to quickly bring agents online
- improve management of staffing levels during a pandemic, since agents can work from home

In all these situations, the ability for agents to work from home without specialized equipment, and with a small amount of additional training and orientation, provides an improved service to the customer and a clear business advantage. Agents simply log in to the contact center using a smart client application on their home PC or their laptop. They receive skillset calls on PSTN home or mobile phones.

The Offsite Agent feature allows agents to appear as local to the contact center, thus functionality such as availability in Contact Center Manager Server skillsets, visibility in contact center reports, and contact recording all function in the regular manner.

A broadband connection to the contact center is usually required, but because calls are routed to a PSTN phone, this does not need to provide voice-quality data streams.

Avaya recommends that you create a specific Return to Queue Call Presentation Class (CPC) for offsite agents. This CPC must provide sufficient time for a call to route through the public telephone network and be answered by an agent on their home telephone. Avaya recommends that you do not assign offsite agents to a Let Ring or Call Force Answer CPC.

Chapter 4: Solution specification

This section specifies the overall maximum capacities for an Avaya Aura® Contact Center and Avaya Aura® Unified Communications solution.

Maximum agent capacity and call rate values

The following table specifies the maximum capacity values supported by Contact Center.

The following conditions apply to the table:

- The capacities supported on a server are limited by the server platform. Use the server guidelines to determine the capacity of your server hardware.
- These values are supported by Contact Center. Capacity values are also limited by telephone switch capacity. To find the limits for your telephone switch, check your telephone switch documentation.

Table 4: Contact Center capacity figures in detail

Parameter	SIP maximum
Number of logged-on agents: Configurations with greater than 1500 agents require special consideration for contact center subnet bandwidth and disk requirements.	• Avaya Aura® Unified Communications platform based SIP: 3,000
Number of logged-on multimedia agents. (No voice agents on Contact Center in this configuration)	• Avaya Aura® Unified Communications platform based SIP: 3,000 • No switch configured - Multimedia only: 3,000
Number of agents defined in the system	10,000
Number of phones:	N/A
Number of supervisors logged on	600
Number of supervisors defined in the system The number of configured supervisors defined in the system is not limited, but Avaya tests only up to 600 configured supervisors.	600
Number of scripts The number of scripts defined in the system is not limited, but Avaya tests only up to 1500 scripts.	1,500
Number of active scripts The product contains three predefined scripts. Therefore, you can create 997 scripts.	1,000 (997)
Maximum script size—Master_Script (characters)	100,000
Maximum script size—other scripts (characters)	50,000
Number of applications (that is, exit points from the Master_Script) The product contains six predefined applications. You can create 1000 applications for the current release.	1,005 (1,000)
Number of user defined call variables	500

Parameter	SIP maximum
Maximum number of supported SIP Contact Intrinsics per contact	32 key-value pairs. Each key-value pair has a maximum *key* length of 25 characters and a maximum *value* length of 80 characters. Only ASCII key-value-pairs are supported.
Number of skillsets The maximum includes both local skillsets and network skillsets.	3,000
Number of skillset priority levels	48
Number of skillsets for each call	20
Number of activity codes The product contains five predefined activity codes. Therefore, you can create 4995 activity codes.	5,000 (4,995)
Inbound voice calls per hour The number of inbound calls per hour assumes a hold time of three minutes. For shorter call durations, higher call rates can be supported.	Avaya Aura® solution based SIP: 45 000
Stand-alone Multimedia server Inbound Multimedia contacts per hour (for stand-alone server)	12,000
Co-resident Multimedia server Inbound Multimedia contacts per hour	2,400
Stand-alone Multimedia server new contacts backlog	100,000 The Extended Email Capacity backlog is 100 000 contacts.
Co-resident Multimedia server new contacts backlog	4,000
Number of waiting contacts	3,000
Call resources parameters	
Number of IVR queues (Communication Server 1000)	N/A
Number of IVR ports	1,000
Number of ACCESS ports (Communication Server 1000)	N/A
Number of routes	513
Number of CDNs	5,000
Number of RAN and music routes	512
Number of DNISs	10,000
Web Communications	
Number of concurrent Web Communication sessions. Contact Center supports up to 500 concurrent Web Communication (Web chat) sessions between agents and customers with an average chat duration of 5	500

Parameter	SIP maximum
minutes. This can be configured as 500 individual agents each handling a single Web chat contact, or 100 agents handling five concurrent web chat sessions, or any multiplicity configuration not exceeding 500 concurrent chat sessions. For capacity requirements beyond 500 sessions, use Enterprise Web Chat (EWC).	
Number of assigned active agents per supervisor for observe and barge-in.	25
Number of Instant Messages (IMs) per hour	100 000 (If an average instant message contact in the contact center consists of the agent and customer exchanging 10 messages, the contact center supports 10 000 IM contacts per hour)
Number of presence changes per hour	200,000
Assignment parameters	
Number of agents in an agent-to-supervisor assignment (No CCT)	1,000
Number of agents in an agent-to-supervisor assignment (CCT enabled)	100
Matrix size for agent-to-skillset assignments This parameter is the supported matrix size for displaying agent-to-skillset assignments. An agent-to-skillset assignment contains a matrix with a row for each agent in the assignment, and a column for each skillset to which the agents belong. The matrix size is the number of agents multiplied by the number of skillsets. This parameter works in conjunction with the Number of agent-to-skillset reassignments in an agent-to-skillset assignment parameter. Even though this window allows a 5000 element matrix to be displayed, non-blank elements in the matrix must not exceed the parameter. Number of agent-to-skillset reassignments in an agent-to-skillset assignment (that is, the maximum number of agent-to-skillset reassignments in a single agent-to-skillset assignment is 1500).	5,000
Number of agent-skillset reassignments in an agent-to-skillset assignment In an agent-to-skillset assignment, you can change an agent's status for multiple skillsets. For example, you can put the agent James Jones on Standby for the skillset Bookings, and give him priority 1 for the skillset European Vacations. Thus, you have two reassignments for the agent James Jones in the agent-to-skillset assignment.	1,500

Parameter	SIP maximum
Networking parameters	
Number of call processing nodes in the network (including local node) The number of configured nodes is 30; however, only 20 nodes can be configured in the routing table.	30
Number of network skillsets The maximum includes the predefined skillsets, local skillsets, and network skillsets.	1,500
Number of skillsets per agent	150
Number of sites in the routing table for a network skillset	20
Number of network skillsets to which a call is queued	10
Number of agent reservation requests per call	30
Number of remote applications (applications accessible over the network)	6,000
Network calls per hour for which CBC data is collected	10,000
Number of target nodes	20
Database parameters	
Number of client PCs and RTI applications connected to the database	100
Number of other applications connected to the database	100
Number of Fault Management messages in database	7,500
Maximum number of report clauses The database server supports a maximum of 255 clauses on a single SQL statement.	255
Maximum number of contacts in the active Multimedia database (includes all contact types) You must purge the active Multimedia database regularly to archive closed contacts to the Multimedia Offline database. For more information about the Multimedia Archive Utility, see *Maintaining Avaya Aura® Contact Center*.	1,000,000
Maximum number of contacts in the Multimedia Offline database	The Multimedia Offline database does not have a maximum limit for the number of Multimedia contacts. The maximum size depends on the available disk space, contact attachment sizes, and attachment ratio. For more information about disk storage requirements, see Contact Center Multimedia disk storage requirements on page 43.
Maximum number of multimedia contacts per customer	1,000
Third-party interface parameters	

Parameter	SIP maximum
Number of MLS applications	N/A
Number of MLS DN registrations across all MLS applications	N/A
Number of MLS calls per hour The number of MLS calls per hour at 58,000 and 68,000 assumes a hold time of three minutes. For shorter call durations, higher call rates can be supported.	N/A
Number of HDX connections When configured, Database Integration Wizard (DIW) uses a single HDX connection.	10
Number of RTI client systems/applications	100
Other parameters	
Number of scripts activated under load Script activation supports activation cascading, where the activation of a parent script forces activation of all lower level scripts. Do not use this feature on a system under load. Under load, activate scripts from the lowest level up, with the Master script activated last.	1
Steady state CPU	70%
Number of CCMS servers per Avaya Communication Server 1000	3 (Only to support phased migration between Contact Center releases)
Number of AML-based application servers per Avaya Communication Server 1000	N/A
Number of Avaya Aura® Contact Center (AACC) instances per Avaya Aura® Unified Communications (UC) platform. **Note:** The overall capacity of the combined AACC servers connected to a single UC platform must not exceed the maximum specified capacity of a single AACC instance connected to that UC platform. Where multiple AACC servers share a UC platform, AACC High Availability and or UC High Availability are not supported.	3
Number of Phonebook entries on Avaya Agent Desktop	10,000

Orchestration Designer application Variables and Intrinsics

Avaya Aura® Contact Center Orchestration Designer (OD) applications support the following variables and intrinsics for voice contacts.

Type	Description	SIP	Access	Maximum
Global variable	Global variables are constants that you can use in all OD applications. For example, the global variable holidays_gv stores information about the dates when your contact center is closed. You can use the OD Application Variables manager to add an extra date to the holidays_gv global variable. This extra date is then automatically used by all OD applications using that global variable. Some examples of default global variables: holidays_gv, business_hours_gv, primary_Skillset_gv.	Yes	OD applications have read-only access to global variables.	N/A
User defined call variable	Call variables have a value that can change for each contact. These variables follow the contact through the system and pass from one OD application to another with the contact. Call variables have values defined on a call-by-call basis. An example of a call variable is a customer account number collected through a voice processing session, as this changes for each caller referenced by the OD application.	Yes	OD applications have read and write access to call variables.	500
System intrinsic	System intrinsics contain system-wide information about skillsets, time, traffic, and voice contacts. Avaya Aura® Contact Center (AACC) automatically creates and maintains system intrinsic. Intrinsics are available only to query data about the system within OD applications, not to modify data. Some examples of system intrinsics: Call intrinsic – CDN, Skillset intrinsic - POSITION IN QUEUE, Traffic intrinsic - TOTAL ACTIVE CALLS.	Yes	OD applications have read-only access to System intrinsics.	N/A — Existing defined intrinsics
SIP contact intrinsic	In a SIP-enabled Avaya Aura® Contact Center, Contact Intrinsic data makes it easy to develop screen pops, reducing the time, effort and cost required to launch new capabilities. In a SIP-enabled contact center solution, each contact has associated SIP Contact Intrinsic data. This Contact Intrinsic data might contain data relevant to that call, the calling customer, and other information retrieved by self-service or third party applications.	Yes	OD applications have read and write access to SIP Contact Intrinsics.	32

Email limits and capacity values

The following table specifies the maximum email and mailbox capacity values supported by Contact Center.

Table 5: Contact Center email and mailbox capacity figures

Parameter	Maximum
Email servers	
POP3 or IMAP servers	5
SMTP servers	5
Mailboxes	
Maximum number of Mailboxes which can be configured	3000
Maximum number of fax mailboxes which can be configured	50
Maximum number of voice mail mailboxes which can be configured	50
Maximum number of SMS mailboxes which can be configured	50
Maximum number of Scanned Document mailboxes which can be configured	50
Email field limits	
Maximum length of **To:** field	4096 CCMM supports a maximum of 4096 characters in the To: address field. If an email exceeds this limit, CCMM does not process the email and does not create a contact.
Rule Groups	
Maximum number of Rule Groups	3000
Maximum number of Rules in a Rule Group	50
Rules	
Maximum number of Rules	10 000
Maximum number of Auto-Suggests assigned	5
Maximum number of Search Criteria	5
Prepared Responses	
Maximum number of Prepared Responses	5000
Maximum number of Response Categories	50
Maximum number of Prepared Responses Assigned to a Rule	5
Sender Groups	
Maximum number of Sender Groups	100

Parameter	Maximum
Email servers	
Maximum number of addresses per Sender Group	50
Keyword Groups	
Maximum number of Keyword Groups	3000
Maximum number of Keywords per Keyword Group	50
Barred Outgoing Addresses	50

Contact Center Multimedia disk storage requirements

This section describes the database files used by Contact Center Multimedia and provides database capacity calculations for a stand-alone Contact Center Multimedia server.

Important:

The total disk space usage on the Contact Center Multimedia database volume must not exceed 90% of the volume space. If this happens, expand the disk space on the server and extend the Multimedia database volume.

Required database files

When you install the Contact Center Multimedia server component, you install the following files required to operate the database:

- CACHE.DAT in the `Avaya\Contact Center\Databases\CCMM\MULTIMEDIA\DATA` folder. This stores the active Multimedia data.
- CACHE.DAT in the `Avaya\Contact Center\Databases\CCMM\MULTIMEDIA\OFFLINE` folder. This stores the offline Multimedia data.
- Cache Journal in the `Avaya\Contact Center\Databases\Journal` folder.
- `Avaya\Contact Center\Journal` folder is created during installation. This folder contains the Database Journal Files, which are used for High Availability.

During the installation you can select the drive letter that these folders or files are created on. The folder information is fixed.

The CACHE.DAT files grow dynamically as the volume of data in the databases grows. Initially they are just under 45 MB. One million contacts takes approximately 20 GB of space. The OFFLINE database must not exceed 70% of the total disk space on the Multimedia database volume: if this happens, expand the disk space on the server and extend the Multimedia database volume.

The Journal files are deleted after seven days. Therefore, the maximum size of this folder is determined by the number of contacts that arrive in a seven-day period. The space taken is in proportion with the one million available contacts in 20 GB space.

Email attachment storage

Attachments for new email contacts are stored in the attachment folder. When the CCMM Offline Synch task runs, it copies each attachment into the OFFLINE database. CCMM stores two copies of each attachment, one on disk and one in the OFFLINE database, until a scheduled cleanup task clears the contact from the MULTIMEDIA database. The maximum additional disk space required to store attachments is calculated as:

Disk space for email attachments in MB

= number of email messages per day

* percent with attachment

* average attachment size in MB

* 2

Example

The following is the additional disk storage calculation for a contact center that receives 9000 email messages every day, where 30 percent of the email messages have an attachment averaging 0.5 MB in size. Contacts stay in the MULTIMEDIA database 10 days before a scheduled cleanup task clears them from the MULTIMEDIA database.

Disk space for email attachments in MB:

= 9 000 * 0.3 * 0.5 * 10 * 2

= 27000 MB

Outbound capacity

Contact Center Outbound components have the following capacity:

- Outbound Campaign Management Tool monitors a maximum of 100 simultaneous outbound campaigns, with a maximum of 20 000 contacts per campaign.
- The contact rate for outbound contacts is a subset of the total multimedia contact rate. For example, if a system has a maximum capacity of 1200 multimedia contacts per hour, and is processing 400 outbound contacts per hour, it can process a maximum of 800 other multimedia contact types per hour.
- InterSystems Caché database server, and its associated Web services, store information for 1 000 000 contacts in a database that is saved on a 20 GB disk.

- Open queue can queue up to 20 000 contacts at one time for routing and reporting. Contact Center Manager Server processes Open Queue contacts at a rate of 20 contacts per second. This ensures Contact Center Manager Server does not get overloaded.

Chapter 5: SIP Contact Center configuration requirements

This section describes the configuration requirements for a SIP-enabled Avaya Aura® Contact Center.

General requirements

This section describes the general requirements for a SIP-enabled contact center.

SIP-enabled Contact Center feature limitations

SIP-enabled Avaya Aura® Contact Center has the following limitations:

- In a SIP-enabled Contact Center using a Communication Manager, Avaya Aura® Contact Center supports a limited configuration of the Communication Manager - Coverage Path feature. For more information, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- In a SIP-enabled Contact Center, blind (single-step) transfers are not supported. However, early transfer completion is supported. Early transfer completion is the ability to complete a supervised (two-step) transfer while the far end is still ringing. In a SIP-enabled Contact Center, references to blind transfer mean supervised transfer with early transfer completion.
- Trunk information in Historical Reports is not supported.
- Host Enhanced Routing is not supported.
- Call Force Delay for Instant Message (IM) contacts is not supported.
- The Instant Messaging CDN alias and number must be configured the same.
- Walk-away is not supported.
- Agents must not use their desk phone or Agent Desktop to phone, transfer a call, or conference a call to a phone number that is:
  - routed to a CDN (Route Point). For example, a Virtual Directory Number (VDN) routed to a CDN (Route Point).
  - converted to a CDN (Route Point). For example when using digit manipulation on the call server.

- call forwarded to a CDN (Route Point).

Agents can use their desk phone or Agent Desktop to transfer a call, conference or phone directly to a CDN (Route Point). Agents can dial directly to a CDN (Route Point). Agents can transfer a call directly to a CDN (Route Point). Agents can conference a call directly with a CDN (Route Point).

Dependent platform and switch compatibility

The following table displays the SIP-enabled platforms available and the release compatibility.

Table 6: SIP-enabled switch compatibility

Platform	Release
Avaya Aura® Unified Communications platform	7.0.x, 7.1.x, 8.0

Upgrade path

Avaya supports migrations from CS1000 AML-based (non-SIP) Contact Center products to SIP-enabled Avaya Aura® Contact Center on an Avaya Aura® Unified Communications platform.

Avaya does not support migrations from SIP-enabled Contact Center products on a CS1000 platform to SIP-enabled Avaya Aura® Contact Center on an Avaya Aura® Unified Communications platform.

SIP session expiry parameters

SIP session timer, a keep alive mechanism for SIP sessions, is an extension to the SIP RFC that allows the setting of SIP session refresh parameters. Refreshing allows both the SIP User Agent (UA) and SIP Proxy to determine if the SIP session is still active. The absence of session expiry parameters in the SIP INVITE can result in speech path issues. In some cases the SIP session and the corresponding call can be prematurely terminated when the UA or the Proxy refreshes the session. Contact Center requires that the incoming SIP INVITE contains session expiry parameters.

Digital Signal Processing Considerations

This section introduces Digital Signal Processing (DSP) in a SIP-enabled contact center.

- Voice over Internet Protocol on page 48
- PABX Digital Signal Processors on page 49

- Avaya Aura® Shuffling on page 50
- PABX DSP consumption examples on page 50
- Avaya Aura® Unified Communications platform DSP on page 51

Voice over Internet Protocol

Voice over Internet Protocol (VoIP) is an internet technology and communications protocol that delivers voice and multimedia communications over IP networks. Voice over IP is widely used as a flexible and cost-effective alternative to the Public Switched Telephone Network (PSTN).

- Signaling—Voice over IP is used by industry standard protocols and proprietary Avaya signaling protocols. Avaya Aura® Contact Center uses industry standard signaling protocols such as SIP and H.323.
- Media—VoIP supports many media variants such as audio, video, and Instant Messaging. Communication systems use codecs to encode media streams for transmission and to decode the media for playback. Codecs encode and decode media such as VoIP audio (G. 711, G.729, and G.726).

Communication endpoints must each use a common VoIP signaling protocol and media codec in order to communicate with each other. Communication endpoints that do not share common signaling and media protocols must transverse a gateway that performs the translation to both signaling and media.

Example 1:

Communication systems that use both H.323 and SIP endpoints:

- Signaling: the gateway translates from H.323 to SIP.
- Media: H.323 and SIP endpoints commonly share G.711 codecs – transcoding is not required so no Digital Signal Processors (DSPs) are used.

Example 2:

Communication systems that use both Integrated Services Digital Network (ISDN) and SIP endpoints:

- Signaling: the gateway translates from ISDN D-Channel signaling to SIP signaling and vice versa.
- Media: a DSP is required to transcode ISDN Pulse-code modulation (PCM) audio into G.711 audio for SIP communications.

Avaya Aura® Contact Center uses SIP signaling. Contact Center uses Avaya Aura® Media Server to handle the VoIP audio media. Avaya Aura® Contact Center uses the Avaya Aura® Media Server software DSP capabilities to handle VoIP media on its behalf. Contact Center communicates with the Avaya Aura® Media Server using SIP. Avaya Aura® Media Server communicates with the PABX using SIP signaling and media. Calls enter Avaya Aura® Contact Center through SIP signaling. Agents are joined to customers using SIP. Avaya Aura® Media Server provides conference facilities, telephony ringback and busy tones, music playing for scripted music and IVR capability (play & collect digits).

When a customer phones a contact center, their (VoIP audio media) call is initially terminated on an Avaya Aura® Media Server conference port, on a dedicated customer conference bridge.

A Contact Center Task Flow Executor (TFE) script application uses the Avaya Aura® Media Server to insert call treatments such as ringback into the conference bridge for the customer to hear. Customers are normally connected to an appropriate agent using this same conference bridge and the call ends up as a simple two-party conference on Avaya Aura® Media Server. Contact Center TFE typically instructs Avaya Aura® Media Server to play a few seconds of ringback tones into the conference bridge the customer is anchored on, so the customer can hear their phone call progress. The Task Flow Executor (TFE) can then instruct Avaya Aura® Media Server to play a welcome greeting to the customer. In Interactive Voice Response (IVR) solutions, Avaya Aura® Media Server can use a play and collect application to play a message asking the customer to enter digits from their phone set. Avaya Aura® Media Server then collects these digits.

Once a Contact Center agent is identified, they are called up by Avaya Aura® Contact Center to join the same Avaya Aura® Media Server conference as the caller, thereby creating a simple two-party conference.

Avaya Aura® Contact Center supports TDM and VoIP voice communication device protocols.

- TDM—The Time Division Multiplex (TDM) protocol is used by Plain Old Telephone sets (POTS), PSTN, ISDN, ATM, and others.
- VoIP—Avaya Aura® Contact Center supports VoIP for H.323 and SIP. The VoIP protocol is used by Skype, Avaya 9641 deskphone, and others.

PABX Digital Signal Processors

Digital Signal Processors (DSPs) can be used to transcode or convert media from one protocol to another. Transcoding is the direct digital-to-digital conversion from one encoding type to another.

A Digital Signal Processor is consumed each time a TDM user and an IP agent are connected. A DSP is consumed each time a TDM PSTN user call is connected to an agents' IP deskphone. A DSP is also consumed each time an agent with an IP deskphone calls a TDM-based user or customer. In a SIP-enabled contact center each TDM endpoint consumes a DSP. Local IP endpoints do not consume a DSP.

The Avaya Aura® G450 Media Gateway Chassis has DSP daughter boards (MP-20 and MP-80) for transcoding media from one protocol to another.

You must engineer your Avaya Aura® Unified Communications platform PABX with a sufficient number of Digital Signal Processor channels to handle the TDM and VoIP transcoding in your contact center solution.

Each contact center is different – the number of agents, the number of supported simultaneous customer calls supported, the blend of TDM and VoIP traffic, and customer expectations determine the number of DSPs required. It is important that there are sufficient DSPs to support the intended Avaya Aura® Contact Center deployment. Avaya recommends that you engineer the DSP quantities to minimize call blocking scenarios.

If your solution uses Avaya Aura® Unified Communications platform 7.0 or later, you can use Avaya Aura® Media Server as a DSP resource for Avaya Aura® Communication Manager as an alternative to using the G450 Media Gateway.

Avaya Aura® Shuffling

If you are using an Avaya Aura® Unified Communications PABX, enable the Shuffling feature to avoid unnecessary DSP usage. Avaya Aura® Shuffling (Direct IP-IP Audio Connections) attempts to renegotiate the media on an established SIP call, to update the anchor point of the media processor, thereby reducing the total number of Digital Signal Processor (DSP) channels required.

On your Communication Manager, configure “Direct IP-IP Audio Connections? y” on every agent station, and on the SIP Signaling group configuration screens.

Important:

Avaya Aura® Communication Manager consumes DSPs if shuffling is turned off on either the SIP Signaling groups, or any of the agent IP stations. Enable shuffling on all agent stations (phones) and on the SIP signaling group.

PABX DSP consumption examples

The following examples examine a variety of contact center solutions, and show how to calculate the number of Digital Signal Processor (DSP) channels required for that solution type.

- Each TDM customer consumes one DSP. Customer calls typically enter Avaya Aura® Communication Manager on the TDM side of the PABX. These calls require transcoding from TDM to VoIP for Avaya Aura® Media Server and Avaya Aura® Contact Center. For example, if you have 10 TDM calls waiting, and 5 TDM calls answered by agents with IP desk phones, your PABX is consuming 15 PABX DSP channels.
- Each TDM agent consumes one DSP channel while on a Contact Center call. Customer calls can enter Communication Manager on the VoIP side of the switch. If your contact center uses TDM agents then these calls require transcoding from VoIP to TDM for the TDM agents. For example, if you have 10 TDM calls waiting, 5 TDM calls answered by 2 TDM agents, and 3 IP Agents, your solution is consuming 10+5+2=17 DSP channels.
- If a customer call arrives into an enterprise through SIP, and is finally transferred to a TDM user, for example using ISDN, then Avaya Aura® Communication Manager consumes one DSP channel to tandem this call from VoIP to TDM.
- If a customer call arrives into an enterprise using TDM (PSTN - ISDN), and is finally transferred to a TDM user, for example using ISDN, Avaya Aura® Communication Manager normally optimizes the call so the call no longer tandems though DSPs, and all DSP resources are released.
- If a customer call originates on a SIP carrier, the call enters the contact center through the SIP voice proxy. Avaya Aura® Contact Center supports Session Manager as a SIP voice proxy. The SIP proxy routes the call directly to Avaya Aura® Contact Center which anchors

the call on an Avaya Aura® Media Server. VoIP agents handle this call. There is no DSP requirement for this call scenario.

These are some examples of calculating the number of Digital Signal Processor (DSP) channels required for your solution type. For more details, see your PABX documentation.

Avaya Aura® Unified Communications platform DSP

Engineer the Avaya Aura® Unified Communications platform and G450 Media Gateway so they are capable of supporting SIP, in particular engineer the DSP hardware resources to support TDM and IP transcoding. Incoming PSTN calls require one DSP per call. Agents with TDM phones each require another DSP. For more information, see *Administration for the Avaya G450 Media Gateway*.

If your solution uses Avaya Aura® Unified Communications platform 7.0 or later, you can use Avaya Aura® Media Server as a DSP resource for Avaya Aura® Communication Manager as an alternative to using the G450 Media Gateway.

Dialed Number Identification Service

A Dialed Number Identification Service (DNIS) is a method by which the Contact Center system recognizes the phone number that a caller dials. Agents can receive contacts from customers calling in on different DNISs and customize their response according to the DNIS. Based on the DNIS, the system can direct contacts to a controlled CDN and supply different treatments.

DNIS Options in SIP-enabled contact centers

Session Manager supports DNIS information for Contact Center using the To header technique.

- Incoming SIP Invite message with DNIS information in the To header on page 52
- Session Manager systems on page 52

Session Manager supports DNIS information for Contact Center using the Virtual Directory Number “DNIS” prefix technique.

- Incoming SIP Invite message with DNIS information in the History-Info header on page 52
- Session Manager systems on page 52

Incoming SIP Invite message with DNIS information in the To header

If the incoming SIP Invite message to Avaya Aura® Contact Center contains a REQUEST URI that differs to the To address URI, Contact Center deems the To address to contain the DNIS information of the call.

Session Manager supports DNIS information for Contact Center using this To header technique.

Incoming SIP Invite message with DNIS information in the History-Info header

If the SIP REQUEST URI message username and the To address URI username are the same, then Avaya Aura® Contact Center looks for DNIS information in the SIP “History-Info” message headers. The only way Contact Center can identify valid DNIS information in the “History-Info” header is if one of the “History-Info” headers contains the case sensitive keyword “DNIS”.

Session Manager systems

In solutions that use a Communication Manager and a Session Manager, the DNIS information can be provided in the SIP ‘To’ header of the incoming SIP Invite message by configuring an adaptation on the Session Manager.

If necessary, DNIS information can also be provided in the History-Info header using the Virtual Directory Number “DNIS” prefix naming convention. On the Communication Manager create a Virtual Directory Number (VDN) for each DNIS required. The VDN name must contain the capitalized keyword “DNIS”.

Chapter 6: Licensing

This section describes how to obtain a license for your solution.

How to obtain a license for a nodal SIP-enabled solution

In an Avaya Aura® Unified Communications platform SIP-enabled environment, Avaya Aura® Contact Center can use an Avaya WebLM license file or a remote Avaya WebLM server to provide nodal licensing control.

The following diagram shows the licensing options for SIP-enabled Avaya Aura® Contact Center:

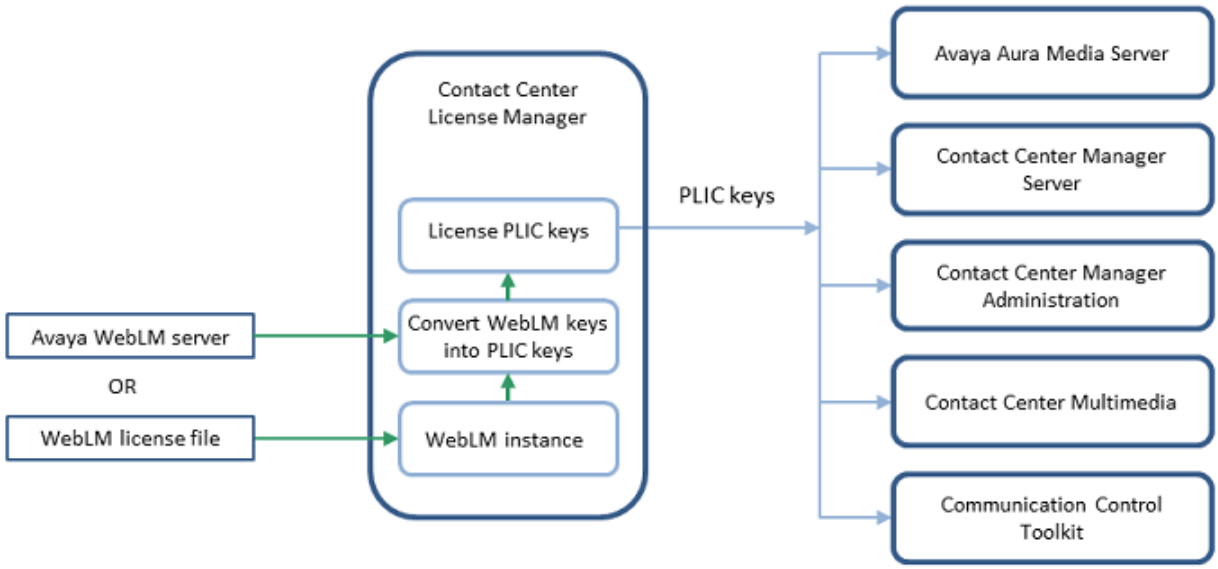


Figure 4: Licensing options for SIP-enabled Contact Center

Depending on the order tool path you used, you have the following options:

1. Obtain the Avaya WebLM host ID of the Contact Center License Manager WebLM instance.
2. Use the Avaya WebLM host ID to obtain a nodal Avaya WebLM license file from the Avaya Product Licensing and Delivery System (PLDS).

3. Load the Avaya WebLM license file into Contact Center License Manager and use it to enable Contact Center licensed features. When Contact Center License Manager loads the license, if the Avaya WebLM host ID is incorrect, then License Manager shuts down and Avaya Aura® Contact Center cannot process contacts. If the Avaya WebLM host ID is correct, then License Manager provides license keys, and Avaya Aura® Contact Center processes customer contacts.

OR

1. When using the Virtualized Environment deployment of Avaya WebLM server, obtain the Avaya WebLM host ID from the WebLM user interface.
2. Use the WebLM host ID to obtain WebLM license keys from the Avaya Product Licensing and Delivery System (PLDS).
3. Enter these license keys on the remote Avaya WebLM server. Contact Center License Manager connects to the remote WebLM server and uses the Contact Center-specific license keys from it to control Contact Center licensed features. If Avaya Aura® Contact Center is using a remote Avaya WebLM server, Avaya Aura® Contact Center does not import the license file to a Contact Center server; WebLM stores the license file on the Avaya WebLM server.

You can use the License Manager Configuration Utility to check which Avaya Aura® Contact Center features are licensed and how many agent licenses are available.

Chapter 7: Avaya Aura® Experience Portal Integration

Avaya Aura® Experience Portal is an open standards-based self-service software platform which offers industry leading reliability and scalability to help reduce costs and simplify operations.

Avaya Aura® Experience Portal software is deployed on standard Linux servers and it supports integration with SIP-enabled systems, including Avaya Aura® Communication Manager and Avaya Aura® Contact Center.

The Avaya Aura® Experience Portal system consists of an Experience Portal Manager (EPM), which controls the Experience Portal system and Media Processing Platform (MPP) servers, which process all calls. The Experience Portal system typically includes an Automatic Speech Recognition (ASR) server, Text-to-Speech (TTS) speech servers, and application servers.

Avaya Aura® Contact Center supports the following types of integration with Avaya Aura® Experience Portal:

- Front-end Avaya Aura® Experience Portal with SIP-enabled Contact Center
- Back-end Avaya Aura® Experience Portal with SIP-enabled Contact Center using SIP header information
- Back-end Avaya Aura® Experience Portal with SIP-enabled Contact Center using Context Creation
- Front-end Avaya Aura® Experience Portal with Contact Center - Web Service Open Interfaces

In a front-end Avaya Aura® Experience Portal integration, the customer call is processed first by Avaya Aura® Experience Portal and then by Avaya Aura® Contact Center. In a back-end Avaya Aura® Experience Portal integration, the customer call is processed first by Avaya Aura® Contact Center and then by Avaya Aura® Experience Portal. Avaya Aura® Contact Center supports front-end and back-end Avaya Aura® Experience Portal integration in a single solution.

The following mechanisms support transferring calls and call data between Avaya Aura® Experience Portal and Contact Center:

- Landing Pads. Contact Center Web Service Open Interfaces enable self-service systems to transfer a call into Avaya Aura® Contact Center by reserving a Landing Pad. Contact Center Web Service Open Interfaces allow custom data to be passed with the call. To enable Contact Center Landing Pads you must configure Contact Center Web Service Open Interfaces.
- SIP header information. SIP includes a number of message headers in each SIP message. These headers contain information that enables the receiver to understand and use the message properly. In a contact center solution, SIP headers can be used to transfer small

amounts of call-related information between SIP-enabled applications. Avaya Aura® Contact Center supports the User-to-User Information (UUI) SIP header and the Avaya custom P-Intrinsics SIP private header. Avaya Aura® Contact Center Web Service Open Interfaces do not support SIP headers.

- SIP INFO message body using Context Creation: If your call-related context information does not fit in a SIP User-to-User Information (UUI) header or in the larger P-Intrinsics header, you can use the sample Context Creation application to pass more context information from Avaya Aura® Experience Portal to Avaya Aura® Contact Center. This sample Context Creation application can return multiple values from Avaya Aura® Experience Portal, rather than the single value returned by the sample Play and Collect application. The Context Creation sample application can return call-related context information in a SIP INFO message body. A SIP INFO message body holds and transfers much more information than a SIP header.

In an Avaya Aura® Unified Communications platform based solution, Avaya Aura® Contact Center supports the following methods of integration with Avaya Aura® Experience Portal:

- Landing Pads
- SIP header information
- SIP INFO message using Context Creation

Data transfer methods

The following table shows the maximum amount of data supported by each transfer type:

Transfer method	CS 1000 AML-based Contact Center	Avaya Aura SIP-enabled Contact Center
Landing Pads	Maximum Call Attached Data is 4096 bytes. Maximum 5 ASCII key-value pairs of Contact Intrinsics.	Maximum Call Attached Data is 4096 bytes. Maximum 5 ASCII key-value pairs of Contact Intrinsics.
UUI SIP header using ASAI	N/A	96 bytes maximum.
P-Intrinsics SIP header	N/A	Depends on your solution. Note 1
SIP INFO message body using Context Creation	N/A	8K bytes total maximum: • Maximum of 10 ASCII key-value pairs. • And 4729 characters of Call Attached Data (CAD) within the CC application.

Note 1 The following limitations apply to P-Intrinsics SIP header information:

- The amount of P-Intrinsics information associated with a call depends on the other SIP headers in the call and on the call flow path. Typically, Contact Center supports up to 10 ASCII key-value pairs of P-Intrinsics.

Transfer method	CS 1000 AML-based Contact Center	Avaya Aura SIP-enabled Contact Center
• If your solution has an Avaya Aura® Communication Manager in the incoming call path, the Refer-To header for blind transfers is limited to 1500 bytes overall.		

Contact Center supports ASCII key-value pairs with a key name of up to 25 characters and a value size of up to 80 characters.

Avaya Aura® Experience Portal Orchestration Designer

Avaya Aura® Experience Portal Orchestration Designer is an Eclipse-based application development environment which supports the development of Voice XML and CCXML speech applications. Orchestration Designer generates Avaya Aura® Experience Portal compliant XML-based applications which are deployed on software application servers such as Apache Tomcat Server in a self-service solution.

Voice XML

Voice XML (VXML) is a standard XML format for specifying interactive voice dialogs between a human and a computer. Voice XML is designed for creating audio dialogs that feature synthesized speech, digitized audio, recognition of spoken and DTMF key input, recording of spoken input, telephony, and mixed initiative conversations. A typical Voice XML play and collect application plays voice prompts to customers asking them to enter digits using their phone. The application then collects the customer digits and returns them for processing to the contact center.

Call Control XML

Call Control XML (CCXML) is a standard markup language for controlling how phone calls are placed, answered, transferred, conferenced, and more. CCXML works with Voice XML to provide an XML-based solution for any telephony application. Voice XML and CCXML are two separate languages and are not required in an implementation of either language. For example, CCXML can be integrated with a more traditional Interactive Voice Response (IVR) system and Voice XML dialog systems can be integrated with other call control systems.

SIP-enabled Avaya Aura® Contact Center

Avaya Aura® Contact Center uses Session Initiation Protocol (SIP) architecture to provide maximum interoperability and flexibility. SIP-enabled Avaya Aura® Contact Center simplifies solution architecture and CTI deployments. Avaya Aura® Contact Center SIP-enabled architecture

and Contact Intrinsic data make it easy to develop screen pop applications, reducing the time, effort, and cost required to launch new capabilities.

Contact Center Manager Server (CCMS) contains a SIP Gateway Manager (SGM) component which is the call processor in a SIP-enabled Contact Center. The SIP Gateway Manager is a standalone SIP element that can receive and process calls from SIP-enabled communication systems such as the Communication Manager platform.

Avaya Aura® Contact Center supports User-to-User Information (UUI) SIP header information and P-Intrinsic SIP header information. Contact Center uses the header information in each SIP call to generate call-related Contact Intrinsic information and Call Attached Data (CAD). This Contact Intrinsic data can contain information relevant to that call, the calling customer, and other information retrieved by self-service or third party applications. Contact Intrinsics are key-value pairs of relatively small amounts of data. Call Attached Data is a longer unstructured amount of data.

In a SIP-enabled contact center solution, the information stored in some SIP INFO messages can be used to transfer call-related information between SIP-enabled components. This call-related information enables the receiver to better understand and handle the call. If your call-related context information does not fit in a SIP User-to-User Information (UUI) header or in the larger P-Intrinsics header, you can use the sample Context Creation application to pass more context information from Avaya Aura® Experience Portal to Avaya Aura® Contact Center. The Context Creation sample application can inject multiple pieces of context information (Intrinsics and Call Attached Data) into Avaya Aura® Contact Center, where as the Play and Collect sample application can retrieve only a single piece of data, for example collected digits. The call-related context information is returned in a SIP INFO message body. A SIP INFO message body holds and transfers much more information than a SIP header.

Contact Intrinsic data enriches the context and information presented to agents with each customer contact. Contact Intrinsic data makes it easy to develop screen pops, reducing the time, effort and cost required to launch new capabilities. Avaya recommends that you use Contact Intrinsic data.

P-Intrinsic SIP Header

Avaya Aura® Contact Center supports the custom P-Intrinsics private header. The Session Initiation Protocol (SIP) includes a number of message headers in each SIP message. These headers contain information that enables the receiver to understand and use the message properly. In a contact center solution, you can use SIP headers to transfer small amounts of call-related information between SIP-enabled applications. The application receiving this SIP message reads these headers and performs some action based on the contents of the headers. SIP header information can provide additional data about a call that applications can use to process that call.

You can use P-Intrinsics header information to pass context information between SIP-enabled applications. Avaya Aura® Contact Center parses the P-Intrinsics SIP header information and uses it to create Contact Intrinsics or Call Attached Data. You can use P-Intrinsics in conjunction with User-to-User (UUI) information if backwards compatibility with existing applications is required.

SIP private headers (P-Headers) are purely informational. They do not create new commands and they do not interfere with the regular transmission of SIP messages. SIP private headers are used only to pass extra information that the receiving application can use. Avaya Aura® Contact Center supports the P-Intrinsics SIP header in incoming SIP INVITE messages.

Components that support this private header include front-end IVRs systems such as Avaya Aura® Experience Portal, SIP proxies such as Avaya Aura® Session Manager, or other SIP-enabled entities in the call flow.

P-Intrinsics information is not restricted by legacy limitations like UUI. P-Intrinsics information can grow in size, depending on other headers in the call, and on the call flow path. It can also be used to inject call attached data. It is therefore more flexible than UUI data. You can use both headers together, and customers can retain backwards compatibility with applications that already use UUI data.

Typical solution using P-Intrinsics

A front-end Avaya Aura® Experience Portal system uses XML speech applications and SIP header information to integrate with Avaya Aura® Contact Center. A self-service Voice XML speech application running on the Avaya Aura® Experience Portal – Application Server answers customer calls and gathers call-associated information based on customer's answers and inputs. Experience Portal then transfers the customer call, complete with this call-associated information stored in the P-Intrinsics SIP header, to Avaya Aura® Contact Center.

Contact Center uses the P-Intrinsics header to generate Contact Intrinsic and/or Call Attached Data specific to that call. If this call is ultimately answered by an agent, the agent can use the call-related Contact Intrinsic data to access customer details. The agents might receive the Contact Intrinsic data in a screen pop, or they might need to access these details manually using Avaya Agent Desktop.

P-Intrinsics reduce the amount of time the agents spend on each call, improve the customer experience, and make Contact Center more efficient.

User-to-User Information

SIP-enabled systems can use User-to-User Information (UUI) to transmit small amounts of data between systems within SIP header messages.

Voice XML applications can use SIP header information to collect, store, and transport customer call-related information. Voice XML application can use customer interview data to modify the SIP header, and then pass the customer call along with updated header data to the next application in the solution. Voice XML applications can also use SIP header information to make processing decisions about a customer call. Examples of SIP header UUI data include a customer account number obtained during a self-service customer interview.

Avaya Agent Desktop and Avaya Aura® Contact Center Orchestration Designer can also modify User-to-User Information.

This SIP header UUI data can be used to support Avaya Aura® Application Sequencing.

Universal Call Identifier

Universal Call Identifier (UCID) is an Avaya proprietary call identifier used to help correlate call records between different systems. Universal Call Identifier information, where enabled, is added to the User-to-User Information (UUI) data in SIP calls.

This identifier can be generated by the Avaya Aura® Experience Portal MPP server. Universal Call Identifier can be passed to Avaya Aura® Experience Portal through an application's SIP headers. Avaya Aura® Experience Portal can receive UCID from Avaya Aura® Communication Manager.

Avaya Aura® Contact Center Web Service Open Interfaces

Avaya Aura® Contact Center provides open standards-based Web services to support maximum interoperability and flexibility.

Web Services Open Interfaces

Avaya Aura® Contact Center Web Service Open Interfaces simplify the integration between the Contact Center and self-service systems allowing enterprises to quickly and easily adapt to changes.

Avaya Aura® Contact Center Web Services are a series of licensed SOAP-based open interfaces available to applications based on Service-Oriented Architecture (SOA).

The Web Service Open Interfaces enable self-service systems and third-party applications to transfer a call into the Contact Center by reserving a Landing Pad on the target Contact Center; it also allows custom data to be passed with the call. When the Landing Pad is reserved, the call must be transferred to Contact Center within 20 seconds. If not, the Landing Pad is unreserved and the call fails, giving a fast busy tone. Avaya recommends that you put the Landing Pad reservation code just before the transfer in the Voice XML application code.

Avaya recommends that you configure multiple Landing Pads in each Contact Center to ensure proper capacity and scalability.

Front-end Avaya Aura® Experience Portal self-service using Contact Center Web Service Open Interfaces

This section describes a front-end Avaya Aura® Experience Portal self-service integration using Avaya Aura® Contact Center - Web Service Open Interfaces. Integrating Avaya Aura® Experience

Portal with Avaya Aura® Contact Center - Web Service Open Interfaces is supported with the following platforms:

- SIP-enabled Avaya Aura® Unified Communications platform
- AML-based Avaya Communication Server 1000 solutions

Application Module Link (AML) is an internal protocol used by Avaya Aura® Contact Center to communicate directly with Avaya Communication Server 1000.

A combined Avaya Aura® Experience Portal self-service system and Avaya Aura® Contact Center solution gives your customers exceptional service and improved efficiency. Front-end self-service automation reduces contact center operating costs and improves Customer Satisfaction (CSAT).

Avaya Aura® Experience Portal uses XML voice applications to integrate with Avaya Aura® Contact Center open standard Web services. The Avaya Aura® Contact Center open standard Web services are supported in AML-based and SIP-enabled contact centers.

Avaya Aura® Experience Portal supports any XML speech application that is compliant with Voice XML Version 2.1 or Call Control eXtensible Markup Language (CCXML), regardless of the tool in which the application was created. However, Avaya recommends that you create your speech applications with Orchestration Designer. Avaya Aura® Experience Portal automatically includes all Orchestration Designer applications in the Application Summary report and Application Detail report. If you want these reports to display messages and status information from an application developed in a third-party tool, you must manually log the messages and status information from that application using the Application Logging Web service.

The following diagram shows a typical solution layout of a front-end Avaya Aura® Experience Portal self-service integration with Avaya Aura® Contact Center and Communication Manager platform.

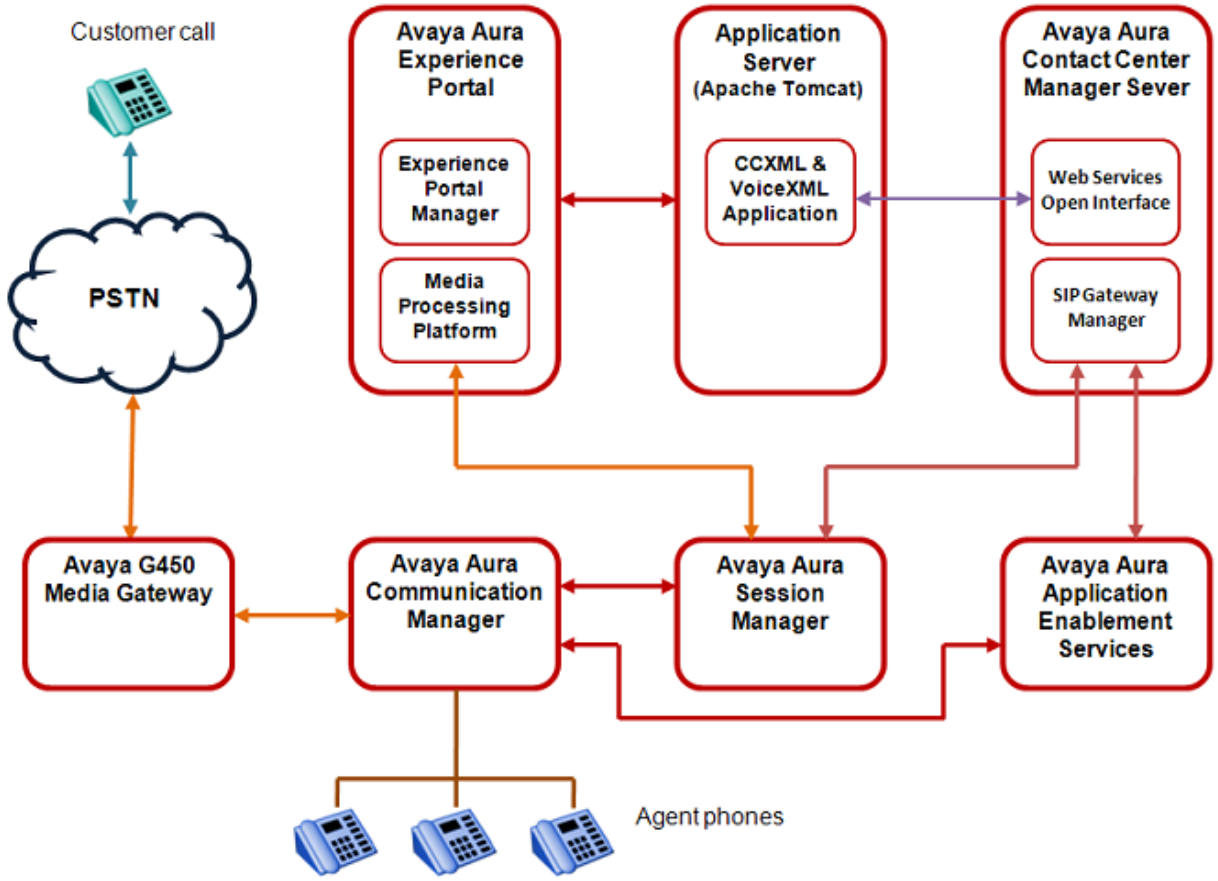


Figure 5: Example of front-end Avaya Aura® Experience Portal using Contact Center Web Service Open Interfaces

Call flow example using CCMS Web service Open Interfaces

This call flow example shows how the Avaya Aura® Experience Portal system interacts with Avaya Aura® Contact Center Web Service Open Interfaces to handle a typical automated front-end self-service customer transaction.

1. Incoming customer calls are routed to a Media Processing Platform (MPP) server in the Avaya Aura® Experience Portal system.
2. The MPP server checks the Dialed Number Identification Service (DNIS) for the incoming call and uses the configuration information downloaded from the Experience Portal Manager (EPM) server to match the number to a speech application on Avaya Aura® Experience Portal.
3. The Experience Portal Management System starts an Avaya Voice Browser session and passes it the Universal Resource Indicator (URI) specified for the selected speech application.

4. The Avaya Voice Browser contacts the application server and passes it the URI.
5. The application server returns a Voice XML page to the Avaya Voice Browser.
6. Based on instructions on the Voice XML application, the MPP uses prerecorded audio files, Text-to-Speech (TTS), or both to play a prompt to start interaction with the caller.
7. If the customer responds by:
   - Entering Dual-tone multi-frequency (DTMF) digits, the MPP establishes a connection to a TTS server and the ASCII text in the speech application is forwarded for processing. The TTS server renders the text as audio output in the form of synthesized speech which the MPP then plays for the caller.
   - Speaking, the MPP establishes a connection to an Automatic Speech Recognition (ASR) server and sends the caller's recorded voice response to the ASR server for processing. The ASR server then returns the results to the application for further action.
8. The customer chooses to speak to an agent.
9. The Voice XML application connects to the Contact Center Manager Server Open Interface Web services. The Voice XML application requests a Landing Pad number. As part of the Landing Pad number request the Voice XML applications specifies a destination Controlled Directory Number (CDN), transfer type (blind, bridged, or consult transfer), contact ID number, and Contact Intrinsics.
10. Contact Center Manager Server returns the Landing Pad number to the Voice XML application.
11. The Experience Portal Media Processing Platform (MPP) server uses this Landing Pad number to complete the blind transfer of the customer call to the destination CDN.
12. Contact Center Manager Server is now controlling the customer call. Contact Center Manager Server routes the call to an appropriate agent skillset.
13. The call is offered to a Contact Center agent.
14. The Contact Center agent answers the customer call.
15. The XML application terminates the call when it finishes execution or when the caller releases the call.

A combined Avaya Aura® Experience Portal self-service system and Avaya Aura® Contact Center solution gives customers exceptional service and improved efficiency. Front-end self-service automation reduces contact center operating costs and improves Customer Satisfaction (CSAT).

Front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

A combined Avaya Aura® Experience Portal self-service system and SIP-enabled Avaya Aura® Contact Center solution gives your customers exceptional service and improved efficiency. Front-

end self-service automation reduces contact center operating costs and improves Customer Satisfaction (CSAT).

Avaya Aura® Experience Portal uses XML speech applications and SIP messaging-based information to integrate with Avaya Aura® Contact Center. A self-service Voice XML speech application running on the Avaya Aura® Experience Portal Tomcat application server answers customer calls and modifies the call-associated User-to-User Information (UUI) based on customer answers and inputs. When customer calls are transferred to Contact Center agents, the agents use the call-related Contact Intrinsic data to access customer details. This reduces the amount of time the agents spend on each call, improves customer experience, making Contact Center more efficient.

Avaya recommends that you create your XML speech applications with Avaya Aura® Orchestration Designer. Avaya Aura® Experience Portal automatically includes all Orchestration Designer applications in the Application Summary report and Application Detail report. If you want these reports to display messages and status information from an application developed in a third-party tool, you must manually log the messages and status information from that application using the Application Logging Web service.

The following diagram shows a typical solution layout of a front-end Avaya Aura® Experience Portal self-service integration with Avaya Aura® Contact Center and Avaya Aura® Communication Manager.

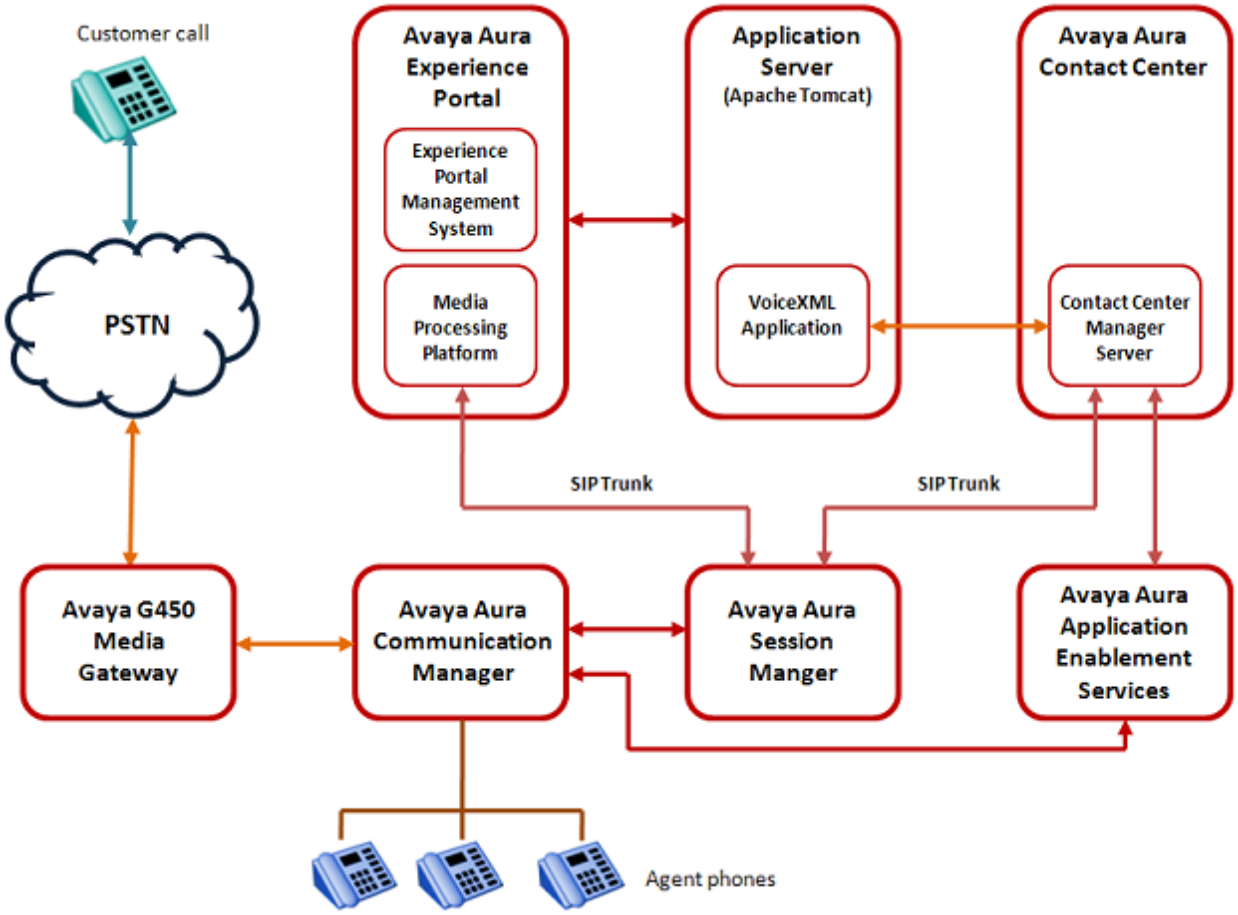


Figure 6: Example of front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

Call flow example for front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

This call flow example shows how the Avaya Aura® Experience Portal system interacts with Avaya Aura® Contact Center to handle a typical automated front-end self-service customer transaction.

1. Incoming customer calls are routed to a Media Processing Platform (MPP) server in the Avaya Aura® Experience Portal system.
2. The MPP server checks the Dialed Number Identification Service (DNIS) for the incoming call and uses the configuration information downloaded from the Experience Portal Manager (EPM), server to match the number to a speech application on Avaya Aura® Experience Portal.
3. The Experience Portal Management System starts an Avaya Voice Browser session and passes it the Universal Resource Indicator (URI) specified for the selected speech application.

4. The Avaya Voice Browser contacts the application server and passes it the URI.
5. The application server returns a Voice XML page to the Avaya Voice Browser.
6. Based on instructions on the Voice XML application, the MPP uses prerecorded audio files, Text-to-Speech (TTS), or both to play a prompt to start interaction with the caller.
7. If the customer responds by entering Dual-Tone Multi-Frequency (DTMF) digits, the MPP establishes a connection to a TTS server and the ASCII text in the speech application is forwarded for processing. The TTS server renders the text as audio output in the form of synthesized speech which the MPP then plays for the caller.
8. The customer chooses to speak to an agent.
9. The Voice XML application connects to the Contact Center Manager Server. The Voice XML application specifies a destination Controlled Directory Number (CDN) or Agent, transfer type (blind, bridged, or consult transfer), contact ID number, and UUI data generated Contact Intrinsics.
10. The Experience Portal Media Processing Platform (MPP) server completes the blind transfer of the customer call to the destination CDN.
11. The Contact Center Manager Server SIP Gateway Manager (SGM) is now controlling the customer call. The SGM routes the call to an appropriate agent skillset.
12. A Contact Center agent is offered the call. The agent can access customer details and Contact Intrinsics before answering the call.
13. The Contact Center agent receives the (customer and call) context information in a screen pop and answers the customer call.
14. The XML application terminates the call when it finishes execution or when the caller releases the call.

A combined Avaya Aura® Experience Portal self-service system and SIP-enabled Avaya Aura® Contact Center solution gives customers exceptional service and improved efficiency. Front-end self-service automation reduces contact center operating costs and improves Customer Satisfaction (CSAT).

Avaya Aura® Experience Portal uses Voice XML applications and SIP header (UUI and P-Intrinsics) information to integrate with Avaya Aura® Contact Center. This gives enterprises complete flexibility and control of the integrated solution. The front-end Avaya Aura® Experience Portal self-service system and Avaya Aura® Contact Center solution is highly flexible and efficient. Avaya supplies sample Voice XML applications for the rapid integration of a front-end Avaya Aura® Experience Portal system with an Avaya Aura® Contact Center.

Back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

Avaya Aura® Experience Portal provides back-end Interactive Voice Response (IVR) services like text-to-speech, digit collection, music, and speech recognition. A combined Avaya Aura®

Experience Portal system and Avaya Aura® Contact Center solution gives your customers exceptional service and improved efficiency. Back-end Interactive Voice Response (IVR) reduces contact center operating costs and improves Customer Satisfaction (CSAT).

In a typical back-end Avaya Aura® Experience Portal solution, customer calls to the Avaya Aura® Contact Center are routed to Experience Portal applications for automated processing. Avaya Aura® Experience Portal applications play voice prompts asking the customer to select items from a menu, or to input account numbers. The customer responds by entering digits on their phone, or by speaking (Experience Portal supports optional Automatic Speech Recognition servers). The Experience Portal applications then collect the customer's response and return it to Avaya Aura® Contact Center for further treatments, or routing to the next available and an appropriate Agent.

The following diagram shows a typical solution layout of an Avaya Aura® Contact Center with a back-end Avaya Aura® Experience Portal integration.

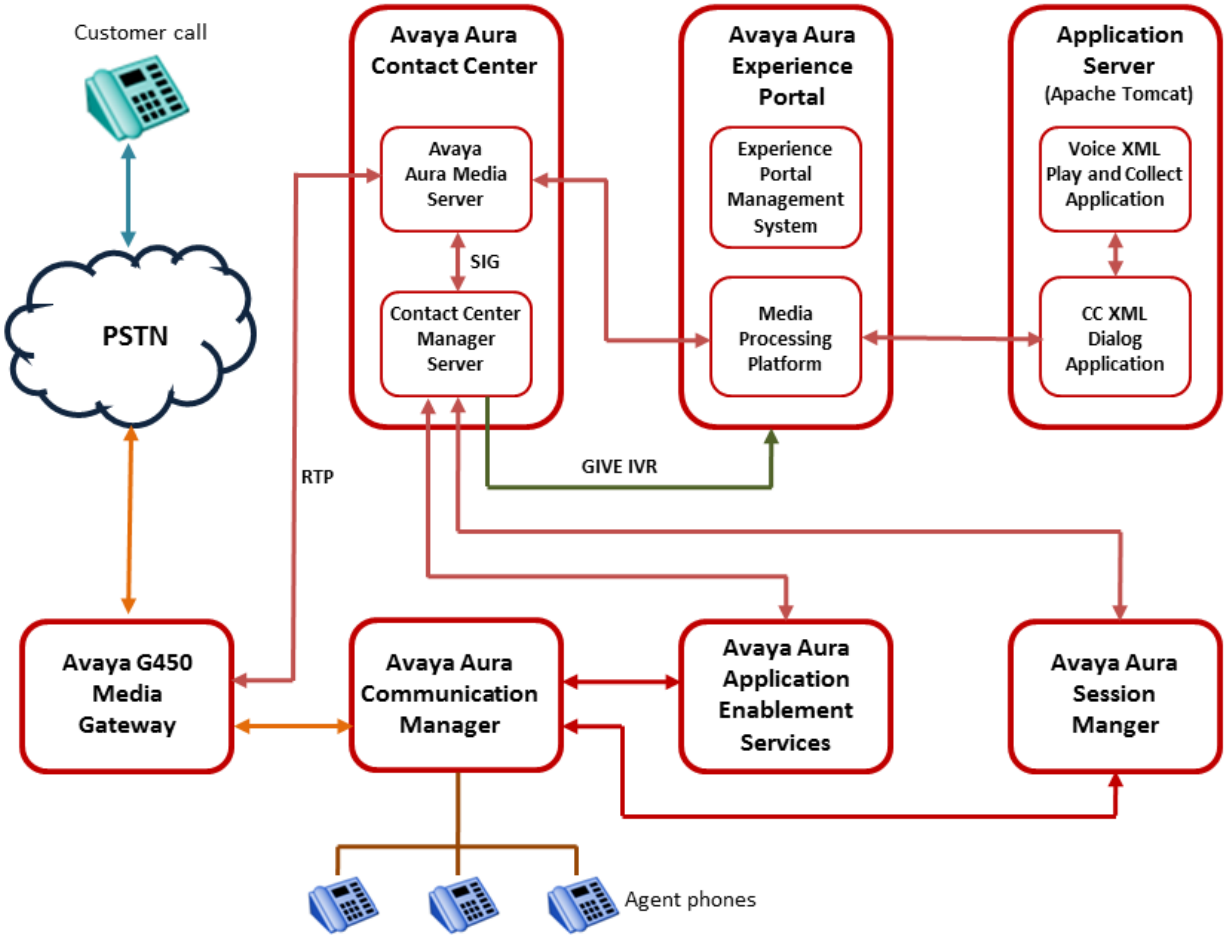


Figure 7: Example of back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

Call flow example using back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

This call flow example shows how the Avaya Aura® Experience Portal system interacts with Avaya Aura® Contact Center to handle a typical automated back-end Interactive Voice Response (IVR) customer transaction.

1. Incoming customer calls to the Communication Manager are routed by the Session Manager to Avaya Aura® Contact Center.
2. Avaya Aura® Contact Center answers the call and runs a flow application, script, and/or optional primary scripts. A primary script is an application ran or referenced by the Master Script. Contact Center Manager Server records Master script and Primary script actions in statistical records.
3. The Avaya Aura® Contact Center script issues a `GIVE IVR` for an external media server (XDIALOG), supplying the URI identifier of the Avaya Aura® Experience Portal.
4. Avaya Aura® Contact Center retains control of the call and sends a `SIP INVITE` message to Avaya Aura® Experience Portal. Avaya Aura® Contact Center specifies treatment parameters in the `SIP INVITE` message.
5. Avaya Aura® Experience Portal passes the call to a CCXML dialog application on the Apache Tomcat application server.
6. The CCXML dialog application accepts and retrieves IVR parameters from the `SIP INVITE` message.
7. The CCXML dialog application invokes the Play and Collect Voice XML application (PlayAndCollect) with the parameters retrieved from Avaya Aura® Contact Center. If available, SIP header UUI data is also extracted and passed to the Voice XML application.
8. The Play and Collect Voice XML application streams Real-time Transport Protocol (RTP) streams into the associated Avaya Aura® Media Server conference, and prompts the customer to enter digits on their phone.
9. The Play and Collect Voice XML application collects the digits entered by the customer.
10. The Play and Collect Voice XML application then passes the customer's digits back to the CCXML dialog application.
11. The CCXML dialog application returns the collected digits to Avaya Aura® Contact Center in a `SIP INFO` message.
12. The CCXML dialog application then drops out (`BYE`).
13. The Avaya Aura® Contact Center script retrieves the IVR collected digits.

A combined Avaya Aura® Contact Center and Avaya Aura® Experience Portal solution gives customers exceptional service and improved efficiency. Back-end Avaya Aura® Experience Portal automation reduces contact center operating costs and improves Customer Satisfaction (CSAT).

Avaya Aura® Contact Center uses Call Control XML and Voice XML applications to integrate with Avaya Aura® Experience Portal. This gives enterprises complete flexibility and control of the

solution integration. The Avaya Aura® Experience Portal system and Avaya Aura® Contact Center solution is highly flexible and efficient. Avaya supplies sample Voice XML applications for the rapid integration of a back-end Avaya Aura® Experience Portal system with an Avaya Aura® Contact Center.

Back-end Avaya Aura® Experience Portal using Context Creation and SIP-enabled Contact Center

Avaya Aura® Experience Portal provides back-end Interactive Voice Response (IVR) services like text-to-speech, digit collection, music, and speech recognition. A combined Avaya Aura® Experience Portal system and Avaya Aura® Contact Center solution gives your customers exceptional service and improved efficiency.

Avaya Aura® Contact Center provides generic sample applications to demonstrate how it integrates with Avaya Aura® Experience Portal. You can select a sample application that suits your integration, review the sample code, and customize it to your solution before deploying it in production.

In a SIP-enabled contact center solution, the information stored in some SIP INFO messages can be used to transfer call-related information between SIP-enabled components. This call-related information enables the receiver to better understand and handle the call. If your call-related context information does not fit in a SIP User-to-User Information (UUI) header or in the larger P-Intrinsics header, you can use the sample Context Creation application to pass more context information from Avaya Aura® Experience Portal to Avaya Aura® Contact Center.

The Context Creation sample application can inject multiple pieces of context information (Intrinsics and Call Attached Data) into Avaya Aura® Contact Center, where as the Play and Collect sample application can retrieve only a single piece of data, for example collected digits.

In a typical back-end Avaya Aura® Experience Portal solution, customer calls to the Avaya Aura® Contact Center are routed to Avaya Aura® Experience Portal applications for automated processing. Avaya Aura® Experience Portal applications play voice prompts asking the customer to select items from a menu, or to input account numbers. The customer responds by entering digits on their phone, or by speaking (Avaya Aura® Experience Portal supports optional Automatic Speech Recognition servers). The Avaya Aura® Experience Portal applications then collect the customer's response and return it to Avaya Aura® Contact Center for further treatments, or routing to the next available and an appropriate Agent.

In a back-end integration where Avaya Aura® Experience Portal is using the Context Creation sample application, the Avaya Aura® Contact Center Orchestration Designer script sends a GIVR IVR (SIP INVITE) message into the Avaya Aura® Experience Portal system. The SIP INVITE message has “treatmenttype” set to “contextcreation”. Avaya Aura® Experience Portal passes the SIP call to a sample Dialog CC XML application. The Dialog CC XML and Context Creation VoiceXML applications process the call, and return hex-encoded call-related information. Because the “treatmenttype” was set to “contextcreation”, the Dialog application returns a SIP INFO message of type “application/x-aacc-info” to the Contact Center. The Contact Center SIP Gateway

Manager (SGM) recognizes this SIP message type and converts the context information in the call into Contact Intrinsics. The Orchestration Designer script can then access and use the Contact Intrinsics for the call, and Contact Center can pass them on to Avaya Agent Desktop.

This sample Dialog and Context Creation applications can return multiple values from Avaya Aura® Experience Portal, rather than the single value returned by the Avaya Aura® Contact Center sample Play and Collect VoiceXML application. The Context Creation sample application supports more complex data. The call-related context information is returned in a SIP INFO message body. A SIP INFO message body holds and transfers much more information than a SIP header.

When using the Context Creation sample application, the SIP message body data is hex-encoded and XML-formatted (using the same encoding as P-Intrinsics).

Example of a single intrinsic in VoiceXML code (Note: spaces are not supported):

```
<cc><i>CUSTOMER_SESSION_ID=12345</i></cc>
```

Example of the single intrinsic when Hex-encoded:

```
3c63633e3c693e435553544f4d45525f53455353494f4e5f49443d31323334353c2f693e3c2f63633e
```

The following diagram shows a typical solution layout of an Avaya Aura® Contact Center with a back-end Avaya Aura® Experience Portal integration.

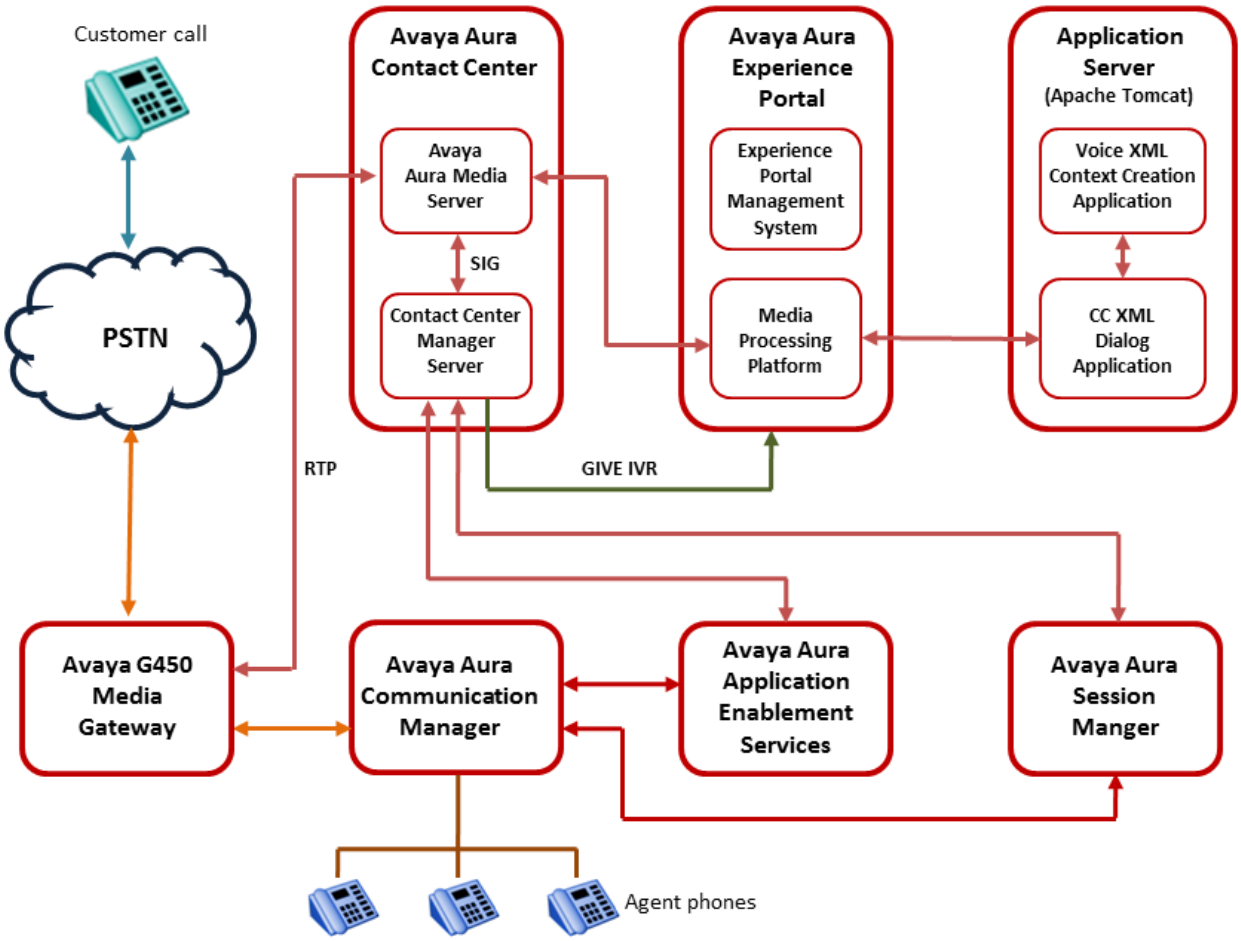


Figure 8: Example of back-end Avaya Aura® Experience Portal using the Context Creation sample application

Call flow example using back-end Avaya Aura® Experience Portal with the Context Creation sample application

This call flow example shows how the Avaya Aura® Experience Portal system interacts with Avaya Aura® Contact Center to handle a typical automated back-end Interactive Voice Response (IVR) customer transaction.

1. Incoming customer calls to the Communication Manager are routed by the Session Manager to Avaya Aura® Contact Center.
2. Avaya Aura® Contact Center answers the call and runs a script, and/or optional primary scripts. A primary script is an application ran or referenced by the Master Script. Contact Center Manager Server records Master script and Primary script actions in statistical records.

3. The Avaya Aura® Contact Center script issues a `GIVE IVR` for an external media server (XDIALOG), supplying the URI identifier of the Avaya Aura® Experience Portal.
4. Avaya Aura® Contact Center retains control of the call and sends a `SIP INVITE` message to Avaya Aura® Experience Portal. Avaya Aura® Contact Center specifies treatment parameters in the `SIP INVITE` message. The SIP INVITE message has “treatmenttype” set to “contextcreation”.
5. Avaya Aura® Experience Portal passes the call to the sample CCXML dialog application on the Apache Tomcat application server.
6. The CCXML dialog application accepts and retrieves IVR parameters from the `SIP INVITE` message.
7. The CCXML dialog application invokes the Context Creation Voice XML application with the parameters retrieved from Avaya Aura® Contact Center.
8. The Context Creation Voice XML application streams Real-time Transport Protocol (RTP) streams into the associated Avaya Aura® Media Server conference, and prompts the customer to enter digits on their phone.
9. The Context Creation Voice XML application collects the digits entered by the customer.
   - If the digits match the first account number (AccountA=123123) in the application’s config.properties file, the Context Creation application uses the “Context Data for account A” data from the configuration file and hex encodes it.
   - If the entered digits match the second account (AccountB=456456) in the application’s config.properties file, the Context Creation application uses the “Context Data for account B” data from the configuration file and hex encodes it.

   The sample Context Creation application uses the account number details from the configuration files for illustration purposes. In a real solution, you can extract the context data from anywhere; be it an external database, a Customer Relationship Management (CRM) system, or from context gathered within the Orchestration Designer application.
10. The Context Creation Voice XML application then passes the encoded hex data back to the CCXML dialog application.
11. The CCXML dialog application returns the encoded hex data to Avaya Aura® Contact Center in a SIP INFO message. Because “treatmenttype” was set to “contextcreation”, the dialog application sets the type of the SIP message body to ‘application/x-aacc-info’.
12. The CCXML dialog application then drops out (`BYE`).
13. The Avaya Aura® Contact Center SIP Gateway Manager (SGM) recognizes this SIP message type and creates context information for the call by converting the hex encoded data in the SIP INFO message body into Contact Intrinsics.
14. The Avaya Aura® Contact Center script logs the returned value.

Avaya Aura® Contact Center uses Call Control XML and Voice XML applications to integrate with Avaya Aura® Experience Portal. This gives enterprises complete flexibility and control of the solution integration. The Avaya Aura® Experience Portal system and Avaya Aura® Contact Center solution is highly flexible and efficient. Avaya supplies sample Voice XML applications for the rapid

integration of a back-end Avaya Aura® Experience Portal system with an Avaya Aura® Contact Center.

Avaya DevConnect

The Avaya DevConnect Program provides a wide range of developer resources, including access to APIs and SDKs for Avaya products, developer tools, technical support options, and training materials. Registered membership is free to anyone interested in designing Avaya-compatible solutions. Enhanced Membership options offer increased levels of technical support, compliance testing, and co-marketing of innovative solutions compatible with standards-based Avaya solutions.

Avaya Aura® Contact Center supplies generic sample Avaya Aura® Experience Portal applications for demonstration purposes. If you plan to use these sample applications, you must review the sample code and customize it to your solution prior to deploying in production.

For more information, and to download the complete Avaya Aura® Experience Portal and Avaya Aura® Contact Center sample files, see Orchestration Designer Sample Applications on www.avaya.com/devconnect.

Chapter 8: Mission Critical High Availability overview

Avaya Aura® Contact Center supports Mission Critical High Availability (MCHA) resiliency for Contact Center Manager Server (CCMS), and Communication Control Toolkit (CCT). Avaya Aura® Media Server on the Linux operating system supports High Availability (HA) resiliency. Avaya Aura® Media Server High Availability is supported only on standalone Linux-based servers. Contact Center Multimedia (CCMM) also supports High Availability.

All of the Contact Center servers must be in the same network subnet IP address range. All of the Avaya Aura® Unified Communications components (CM, SM, and AES) must be in the same campus network location as the Contact Center servers.

All Contact Center servers must be in the same Windows Active Directory domain. All Contact Center servers must be registered with the same Windows Active Directory Domain Controller. The active and standby Contact Center servers must be in the same subnet IP address range for campus High Availability resiliency to work. All Agent Desktop clients must be registered in this domain, or in domains with a two-way trust relationship with this Contact Center server domain.

One set of Contact Center applications (a CCMS, a CCT, and an optional CCMM) actively processes scripts and contacts. This set of applications is called the active set. Another set of Contact Center applications in the same Contact Center system monitors and shadows the active applications in the system. The standby applications track the state of active calls but do not process calls. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, a switchover to the standby server occurs. The standby applications recognize the failure and start processing contacts.

Contact Center Administrators use the active server in daily operation. Configuration changes made to the active system during normal operation automatically replicate to the standby system. Therefore the standby system has the most recent configuration and is ready to take over processing from the active system. Statistical data also automatically replicates to the standby system. Data replicates to the standby system in real-time.

MCHA switchover

In a Mission Critical High Availability campus solution, there are two types of switchovers, managed or unmanaged. A managed switchover is one initiated by the administrator or caused by a failure of a monitored CCMS or CCT service. An unmanaged switchover results from a

hardware, network, database, or power failure. Switchovers can occur only in the following situations:

- The active and standby servers are in running state.
- On the active server, all the critical CCMS and CCT services are monitored and running.
- The active server has Switchover enabled.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database.
- The standby server can communicate with (ping) the Trusted IP address.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an active server, a managed switchover occurs. If the Contact Center Administrator uses System Control and Monitor Utility (SCMU) to stop a monitored service on an active server, a switchover does not occur.

Agent experience during an MCHA switchover

If any Contact Center application or server fails, the Mission Critical High Availability solution provides a zero-touch Agent Desktop experience. Agent Desktop agent calls in progress continue without interruption, agent login and state are maintained. New calls that arrive during the switchover are treated and routed without delay.

Note:

High Availability does not support Instant Message (IM) contact types. If a switchover occurs, IM contacts are lost.

In a Mission Critical High Availability campus solution Agent Desktop clients are registered with both Communication Control Toolkit servers. In multimedia-enabled systems Agent Desktop clients are registered with the managed IP address of the Contact Center Multimedia servers.

Administrator experience during an MCHA switchover

In a Mission Critical High Availability campus solution the Contact Center Administrator launches Contact Center Manager Administration (CCMA) using the Managed name of the pair of campus servers.

If an active Contact Center application or server fails, the CCMA client Web browser continues to use the managed name, and the Contact Center Administrator refreshes the Web browser to continue working.

Supervisor experience during an MCHA switchover

Avaya Aura® Contact Center maintains agent states such as logged in state and ready state, if the active Contact Center server fails, and the Real Time Displays (RTDs) that a supervisor is observing reflect this. However, Contact Center does not maintain all real-time values, such as time in state, and the supervisor notices that some RTD items reset. The supervisor must inform IT staff, who receive an automatic email/SNMP switchover notification in parallel, and can then proceed with the customer's normal follow-up procedure for dealing with a server switchover.

The RTDs must use multicast as opposed to unicast in order eliminate the need to manually restart the RTD after a Contact Center server switchover.

During the switchover there is a small interval of time when contact processing is operational but the reporting subsystem is not. During this interval, Contact Center correctly routes new contacts entering the contact center, but cannot reported on those contacts. Real-time and historical reports do not have an accurate representation of the contacts that enter while the reporting subsystem is unavailable. This does not impact customer calls and contacts continue to be routed to skilled agents.

Note:

At the point where a switchover occurs, the CCMS services stop on the active server. As a result, the historical data being collected on the disk for the 15 minute interval is not saved into the historical statistics tables. It is not possible to recover this data.

Switchover Handling Script

In SIP-enabled Contact Centers using the Mission Critical High Availability feature, the Switchover Handling Script handles calls in treatment during a switchover.

Under normal operation, calls to the Contact Center are routed to the master script for processing, treatments, and queuing to an appropriate skillset. The active CCMS application uses the media processing capabilities of Avaya Aura® Media Server to provide ringback, conferencing, and other treatments to these calls.

If the active CCMS application is shut down or fails, a switchover occurs, and the standby CCMS application starts processing calls. The standby CCMS server is now the active CCMS server. New calls that arrive after the switchover go to the Master script on the currently active CCMS server and call processing continues as normal.

The Avaya Aura® Media Server cannot return calls that were in treatment during the switchover to the CCMS application that originally routed them, because it is no longer available. Avaya Aura® Media Server routes these calls to the Switchover Handling Script on the currently active CCMS.

The Switchover Handling Script expedites the calls that were in treatment at the time of the active server failure. This means that calls are queued as quickly as possible to an appropriate skillset

for that contact type. This can be a default skillset, or a skillset defined by the Contact Center Administrator.

Calls in treatment during a switchover can contain data, depending on their position in the script on the active server before the switchover occurred. Avaya recommends that you modify the default Switchover Handling Script to check each call for useful data. If the call does not have useful data, queue the call to the appropriate default skillset.

If the call has useful data or intrinsics, queue it to the most appropriate skillset as normal. The intrinsics available following a switchover are the intrinsics information at the time of creation. For example:

- Call intrinsics
- Multimedia intrinsics
- Skillset intrinsics
- Time intrinsics
- Traffic intrinsics
- SIP intrinsics. SIP Intrinsics are pieces of data that might be available on a contact depending on factors such as the contact type. If a treatment is performed on a contact, or the contact is transferred, conferenced, or routed to an agent, the intrinsic value might not be available. The SIP_RETURNED_TEXT_n, SIP_RETURNED_DIGITS_n, SIP_RETURNED_DIGITS_LAST, and SIP_RETURNED_DIGITS_2LAST intrinsics are not available following a switchover.

Call and global variable changes during call processing on the active server are not propagated to the standby server.

Note:

After a High Availability switchover, multimedia contacts can be redirected to a different skillset queue. After a switchover, multimedia contacts are re-queued to a skillset appropriate to their contact intrinsics. If the multimedia contacts have insufficient intrinsic data or if the appropriate skillset is Out Of Service, Contact Center queues the multimedia contacts to the default skillset for the contact type. Contact Center queues email contacts transferred to agents or Pulled Closed email contacts that are in-queue at switchover time only to a skillset after switchover. Contact Center does not queue them to the agent.

You can use Contact Center Orchestration Designer to edit the default Switchover Handling Script. The Switchover Handling script does not support commands that delay the handling of calls.

The Switchover Handling Script does not support the following HDX commands:

- SEND INFO
- SEND REQUEST
- GET RESPONSE

The Switchover Handling Script does not support the following commands:

- EXECUTE SCRIPT

- GIVE BUSY
- GIVE MUSIC
- GIVE OVERFLOW
- GIVE RAN
- GIVE RINGBACK
- GIVE SILENCE
- GIVE IVR
- GIVE Controlled Broadcast

A Switchover Handling Script containing these commands does not validate in Contact Center Orchestration Designer.

The Switchover Handling Script applies only in Mission Critical High Availability solutions.

Other applications cannot start the Switchover Handling Script, and the Switchover Handling Script cannot start other applications. For more information about scripts and applications, see *Using Contact Center Orchestration Designer*.

Mission Critical High Availability operation

Contact Center supports High Availability for fault tolerant and mission critical contact centers. In High Availability contact center solutions, the active server actively processes scripts and contacts. A standby server in the same contact center solution monitors and shadows the active server. Each active and standby pair of servers forms a High Availability resilient or replication pair. If the active server fails, the standby server detects the failure and starts processing calls.

The level of Contact Center application High Availability you achieve depends on your complete enterprise contact center solution, including the underlying network infrastructure. In a Mission Critical High Availability solution, the active and standby servers constantly communicate with each other and monitor system components. The High Availability - System Management and Monitoring Component (SMMC) monitors network communications, network latency, and contact center components. If a Contact Center component or network link fails, SMMC detects this failure and takes appropriate action.

Network failures

The active and standby servers use a Trusted IP address to diagnose network connectivity faults. Use the IP address of some part of your IT infrastructure that is always available to respond to a ping request, as the Trusted IP address.

If SMMC on the active server cannot communicate with SMMC on the standby server, SMMC pings the Trusted IP address to determine if the network outage is local or remote. If the active server SMMC can communicate with the Trusted IP address, the network outage is remote and the active server continues processing contacts. If the active server SMMC cannot communicate with the Trusted IP address or the standby server, the network outage is local and the active server therefore stops processing contacts.

If SMMC on the standby server cannot communicate with the active server, but can communicate with the Trusted IP address, SMMC enables call processing on the standby server. If SMMC on

the standby server cannot communicate with the active server or with the Trusted IP address, the standby server shuts down.

If both the active and standby servers lose network connectivity, this can lead to a standby-standby scenario. Total network loss means both servers cannot communicate with each other or ping the Trusted IP address. The current standby server cannot go active because it has lost network connectivity. The current active server goes standby because it has lost network connectivity. Contact Center loses call-control during the network outage. When network connectivity returns, you must manually reconfigure High Availability.

Service failures

If a critical service on the active Contact Center server fails, a switchover occurs. The standby Contact Center server becomes active and takes over processing. Contact Center gracefully halts the remaining services on the crashed server, in order to place the original active server in a known state for follow-up analysis of the fault.

Mission Critical HA uses database and in-memory replication to ensure that the standby server is fully synchronized with the active server. If switchovers are not enabled and if the standby server cannot communicate with the active server for a period of time greater than the configured Network Timeout time, the standby server is out of sync and it therefore shuts down. To reinstate High Availability resiliency, you must ensure the active and standby servers can communicate with each other, and then manually restart the standby server (and enable switchovers if required).

The following table shows the Mission Critical active and standby server configurations and outcomes.

Switchover configuration	Server outage	Outcome
Enabled	Active server outage	Switchover
Enabled	Standby server outage	Standby shuts down
Not Enabled	Active server outage	Standby shuts down
Not Enabled	Standby server outage	Standby shuts down

Rebooting High Availability servers

Use the High Availability - System Management and Monitoring Component (SMMC) to stop and start High Availability servers. Rebooting the active or standby server can shut down Contact Center services in the wrong order, resulting in unpredictable contact center behavior. If you must reboot the active or standby server, first use SMMC to shut down the HA system and the Contact Center services. Then, after rebooting the server, use SMMC to start the Contact Center services and HA system.

Changing Mission Critical Standby servers

In High Availability solutions the standby server shadows the active server. If you change the standby server (replace one standby server with another standby server) you must perform the following procedures to reinstate High Availability resiliency and enable switchovers:

- Use SMMC to shut down the HA system on the active and standby servers.
- Configure the new standby server.
- Configure the active server to use the new standby server.
- Reboot the active and standby servers.

- Use SMMC to start the HA system on the active and standby servers.
- Use SMMC to enable Switchover on the active server.

Mission Critical High Availability campus solutions

Avaya Aura® Contact Center Mission Critical High Availability supports a number of solutions running on the Avaya Aura® Unified Communications platform. While these Contact Center solutions are similar in behavior, there are differences depending on the platform components of each solution.

The level of Contact Center application High Availability you can achieve depends on your complete enterprise contact center solution. You can configure your contact center to have no single point of failure. You achieved this by deploying Contact Center with a resilient Avaya Aura® Unified Communications platform configured for High Availability. Contact Center supports the following Mission Critical High Availability solutions:

- Mission Critical HA with Avaya Aura platform resiliency on page 80
- Mission Critical HA without Avaya Aura platform resiliency on page 81
- Mission Critical HA with Avaya Aura Unified Communications Virtualized Environment on page 83

Contact Center also supports Geographic data resiliency and disaster recovery with these campus configurations.

Mission Critical HA with Avaya Aura® platform resiliency

To achieve the highest level of Mission Critical High Availability with no single point of failure you must have a SIP-enabled Contact Center with the following:

- Two Voice Contact Servers configured as a High Availability pair and two Multimedia Contact Servers configured as a High Availability pair.

  OR

  Two Voice and Multimedia Contact Servers configured as a High Availability pair.
- Two or more Avaya Aura® Media Server Linux-based servers, configured as High Availability pairs. Avaya Aura® Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.
- Two Avaya Aura® Session Manager (SM) instances.
- Two Avaya Aura® Application Enablement Services (AES) servers with Avaya Aura® System Platform-based High Availability.
- Two Avaya Aura® Communication Manager (CM) servers configured as a High Availability Duplex pair.

- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

The following diagram shows a typical Mission Critical High Availability solution with a resilient Avaya Aura® platform.

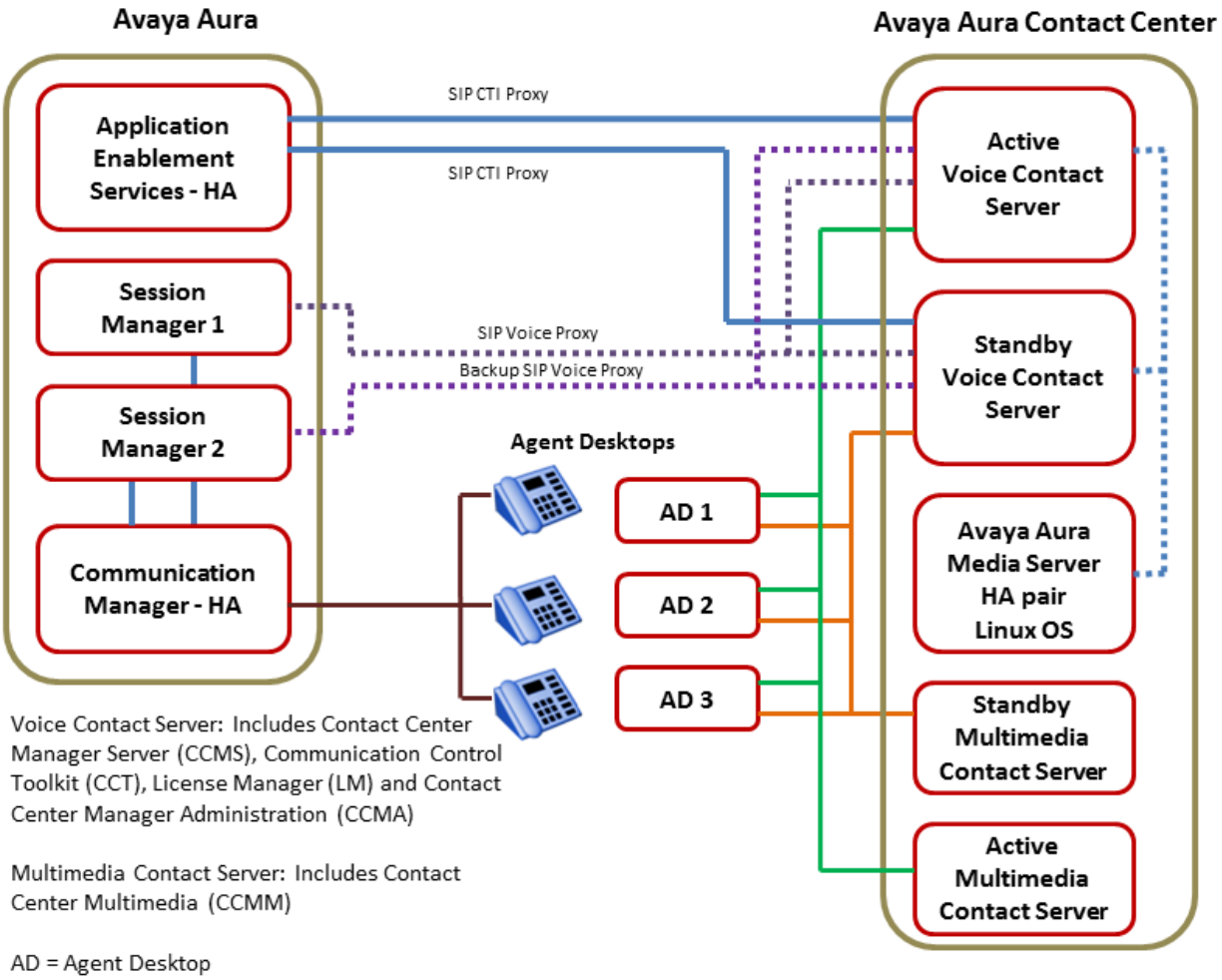


Figure 9: Example of a typical Mission Critical High Availability solution with a resilient Avaya Aura® platform

Mission Critical HA without Avaya Aura® platform resiliency

To achieve Mission Critical High Availability without platform resiliency, you must have a SIP-enabled Contact Center with the following:

- Two Voice Contact Servers configured as a High Availability pair and two Multimedia Contact Servers configured as a High Availability pair.

  OR

Two Voice and Multimedia Contact Servers configured as a High Availability pair.

- Two or more Avaya Aura® Media Server Linux-based servers, configured as High Availability pairs. Avaya Aura® Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.
- One Avaya Aura® Session Manager (SM) instance.
- One Avaya Aura® Application Enablement Services (AES) server.
- One Avaya Aura® Communication Manager (CM) server.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

Note:

This is the least resilient Mission Critical HA solution, as there is no platform resiliency. If an outage occurs on any of the Unified Communications components in this solution, the contact center agents can experience downtime, loss of call control, or call loss.

The following diagram shows a typical Mission Critical High Availability solution without a resilient Avaya Aura® platform.

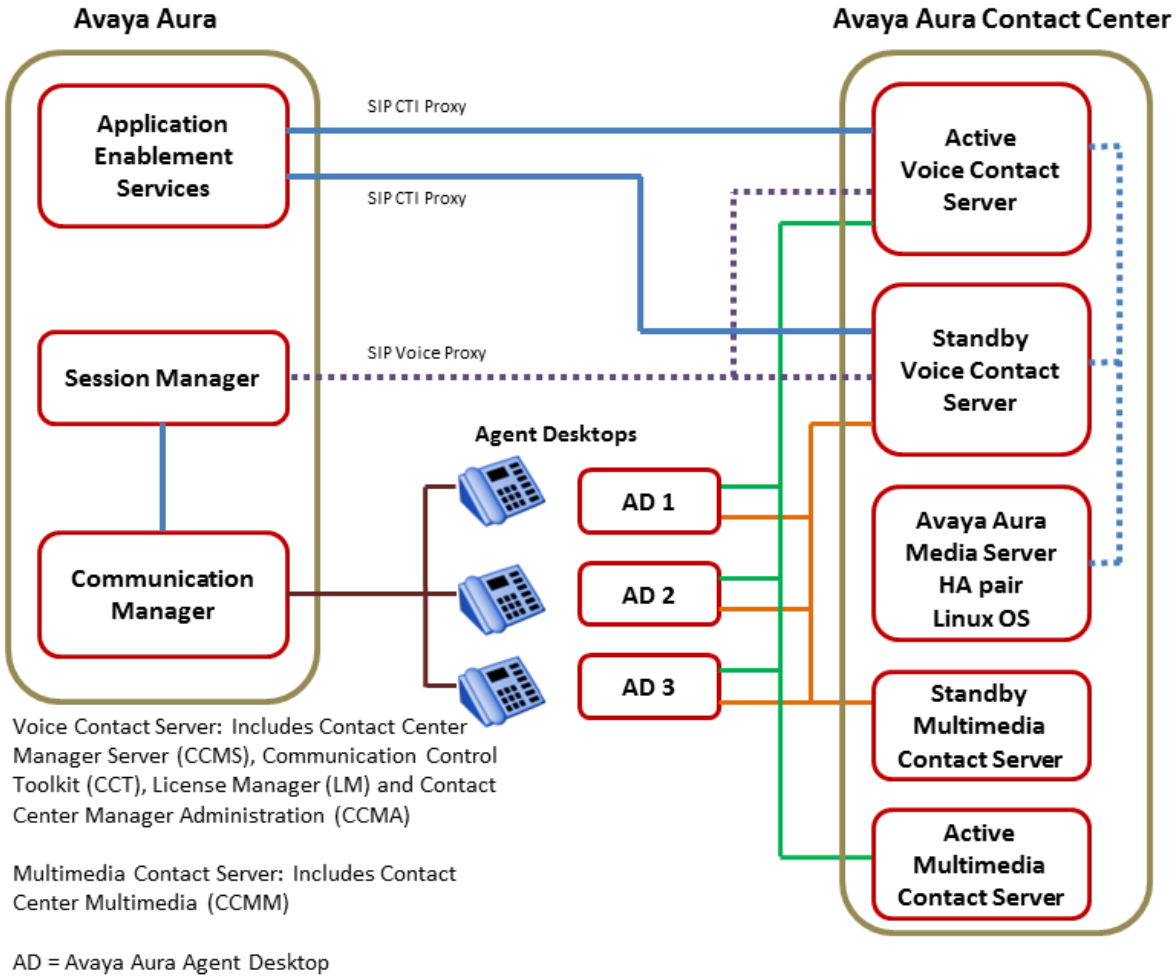


Figure 10: Example of a typical Mission Critical High Availability solution without a resilient Avaya Aura® platform

Mission Critical HA with Avaya Aura® Unified Communications Virtualized Environment

Contact Center Mission Critical High Availability is supported with a simplex or duplex Avaya Aura® Unified Communications Virtualized Environment (VE) voice platform.

To achieve Contact Center Mission Critical High Availability without Avaya Aura® Unified Communications Virtualized Environment (VE) voice platform resiliency, you must have a SIP-enabled Contact Center with the following:

- Two Voice Contact Servers configured as a High Availability pair and two Multimedia Contact Servers configured as a High Availability pair.

  OR

Two Voice and Multimedia Contact Servers configured as a High Availability pair.

- Two or more Avaya Aura® Media Server Linux-based servers, configured as High Availability pairs. Avaya Aura® Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.
- One Avaya Aura® Unified Communications Virtualized Environment (VE) voice platform. This solution type does not provide voice platform resiliency.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

To achieve Contact Center Mission Critical High Availability with Avaya Aura® Unified Communications Virtualized Environment (VE) voice platform resiliency, you must have a SIP-enabled Contact Center with the following:

- Two Voice Contact Servers configured as a High Availability pair and two Multimedia Contact Servers configured as a High Availability pair.

  OR

  Two Voice and Multimedia Contact Servers configured as a High Availability pair.
- Two or more Avaya Aura® Media Server Linux-based servers, configured as High Availability pairs. Avaya Aura® Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.
- Two Avaya Aura® Unified Communications Virtualized Environment (VE) voice platforms.

  Note:

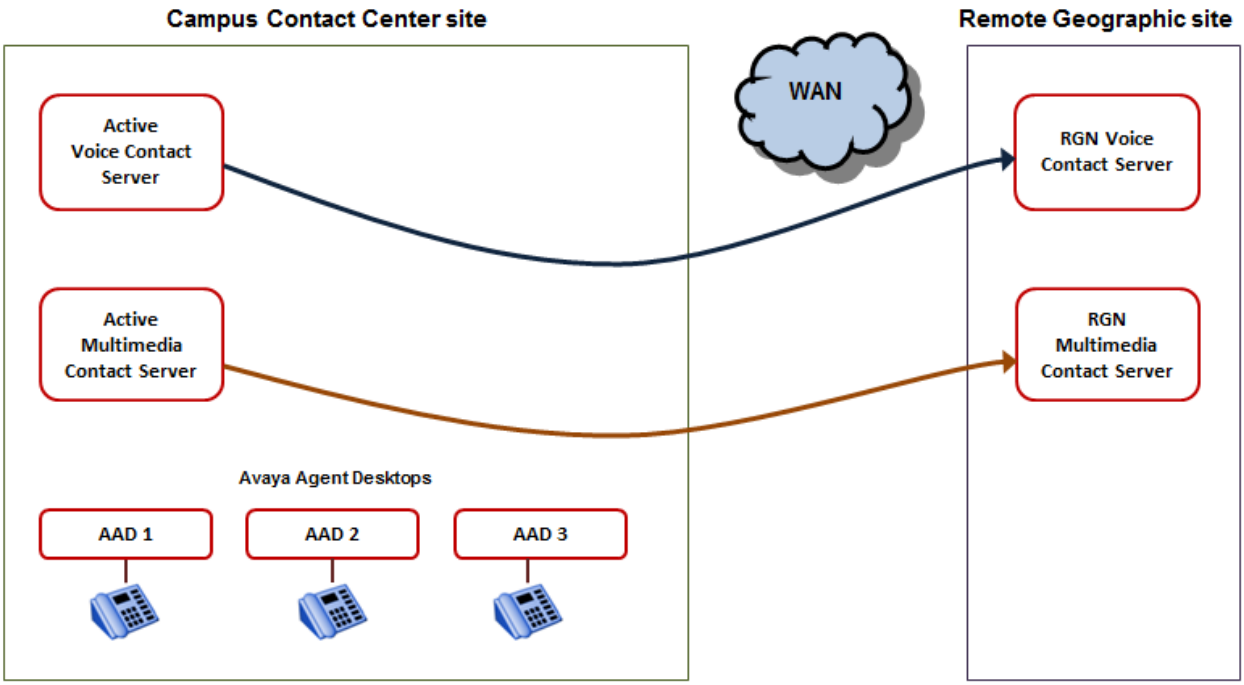
  This solution type provides Contact Center Mission Critical High Availability resiliency, but with limited Avaya Aura® Unified Communications Virtualized Environment voice platform resiliency. This solution uses a single Avaya Aura® Application Enablement Services instance. This Application Enablement Services instance is a single point of failure in the Contact Center solution.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

Geographic High Availability solution

There are two Geographic High Availability solutions:

- Remote Geographic Node server with no HA at the campus
- Remote Geographic Node server with HA at the campus

The following diagram shows an example of a geographic High Availability solution with no HA at the campus. The Remote Geographic Node (RGN) Voice Contact server on the remote geographic site shadows the campus Voice Contact Server. The RGN Multimedia Contact Server shadows the campus Multimedia Contact Server.



Voice Contact Server includes Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), License Manager (LM), and Contact Center Manager Administration (CCMA)

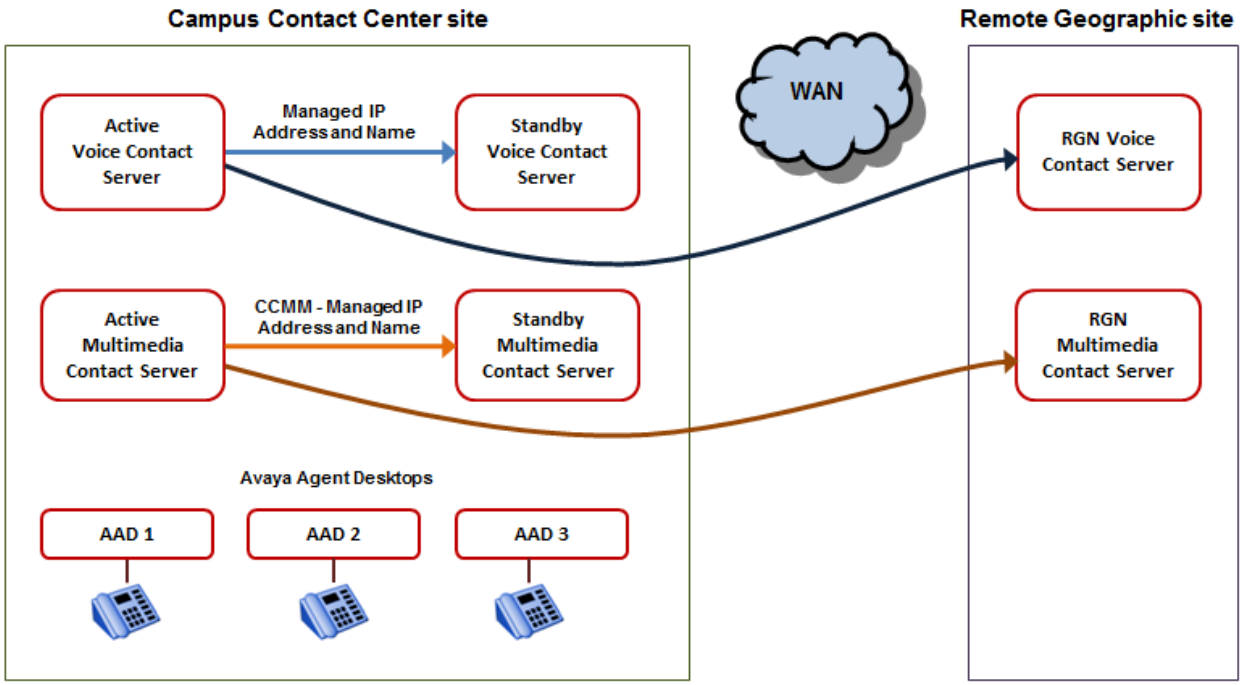
Multimedia Contact Server includes Contact Center Multimedia (CCMM)

AAD Avaya Agent Desktop

RGN Remote Geographic Node

Figure 11: Example of a Geographic High Availability solution with no HA at the campus

The following diagram shows an example of a geographic High Availability solution with HA at the campus. The standby Voice Contact Server shadows the active Voice Contact Server. The standby Multimedia Contact Server shadows the active Multimedia Contact Server. The Remote Geographic Node server on the remote geographic site shadows the active Voice Contact Server on the campus site. The Remote Geographic Node Multimedia Contact Server shadows the active Multimedia Contact Server on the campus site.



Voice Contact Server includes Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), License Manager (LM), and Contact Center Manager Administration (CCMA)

Multimedia Contact Server includes Contact Center Multimedia (CCMM)

AAD Avaya Agent Desktop

RGN Remote Geographic Node

Figure 12: Example of a Geographic High Availability solution with HA at the campus

The main advantages of Geographic High Availability are:

- Support for database shadowing over the WAN.
- Redundancy in the event of a campus site failure.

Geographic High Availability caters for complete campus site failures, that is, a disaster recovery solution. Remote Geographic Node servers do not automatically take over if the campus system fails. You must start the Remote Geographic Node servers manually.

Avaya Aura® Contact Center supports the following geographic High Availability topologies:

- Session Manager and Communication Manager-based solution, with campus active Contact Center server(s), and Contact Center Remote Geographic Node server(s) for data resiliency and disaster recovery.
- Session Manager and Communication Manager-based solution, with campus active and standby Contact Center servers, and Contact Center Remote Geographic Node server(s) for data resiliency and disaster recovery.

Mission Critical High Availability configuration utilities

The Avaya Aura® Contact Center Mission Critical High Availability feature has the following configuration utilities:

- High Availability Utility (Mission Critical High Availability version)
- SMMC system tray

There are two versions of the High Availability Utility, one version for Mission Critical High Availability, and another version for hot-standby High Availability. The Mission Critical High Availability utility works in conjunction with the SMMC system tray.

High Availability Utility (Mission Critical High Availability version)

Configure Mission Critical High Availability resiliency for CCMS, CCT and CCMM using the High Availability (HA) Utility in the Database Utilities. The High Availability Utility configures which server is the active server and which is the standby server. The HA utility also configures the Managed IP for the HA pair.

The High Availability Utility on an active server has the following dialogs under the Configuration tab:

- Server Mode
  - Configure the IP address for the active and standby servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for the optional Remote Geographic Node
  - Identify if the server is active or standby
  - Enable Switchover
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs.
- Notifications
  - Configure an email server for email notifications
  - Configure where and how often to send email notifications
  - Configure the email character set
- System
  - Display information on the system status
  - Verify that database shadowing is running

SMMC system tray

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment. The SMMC system tray has the following main menu options and action items:

- Start HA System
- Stop HA System

- Disable Switchover
- Enable Switchover
- System Information
- Database Information
- Disable Next Auto Startup
- Select Standby Auto Startup Mode (Standby server only)
- Re-enable HA system (this option is available only when the active HA server is running with switchovers disabled)

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar. The SMMC system tray icon displays the status of the High Availability feature on the server.

In the SMMC system tray, the available menu options depend on the state of the HA System. For example, the Start HA menu option is available only when the High Availability system is in a stopped state. The state of critical CCT and CCMS services affects the available SMMC system tray menu options. The state of the License Manager, Avaya Aura® Media Server, CCMA, and CCMM services does not affect the available SMMC system tray menu options.

The Contact Center System Management and Monitoring Component (SMMC) system tray icons display the status of the High Availability feature on a server, whether switchover is enabled or disabled that server, and whether the server can communicate with the High Availability SMMC component on the remote server.

The following table shows the High Availability system status and corresponding SMMC system tray icon.

High Availability status	SMMC icon
Non-HA server in stopped state. High Availability is not configured on this server.	
Non-HA server in starting state. High Availability is not configured on this server.	
Non-HA server in running state. High Availability is not configured on this server.	
Non-HA server in stopping state. High Availability is not configured on this server.	
Active HA server in stopped state. This server is configured as a High Availability active server.	
Active HA server with no connection to a standby system. This server is configured as a High Availability active server.	
Active HA server running with connection to a standby system, fully HA capable system. A switchover is possible.	
Active HA server running, but switchovers disabled. A switchover is not possible.	
Switchover in progress, the active system is switching over to become a standby system. After the switchover, this server becomes a standby server.	
Standby HA server in stopped state. This server is configured as a High Availability standby server.	

High Availability status	SMMC icon
Standby HA server with no connection to an active system. This server is configured as a High Availability standby server.	
Standby HA server running with connection to an active system, fully HA capable system. A switchover is possible.	
Standby HA server running, but switchovers disabled. A switchover is not possible.	
Switchover in progress, the standby system is switching over to become an active system. After the switchover, this server becomes an active server.	
The Geographic standby server HA system is starting.	
The Geographic standby server HA system is stopping.	
The Geographic standby server HA system is stopped.	
The Geographic standby server HA system is shadowing the active server, but the Geographic Standby server is not yet synchronized with the active server.	
The Geographic standby server HA system is shadowing and synchronized with the active server.	

High Availability Utility and SMMC system tray

Use the Mission Critical High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

How to reinstate High Availability resiliency after a switchover

In a Mission Critical campus solution, if the active server fails or if the Contact Center Administrator performs a manual switchover, the standby server starts processing contacts. The initially active server stops (including all services and shadowing), and the High Availability - Enable Switchover option is disabled. The standby server becomes the active server and it continues to process contacts. The High Availability SMTP feature sends an email to the Contact Center Administrator informing them that a switchover occurred. The server that is now active has no corresponding standby server, and the solution is no longer resilient.

When the root cause of the failure has been addressed, the Contact Center Administrator can reinstate High Availability resiliency using the following steps:

- Check whether the switchover was managed or unmanaged. Run the SMMC System Information report on the current standby server, and check the **local last known stop reason**. If the stop reason is Network outage, the switchover was unmanaged.

- If the switchover was unmanaged, or more than 24 hours have elapsed since the switchover:
  - On the currently active running server (previous standby server), run the Database Maintenance utility and back up all database applications to a network share. You do not need to stop the active server to back up the applications.
  - On the currently stopped server (previous active server), ensure that High Availability shadowing is still stopped.

    Use the Database Maintenance utility to restore the Contact Center databases from the network share.

    In the High Availability configuration utility, configure this stopped server to be the standby High Availability server.

    Run Server Configuration to update the local server information to identify the real local IP addresses. Ensure that the License Manager IP address and license type are correct.
- On the active server, start High Availability and enable switchovers.
- On the standby server, start High Availability, enable switchovers, and start shadowing.
- If your HA solution supports multimedia contacts, on the primary Contact Center Multimedia server, restart the CCMM Multimedia Contact Manager service.

In some situations you must perform a backup and restore after a managed switchover caused by a service failure. This can occur, for example, where 24 hours elapse before reinstating HA, or where the database shadow latency was greater than 10 seconds at the time the switchover occurred. In such cases, when you use SMMC to start High Availability on the standby server, Contact Center does not start HA and displays a message that the backup and restore is required.

For more information about these High Availability related procedures, see *Avaya Aura® Contact Center Server Administration*.

How to reinstate High Availability resiliency after a total network outage

During a total network outage, the active and standby servers cannot communicate with each other and/or the Trusted IP address. Because the active server cannot communicate with the Trusted IP address, it stops the Contact Center services. Because the standby server also cannot communicate with the Trusted IP address, it stops the Contact Center services. All Contact Center services on the active and standby servers stop during a total network outage.

When the root cause of the failure is fixed, the Contact Center Administrator can reinstate High Availability resiliency using the following steps.

- Ensure the active and standby servers can communicate with each other and the Trusted IP address.
- Configure the active server to be the High Availability active server.

- Start High Availability on the active server.
- Backup the active server databases and restore them on to the standby server.
- Configure the standby server to be the High Availability standby server.
- On the standby server, use Server Configuration to verify that the standby server details are correct.
- Start High Availability on the standby server.
- Enable switchovers on the active server.

For more information about these High Availability related procedures, see *Avaya Aura® Contact Center Server Administration*.

How to manually switch over to the Remote Geographic Node of a Mission Critical solution

If the High Availability campus site fails or is shut down, you can manually start your Remote Geographic Node solution. During normal operation the Remote Geographic Node (RGN) shadows the campus site database. The RGN is configured to use local voice platform and multimedia resources. The RGN is configured with the same agent and skillset information as the campus site.

In the following example the remote site has an RGN Voice and Multimedia Contact Server, and a single local standalone Avaya Aura® Media Server.

1. On the Remote Geographic Node (RGN), use the System Management and Monitoring Component (SMMC) system tray to stop the High Availability system. This ensures that the Remote Geographic Node server is not shadowing data from the campus site.
2. On the RGN server, using the High Availability configuration utility, select “Temporarily set as non-HA”.
3. On the RGN server, use the SMMC system tray to start Contact Center services.
4. On the RGN server, use the System Control and Monitor Utility (SCMU) to verify that all core Contact Center services started.
5. Log on to the RGN CCMA and confirm that the CCMS, CCT, and CCMM servers have been updated with the RGN server name and IP addresses.
6. On the Avaya Aura® Media Server primary node of the RGN site, on the Element Manager Cluster Configuration - Replication Settings page, clear the 'Master Cluster Primary Node Address' option. This stops the RGN site from attempting to replicate content from the primary Avaya Aura® Media Server data center on the campus site.
7. Log on to the RGN CCMA. From the CCMA Launchpad, select Configuration, and then Media Servers. Ensure that the “Master Content Store” option is selected for the local RGN Avaya Aura® Media Server or the local RGN Avaya Aura® Media Server HA pair.

8. Start Agent Desktop clients using the RGN Voice and Multimedia Contact Server host name.
9. If your Contact Center solution uses an external Web Communications server, configure the Web Communications server to update the files with the RGN server name.
10. If your Contact Center solution uses Proactive Outreach Manager (POM), configure the POM server to point to the RGN server.

The Remote Geographic Node is now commissioned to handle voice and multimedia contacts. The Remote Geographic Node also supports local reporting.

For more detailed information about this outline procedure, see the High Availability chapter in *Avaya Aura® Contact Center Server Administration*.

How to revert to the campus site after running the RGN for a few days

If a Mission Critical High Availability campus site fails or is shut down, you can manually commission and start the Remote Geographic Node solution. You can then use the Remote Geographic Node (RGN) servers until the campus site is available again. When the campus servers are available you must shut down the RGN servers and re-configure High Availability on the campus site. Avaya Aura® Contact Center is out-of-service during this re-configuration period, because the campus HA servers must be re-built with consistent data. This must happen without any configuration or statistical data updates on the RGN server that might not get restored on the new campus HA server.

In the following example the remote site has an RGN Voice and Multimedia Contact Server and a single local standalone Avaya Aura® Media Server.

1. On the Remote Geographic Node (RGN), use the System Management and Monitoring Component (SMMC) system tray to stop the High Availability system.
2. On the RGN server, backup all the application databases and the ADMIN database.
3. On the campus active server, restore the RGN database backups.
4. On the RGN, using the High Availability configuration utility, clear the new "Temporarily set as non-HA" check box. This puts the RGN server back into RGN mode.
5. On the active server, use the SMMC system tray to start the active server.
6. After the campus CCMA server starts up, log on to CCMA. During the first CCMA log on session, CCMA presents a *RGN Information* message box requesting confirmation to change CCMS, CCT, and CCMM server names back to the original campus values. Click Yes to accept the recommended changes.
7. After the active server is up, backup the active server databases and restore them to the standby server and the RGN server. Re-enable and restart High Availability on the standby server and RGN server.

When reverting to the campus site, you must configure Avaya Aura® Media Server content replication settings to allow voice prompt administration to be performed at the primary data center at the campus site. You must also ensure that the voice prompt content replicates to the Avaya Aura® Media Servers at the RGN site.

If you made changes to the voice prompts at the RGN site that now need to be replicated back to the primary data center, you must temporarily force the primary data center Master cluster to replicate content from the RGN Avaya Aura® Media Server or RGN Master cluster. Perform these steps to temporarily force the campus Avaya Aura® Media Servers to replicate from the RGN primary Avaya Aura® Media Server:

1. At the campus site, on the primary data center Avaya Aura® Media Server Master cluster primary node, log on to Element Manager.
2. In Element Manager > Cluster Configuration > Replication Settings, configure the “Master Cluster Primary Node Address” field to the address of the RGN Master cluster primary node.
3. View the Element Status page and wait for any synchronization alarm conditions to clear. This might take a few moments unless you have large volumes of content in your content store. You might not observe alarms if your solution uses small amounts of voice prompt content.
4. View the content for your SIP domain namespace in the Media Management page to confirm that expected updates have replicated successfully.
5. In Element Manager, clear the “Master Cluster Primary Node Address” field. Your Avaya Aura® Media Servers at the campus site now have the same voice prompts as the Avaya Aura® Media Servers at the RGN site.

Perform these steps to configure voice prompt administration at the primary data center at the campus site:

1. At the RGN site, on the Avaya Aura® Media Server primary node of the RGN Master cluster, set the “Master Cluster Primary Node Address” field to the address of the primary data center Master cluster primary node.
2. At the campus site, from the CCMA Launchpad, select Configuration, and then Media Servers. Select the primary Avaya Aura® Media Server or the primary Avaya Aura® Media Server HA pair and ensure that the “Master Content Store” option is selected. This Avaya Aura® Media Server or Avaya Aura® Media Server HA pair now manages the voice prompts in your solution when the campus site is running.

The campus site is now commissioned to handle voice and multimedia contacts. The Remote Geographic Node is shadowing the campus site.

When upgrading a HA-enabled server to Avaya Aura® Contact Center, you must use the HA configuration utility to configure and apply the server mode details again. This reduces the number of steps if you need to switch over from a Remote Geographic Node to a campus solution.

For more detailed information about this outline procedure, see the High Availability chapter in *Avaya Aura® Contact Center Server Administration*.

Avaya Aura® platform campus resiliency

Avaya Aura® Contact Center supports solution High Availability resiliency when using the Avaya Aura® Unified Communications platform. Contact Center provides High Availability application resiliency. The level of Contact Center solution High Availability you can achieve depends on your complete enterprise contact center solution, including the underlying PABX platform. You can configure your contact center solution to have no single point of failure. For improved solution resiliency, the Avaya Aura® Unified Communications PABX platform must be deployed and configured to support High Availability.

Avaya Aura® platform campus resiliency supports the following:

- Communication Manager survivability. For more information, see Communication Manager survivability overview on page 96
- Session Manager redundancy. For more information, see Session Manager redundancy overview on page 96
- Either Application Enablement Services Machine Preserving High Availability (MPHA) or Geographical Redundancy High Availability (GRHA). For more information, see Application Enablement Services Machine Preserving High Availability (MPHA) overview on page 97 or Application Enablement Services Geographical Redundancy Preserving High Availability overview on page 98

High Availability campus site

The following diagram shows a typical High Availability campus site, with the Avaya Aura® Unified Communications platform configured to support platform campus resiliency.

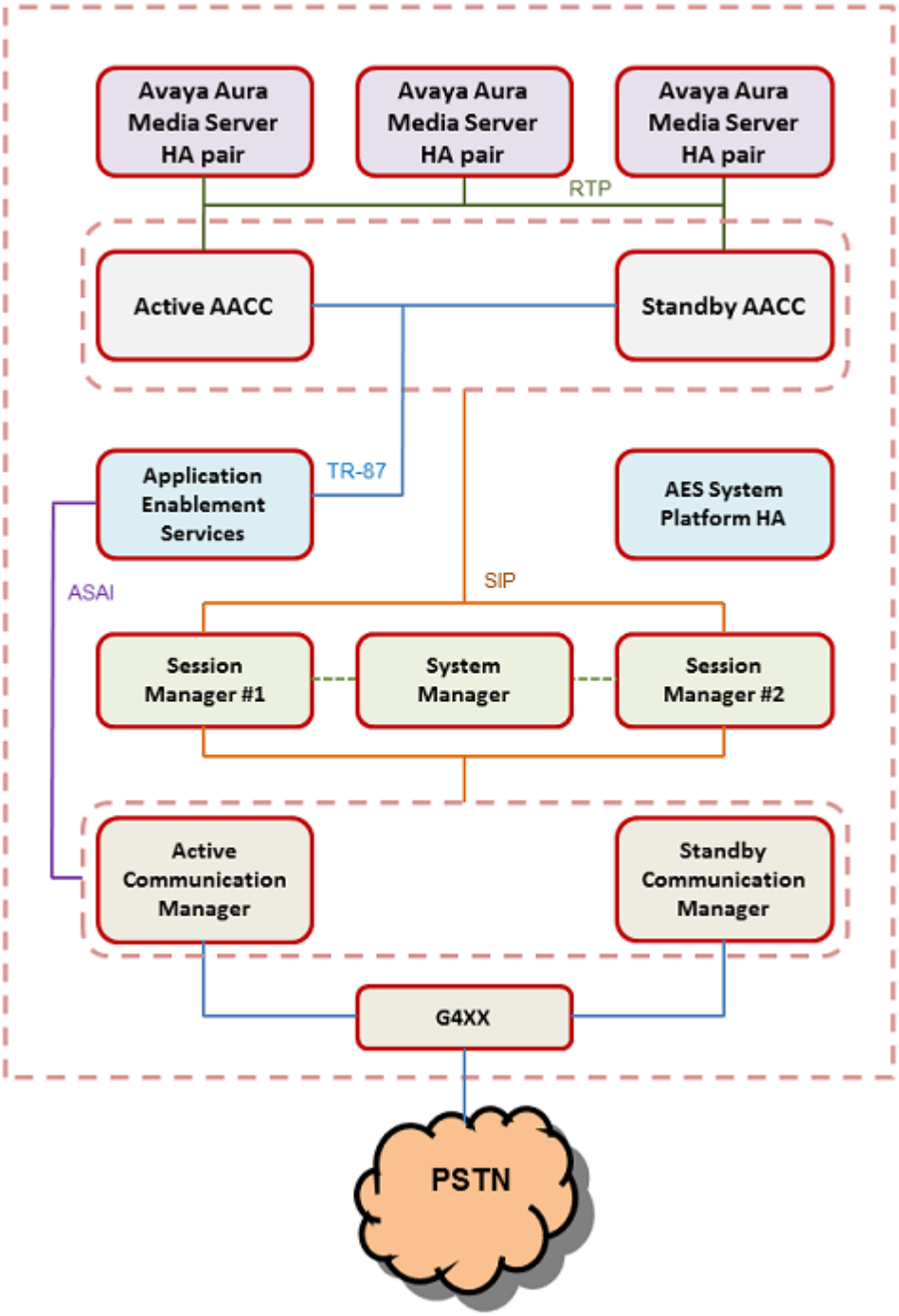


Figure 13: Example of a campus voice-enabled site with platform resiliency

Communication Manager survivability overview

Communication Manager on the Avaya Aura® System Platform supports survivability. Communication Manager survivability typically employs two main Communication Managers, one active Communication Manager and one standby Communication Manager. Both Communication Managers are running but only the active one is processing calls.

Example of Communication Manager campus survivability:

- Two System Platform supported servers with exactly the same hardware configuration.
- Both servers in close proximity, connected with a crossover cable.
- The same version of System Platform installed on the active and standby nodes.
- The Communication Manager Duplex template installed on both System Platforms.
- A Duplication Link exists between both Communication Managers.

For more information about Communication Manager and survivability, see *Avaya Aura® Communication Manager Survivability Options Release 6.0.*

Contact Center experience if a Communication Manager fails

If the active Communication Manager fails the standby Communication Manager starts processing calls. If Avaya Aura® Contact Center is impacted by the Communication Manager switchover, it automatically re-connects and agent functionality continues. Otherwise Avaya Aura® Contact Center continues processing calls without interruption.

Session Manager redundancy overview

Avaya Aura® Session Manager uses the active-active approach where two instances are simultaneously active; any request routes to either instance, and a failure of one of the Session Manager instances does not interrupt new calls. Active-active redundancy requires that the Session Manager instances be interconnected over an IP network with sufficient bandwidth and low enough latency to synchronize runtime data.

Example of Session Manager redundancy:

In the following configuration example, SM-1 is one Session Manager instance, and SM-2 is the active backup. Route-through failover relies on Communication Manager look-ahead routing to choose a secondary route. The route pattern form needs to add the secondary or failover trunk group administration. If you are using load balancing, you do not need additional administration if you reuse the same Port IDs and IP addresses for the added SM-2 trunk group(s).

Add SM-2 as the backup Session Manager server.

- On SM-2, create the entity links that exist on SM-1.
- For route-through failover, add an entity link SM-1 to SM-2.

- Add the trunk setup on your device. For example, if you have a Communication Manager signaling group to SM-1, you need to add a Communication Manager signaling group to SM-2.
- All other administration is accessible to SM-2 automatically. Additional dial plan administration is not necessary.

For more information about Session Manager and Redundancy, see documentation on installing and configuring Avaya Aura® Session Manager.

Contact Center experience if a Session Manager fails

Avaya Aura® Contact Center uses the Session Manager as a SIP voice proxy. If a Session Manager fails, new Contact Center calls are routed by the remaining Session Manager(s) and there is no impact to Avaya Aura® Contact Center functionality. Calls in progress during a Session Manager failure might be impacted and the agent might have to complete the call using their phone.

Application Enablement Services Machine Preserving High Availability overview

Machine Preserving High Availability (MPHA) mode implements a new Virtual Server Synchronization Technology (VSST) offering on System Platform. MPHA is a dual server configuration, which includes an active server and a standby server. Only the active server provides service. System Platform High Availability is a licensed feature, and, if required, you must purchase it when ordering Application Enablement Services.

With MPHA mode, the standby server monitors the active server, and takes over when one of the following conditions occurs on the active server:

- a hardware failure
- a network failure
- a server reboot or server shutdown

Failovers from the active server to the standby server in MPHA mode are not service affecting: that is, the standby server does not need to reboot. The failover from the active server to the standby server is transparent.

Important Considerations

For a sudden hardware failure (uncontrolled), the protected Virtual Machine (VM) on the new active server starts running from its last check pointed state within approximately one second.

For a controlled failover, or if hardware health degrades, the protected VM on the new active server starts running without loss of any data within 500 milliseconds.

Detection of a network failure can take up to 10 seconds, so for network failures the failover takes longer.

MPHA does not protect against AES software failures.

Important:

Avaya Aura® Contact Center does not support the native AES geographic redundancy feature on the campus site. Contact Center supports only a single IP address for the campus SIP Proxy.

MPHA failover requirements

Machine Preserving High Availability failover requires the following:

- Both System Platform servers must have exactly the same hardware configuration.
- Both servers must be in close proximity, within 100 meters. This is to allow a Category 6 crossover cable, suitable for 10Gb Ethernet, can connect them.
- The same version of System Platform must be installed on the active and standby nodes, and both servers must be patched to the same level.

For more information on the MPHA feature, see *Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform 6.3*.

Contact Center experience during the MPHA failover

Contact Center uses AES as a SIP CTI proxy to control Contact Center telephone calls on Communication Manager.

For a manual switchover, power loss, or hardware failure, an AES failover using MPHA is transparent to AACC agents. The agents do not experience any loss of Agent Desktop functionality, or any loss of CTI control messages.

For network failures, the agent can experience a loss of CTI control; this is because detection of network failures takes longer and the MPHA failover does not occur immediately. Agent Desktop displays a message box advising agents to use their desk phones to answer voice contacts. Agents continue to handle Customer voice contacts using their desk phones during the AES service outage. Agents can process Multimedia contacts using Agent Desktop. When the AES services resume, and Contact Center Manager Server regains call control, Agent Desktop displays another message advising agents to use Agent Desktop to handle voice calls.

Note:

For network failures, agents that use Avaya Agent Desktop in the embedded softphone mode, without a desktop phone, cannot process customer calls during an AES outage or switchover.

Application Enablement Services Geographical Redundancy Preserving High Availability overview

Geographical Redundancy High Availability (GRHA) is a partial state preserving HA which supports a virtual IP address. GRHA is a dual server configuration, which includes an active server and a standby server. Only the active server provides services. GRHA works either on System Platform or on VMware implementations of AES. System Platform High Availability is a licensed feature, and, if required, you must purchase it when ordering Application Enablement Services. You can use GRHA to implement AES redundancy either at the campus or to a remote data center.

With GRHA mode, the standby server monitors the active server, and takes over when one of the following conditions occurs on the active server:

- a hardware failure
- a network failure
- a server reboot or server shutdown

Failovers from the active server to the standby server in GRHA mode recreate all sessions. In this way, GRHA is partially state preserving.

Important Considerations

For a sudden hardware failure (uncontrolled), the new active server starts running from its last check pointed state within approximately one minute from the failure detection.

When a controlled failover occurs, AE Services stop on the current active Virtual Machine (VM), and AE Services start on the new active VM (previously the standby VM).

The GRHA failure detection interval determines when the AES standby VM starts in an uncontrolled failover. If the standby VM has not been able to contact the active VM for the failure detection interval, then the standby VM AE Services start. The failure detection interval is configurable, and can be between one second and 60 minutes. Avaya recommends that you set the AES failure detection interval to 20 seconds to support Contact Center High Availability.

GRHA does not protect against AES software failures.

GRHA failover requirements

Geographical Redundancy High Availability failover requires the following:

- Both System Platform servers must have exactly the same hardware configuration or both VMware virtual guests must have exactly the same configuration.
- Both servers must be able to communicate on a network connection with less than 100 ms RTT.
- If you are using System Platform, the same version must be installed on the active and standby nodes, and both servers must be patched to the same level.

For more information on the GRHA feature, see *Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform 6.3*.

Contact Center experience during the GRHA failover

Contact Center uses the AES as a SIP CTI proxy to control Contact Center related phone calls on the Communication Manager. During the GRHA switchover interval, AES services are not available and Contact Center is unable to control or monitor Communication Manager phone calls. Contact Center continues to receive customer calls from the Communication Manager and Session Manager, and it continues to route these calls to agents.

If Contact Center Manager Server is unable to communicate with the AES, Avaya Agent Desktop client software displays a message box advising agents to use their desk phones to answer voice calls. The agents continue to handle Customer calls using their desk phones during the AES service outage. Agents continue processing email messages and IM customer contacts using Agent Desktop software. When AES services resume and Contact Center Manager Server regains call control, Agent Desktop client software displays another message box advising agents to use Agent Desktop to handle voice calls.

Note:

Agents that use Avaya Agent Desktop in the embedded softphone mode, without a desktop phone, cannot process customer calls during an AES outage or switchover.

For network failures, the agent can experience a loss of CTI control; this is because detection of network failures takes longer and the GRHA failover does not occur immediately. Agent Desktop displays a message box advising agents to use their desk phones to answer voice contacts. Agents continue to handle customer voice contacts using their desk phones during the AES service outage. Agents can process Multimedia contacts using Agent Desktop. When the AES services resume, and Contact Center Manager Server regains call control, Agent Desktop displays another message advising agents to use Agent Desktop to handle voice calls.

Avaya Aura® platform geographic resiliency

The Avaya Aura® Unified Communications PABX platform supports resiliency in geographic Wide Area Network (WAN) solutions. For improved solution resiliency the Avaya Aura® Unified Communications PABX platform must be deployed and configured to support campus High Availability. For multi-site enterprises, the Avaya Aura® Unified Communications platform can be deployed and configured to support geographic resiliency and disaster recovery.

Avaya Aura® platform geographic resiliency supports the following:

- Communication Manager Survivable Core (ESS) on page 101
- Session Manager geographical redundancy overview on page 102
- Application Enablement Services geographical redundancy overview on page 102

Campus site and remote geographic site

The following diagram shows a typical campus site and a remote geographic site. The remote geographic site can be used for disaster recovery if the campus site fails.

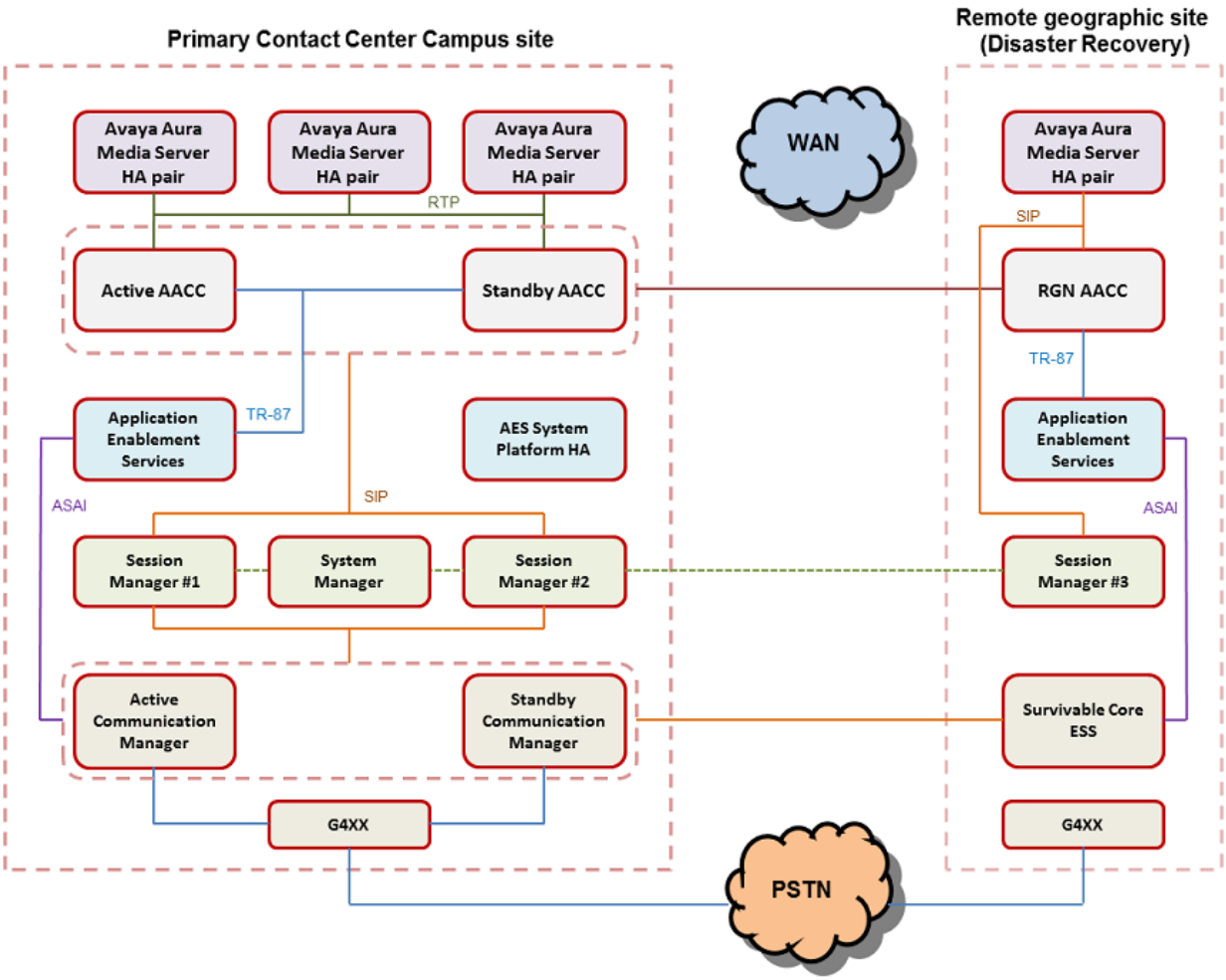


Figure 14: Example of a campus site with a disaster recovery remote geographic site

Communication Manager Survivable Core (ESS)

Communication Manager on the Avaya Aura® System Platform supports survivability. Communication Manager survivability typically employs two main Communication Managers, one active Communication Manager and one standby Communication Manager. Both Communication Managers are in the same campus location and run but only the active one processes calls.

Communication Manager also supports geographical redundancy using a version of a Communication Manager called a Survivable Core.

Install the Survivable Core on the remote geographic site. Using the Communication Manager System Management Interface (SMI), configure the Survivable Core to have a “Server Role” setting of “Enterprise Survivable Server (ESS)”. Then configure the Survivable Core - “Registration address of the main server” setting to be the managed IP address of the Communication Manager Duplex pair on the campus site. On the campus site, if the Active Communication Manager fails

the standby Communication Manager takes over call processing. If both the Active and Standby Communication Managers fail, the Survivable Core on the geographic site can take over some call processing.

For more information about Communication Manager Survivable Core and survivability, see *Avaya Aura® Communication Manager Survivability Options Release 6.0.*

Session Manager geographical redundancy overview

Session Manager uses the active-active approach campus resiliency where two instances are simultaneously active; any request routes to either instance, and a failure of one of the Session Manager instances does not interrupt service. To support geographic resiliency you must install an additional Session Manager on the remote geographic site.

Use Avaya Aura® System Manager to administer all the Session Manager instances in your enterprise. The System Manager stores all the Session Manager configuration details in its own database. The two Session Managers on the campus site and the Session Manager on the remote geographic site share this one System Manager and they are all aware of each other. If one or more of the Session Managers fail the remaining Session Manager can continue routing contacts. If the two Session Managers on the campus site fail, the Session Manager on the remote site can still route contacts.

Avaya Aura® System Manager supports System Platform-based High Availability.

For more information about Session Manager and Redundancy, see documentation on installing and configuring Avaya Aura® Session Manager.

Application Enablement Services geographical redundancy overview

Install an Application Enablement Services (AES) server on the remote geographic site.

The Avaya Aura® Contact Center Remote Geographic Node (RGN) server on the geographic site can then use this local AES server as the local CTI proxy to control calls.

If the campus site fails, calls to it are re-directed to the Session Manager on the remote geographic site. The remote site can also have a local G450 Media Gateway or other PSTN connections routing calls to the local Session Manager. The Contact Center RGN server uses the local AES server to control these calls.

For more information about AES High Availability solutions, see *Implementing Application Enablement Services on Avaya Aura® System Platform.*

Offsite Agent resiliency

The impact of a switchover on an agent using the Offsite Agent feature varies depending on what type of failure caused the switchover.

Avaya recommends that all offsite agents use a Call Presentation Class (CPC) with Return to Queue enabled. This provides the best experience for callers as it ensures that their calls continue to queue even if some component of the contact center fails.

Offsite Agent behavior when the Contact Center server fails

Where a failure occurs on the Contact Center server, both Contact Center Manager Server and Communication Control Toolkit become unavailable.

When the contact center recovers, agents sometimes have to re-connect their Agent Desktop. Agent Desktop clients attempt to re-synchronize automatically.

Agents working in On Demand mode lose call control, but can hang up their telephone to terminate voice contacts.

Agents working in Permanent Connection mode lose all call control, and must rely on customers hanging up to terminate voice contacts.

Offsite Agent behavior when there is a failure of the outbound SIP trunk or the PSTN connection

Where a failure occurs on the outbound SIP trunk, the contact center server still routes calls to the Offsite Agent terminal. This results in the offsite agent receiving call notifications on Agent Desktop, but the voice calls do not come through to the offsite telephone. Since the voice call is not answered, the Return to Queue presentation class redirects the call to the contact center and puts the agent in the Not Ready state.

When the outbound SIP trunk recovers, the offsite agents must put themselves in the Ready state to be able to take calls again.

Chapter 9: Microsoft instant messaging server requirements

SIP-enabled Avaya Aura® Contact Center supports Microsoft Lync Server or Microsoft Skype for Business as an Instant Messaging (IM) and Presence services provider. Avaya Aura® Contact Center can process the IM messages it receives from Microsoft instant messaging servers and route the messages to available Agent Desktop agents.

Avaya Aura® Contact Center supports Microsoft Lync Server Release 2010 and Release 2013, or Microsoft Skype for Business 2015.

When integrated with a Microsoft instant messaging server, Avaya Aura® Contact Center agents can use Instant Messaging to communicate in near real-time with customers, supervisors, and experts. Avaya Aura® Contact Center and Agent Desktop support Microsoft instant messaging servers as Instant Messaging (IM) providers only. Integration with Microsoft instant messaging servers enables Agent Desktop to display presence information for agents and supervisors. This makes it easier for an agent to find an available expert or supervisor when they need to consult a colleague about an IM contact.

Important:

Agent Desktop does not support co-resident installation of Microsoft instant messaging client software.

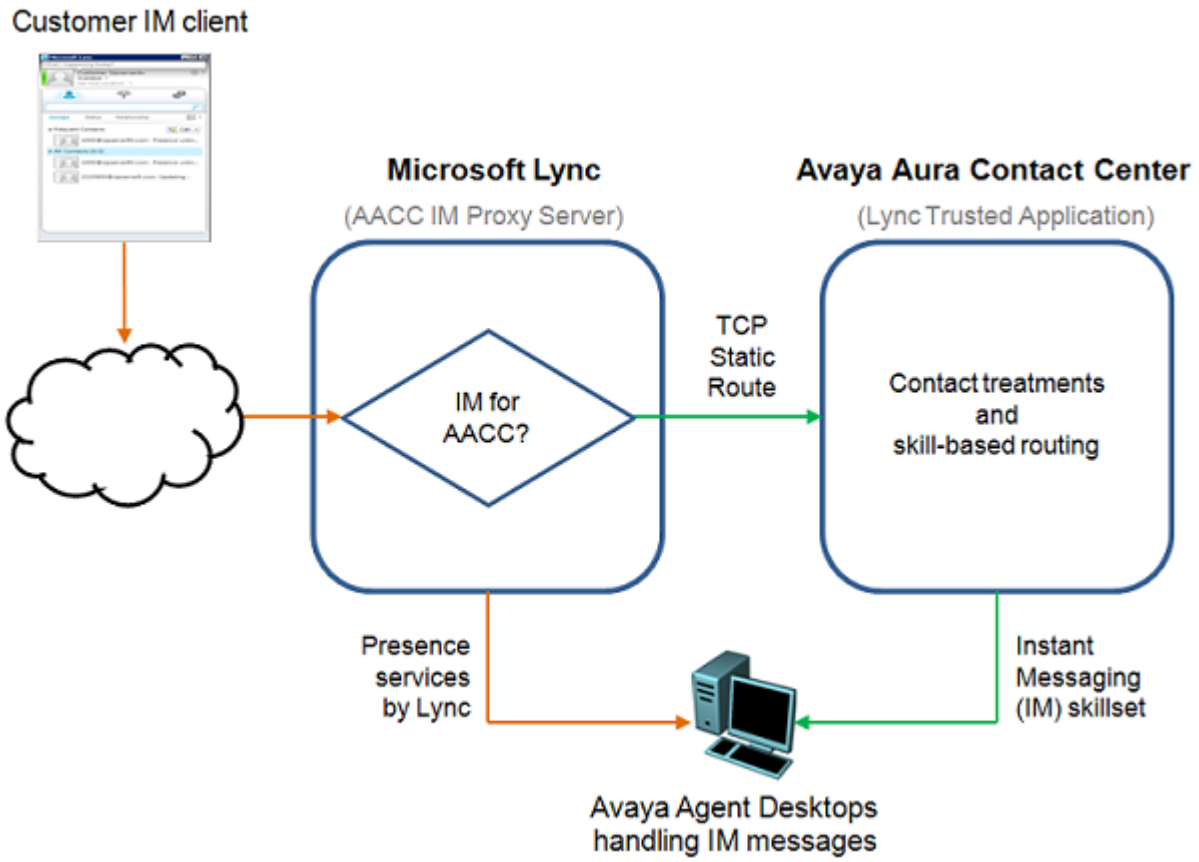


Figure 15: Example of a Microsoft instant messaging deployment with Contact Center, using Microsoft Lync

Avaya Aura® Contact Center uses TCP transport to communicate with Microsoft instant messaging servers. Avaya Agent Desktop uses TLS transport to communicate with Microsoft instant messaging servers.

Note:

Microsoft instant messaging servers require dedicated server. Avaya Aura® Contact Center and Avaya Aura® Media Server do not support co-resident instant messaging servers. For more information about Microsoft instant messaging servers, refer to the Microsoft Lync Server or Microsoft Skype for Business Server product documentation.

Overview of integration

The following is a short overview of how to integrate Avaya Aura® Contact Center and a Microsoft instant messaging server. For more detailed information about the commissioning tasks, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* and *Avaya Aura® Contact Center Client Administration*.

1. Obtain Avaya Aura® Contact Center multimedia Instant Messaging (IM) licenses for the agents and supervisors.
2. Install and commission Microsoft Lync Server of Microsoft Skype for Business Server hardware and software.

3. On the Microsoft instant messaging server, use the Management Shell to define a Trusted Application Pool.
4. Use the Management Shell to create a trusted application for Avaya Aura® Contact Center and add it to the Microsoft instant messaging server Trusted Application Pool.
5. On the instant messaging server, use the Topology Builder to configure the IP address of the Avaya Aura® Contact Center server used by the Microsoft instant messaging server to process Avaya Aura® Contact Center IM contacts.
6. Use the Management Shell to define a static route from the Microsoft instant messaging server to Avaya Aura® Contact Center. Apply a Match URI type filter to the static route, so only IMs matching the Avaya Aura® Contact Center requirements are routed to Avaya Aura® Contact Center for treatment.
7. Use the Management Shell to enable a TCP port so Avaya Aura® Contact Center and the Microsoft instant messaging server can communicate with each other.
8. Configure an Active Directory Windows user account for each agent, supervisor, and expert. The Microsoft instant messaging server must be installed in this Active Directory domain.
9. Using the instant messaging server Control Panel – Users page, search for the Active Directory Windows user accounts, and enable each account for Microsoft Lync or Microsoft Skype for Business, and then configure the SIP address for each account.
10. Using the CCMS Server Configuration utility, configure the Microsoft instant messaging server as the IM Proxy Server.
11. In CCMA, configure supervisors and agents using the above Active Directory Windows user accounts, (now enabled for Microsoft instant messaging support), and assign the agents to an IM skillset.
12. When Agent Desktop agents log on, they enter the user account details that have been enabled for Microsoft instant messaging services support. Agent Desktop agents can then handle routed IM contacts. Agents can also use peer-to-peer IM and Presence services to contact each other, supervisors, and experts.

Licensing requirements

When integrating Avaya Aura® Contact Center and either Microsoft Lync Server or Microsoft Skype for Business Server, Contact Center has no additional licensing requirements other than those normally needed for a multimedia contact center with the IM contact type enabled.

Chapter 10: Avaya Aura® Presence Services requirements

This section describes the requirements for integrating Avaya Aura® Presence Services to provide instant messaging services to support the Instant Message contact type.

Avaya Aura® Presence Services overview

Avaya Aura® Contact Center allows customers to use Avaya Aura® Presence Services to provide instant messaging services to support the Instant Message contact type.

Customers integrating their multimedia Contact Center with Avaya Aura® Presence Services get the additional benefit of providing rich presence information to their agents using Agent Desktop.

Integration with Avaya Aura® Presence Services enables Agent Desktop to display presence information for agents and supervisors. This increases an agent's success in finding an available expert or supervisor when they need to consult a colleague about an IM contact.

Integration with Avaya Aura® Presence Services is available only in a SIP-enabled contact center based on the supported Avaya Aura® platforms.

Important:

The Avaya Aura® Presence Services IM Proxy Server - XMPP Domain name must be different from the Avaya Aura® Contact Center Local SIP Subscriber - Domain Name entry.

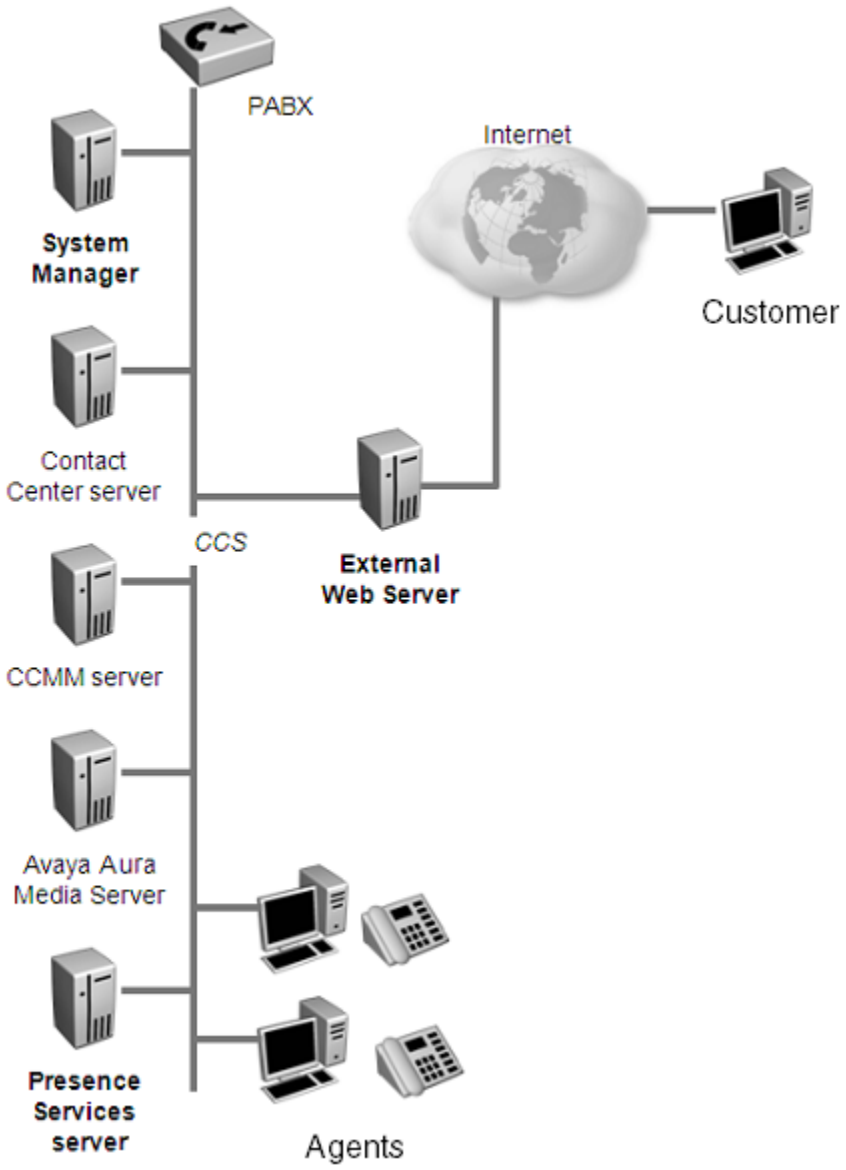


Figure 16: Avaya Aura® Presence Services server deployment

Avaya Aura® Presence Services requires a dedicated server and cannot co-reside with Avaya Aura® Contact Center or Avaya Aura® Media Server. Avaya provides extensions to the Extensible Messaging and Presence Protocol (XMPP) to allow customers to develop applications to establish IM chat sessions with Contact Center, and disconnect them.

To integrate Avaya Aura® Presence Services server with Contact Center, you must develop an application that allows customers to send Instant Messages to the contact center.

Note:

If your solution uses Avaya Aura® Presence Services 7.1 or later, you must ensure that the SIP Network Transport communication protocol is set to TLS in Server Configuration.

Hardware requirements

Apart from the server requirements for both Avaya Aura® Presence Services and Avaya Aura® System Manager, Contact Center has no additional hardware requirements outside those normally needed for a multimedia contact center with the IM contact type enabled.

For 3000 Multimedia agents (the contact center maximum), the contact center requires a single Avaya Aura® Presence Services server.

Operating system requirements

Avaya Aura® Presence Services requires the Linux operating system. See documentation about implementing Avaya Aura® Presence Services.

For integrating Avaya Aura® Presence Services, Contact Center has no additional operating system requirements outside those normally needed for a multimedia contact center with the IM contact type enabled.

Licensing requirements

For integrating Avaya Aura® Presence Services, Contact Center has no additional licensing requirements outside those normally needed for a multimedia contact center with the IM contact type enabled.

High Availability

The Avaya Aura® Presence Services integration does not support Contact Center High Availability. During a Contact Center switchover, in-progress IM contacts are interrupted.

Index

A

about Presence Services 107
about Unified Communications platform 23
AD-LDS 17
agent
    Whisper Coaching 19
Agent Desktop
    integration with Enterprise Web Chat 16
application intrinsics 41
application sequencing 59
application variables 41
assignment parameter limits 36
attachments in email storage 44
Avaya Aura Experience Portal 55
Avaya Call Park and Page Snap-in 18
Avaya Media Server 16
Avaya Real-Time Speech Snap-in 18
Avaya Smart Caller ID Inbound Snap-in 18
Avaya Smart Caller ID Outbound Snap-in 18
Avaya WebRTC Snap-in 18

B

Barge-in and Observation tone 16

C

Caché database 17
Call Control XML 57
Call Force Answer Zip Tone 16
Call Recording 25
call resources limits 36
capacities 36
capacity 36
capacity outbound contact centers 44
CCMM
    database files 43
CCSA 16
CCXML 57
Click-to-Dial 25
compatibility for switches in SIP 47
components 30
Contact Center Services 16
converting protocols 49
CSTA interfaces 23

D

database files
    CCMM 43
database parameter limits 36
Data transfer 56
digital signal processors 49
disk storage requirements for multimedia 43
DNIS 51, 52

E

Elite 19
Elite Complement 21
email 42
email attachment storage 44
Experience Portal 66, 69

F

features 7.0 Feature Pack 1
    Agent Desktop integration with Enterprise Web Chat 16
    Whisper Coaching 19

G

Geographical Redundancy High Availability 98
geographic resiliency 100

H

H.323 60
hardware requirements Presence Services 109
High Availability
    Machine Preserving 97

I

Instant Messaging 104
integration
    Agent Desktop with Enterprise Web Chat 16
intended audience 9
IP voice protocol 48

L

licensing 53
Licensing 106

M

Machine Preserving High Availability 97
MBT 20
Microsoft Lync 104
Microsoft Skype for Business 104
Midsize Business Template 20

Mission Critical 78
Mission Critical HA without platform resiliency 81
Mission Critical HA with platform resiliency 80
Mission Critical High Availability 80
overview 74
Mission Critical High Availability configuration utilities 87
multimedia disk storage 43
multimedia email attachment storage 44

N

networking parameter limits 36
network outage 90
No Switch Configured 21

O

Observation tone 16
Offsite Agent
resiliency 103
operating system requirements Presence Services 109
outbound capacity 44
overview
Offsite Agent 33

P

P-header 58
P-Intrinsics 58
Presence Services 107
Presence Services hardware requirements 109
Presence Services operating system requirements 109
Private Header 58

R

real-time display parameter limits 36
related documentation 9
Remote Geographic Node 91, 92
requirements CCMM disk storage 43
requirements Presence Services hardware 109
requirements Presence Services operating system 109

S

Screen Pop 58
Service-Oriented Architecture 60
SES 20
Session Initiation Protocol 57
Session Manager 52
SGM 57
SIP 57
SIP Domain 29
SIP feature limitations 46
SIP Gateway Manager 57
SIP in Unified Communications platform 23
SIP Network Components 27
SIP session expiry parameters 47
SIP signaling 59
SIP switch compatibility 47
support 14
Survivable Core 101
switch compatibility SIP 47
switchover
reinstate High Availability resiliency 89
Switchover 78
Switchover Handling Script 76
switch processing 49

T

third-party interface limits 36

U

Universal Call Identifier 60
UUI 59, 60

V

VE 83
videos 13
Voice XML 57
VoIP 48
VXML 57

W

Web communications limits 36
Whisper Skillset 16