Avaya Aura® Contact Center Overview and Specification

Release 7.0.2
Issue 01.05
November 2017

© 2015-2017, 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. 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 Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License 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 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

Introduction

This document provides a technical description of Avaya Aura® Contact Center. This document describes the product features, specifications, licensing, and interoperability with other supported products.

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 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.	Customers and sales, services, and support personnel
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	Customers and sales, services, and support personnel

Title	Use this document to:	Audience
	document also describes the features and functional limitations of certain configurations.	
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
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

Title	Use this document to:	Audience
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 optional configuration procedures for server configuration.	System administrators
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	System administrators and support personnel

Title	Use this document to:	Audience
	installing service packs, and maintaining the databases for the Contact Center system.	
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

Related resources

Training

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 changes in Avaya Aura® Contact Center Release 7.0.

Feature changes in the Release 7.0 base build

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

Agent Desktop inter-operation with Avaya Co-Browsing Snap-in

Avaya Aura® Contact Center supports inter-operation between Agent Desktop and Avaya Co-Browsing Snap-in.

Agents engaged with a customer on a voice contact or web chat contact can initiate a Co-Browsing session by starting their browser, navigating to an Avaya Co-Browsing Snap-in URL, and generating a Co-Browsing session. The agent sends the session key to the customer, for example by calling it out in a voice call or copying it into a web chat message. The customer can join the session, and both agent and customer can utilize the Co-Browsing features.

There is no requirement for a license or any configuration in Avaya Aura® Contact Center to support inter-operation with the Avaya Co-Browsing Snap-in. You must provision and license a separate EDP stack to use Avaya Co-Browsing Snap-in.

Automatic insertion of a leading digit before dialing numbers using Agent Desktop Phonebook

In Contact Center Release 7.0, administrators can configure a setting that gives agents the ability to automatically add a leading digit before dialing of any number using Agent Desktop Phonebook. If

administrators enable this feature, the plus sign (**+**) before the phone numbers in Phonebook is replaced with a trunk access code. The trunk access code is added before the phone number. Therefore, agents do not need to manually add a leading digit to call externally or forward a call using Phonebook.

Avaya Aura® Contact Center Ignition Wizard

Avaya Aura® Contact Center Release 7.0 introduces a configuration utility called the Ignition Wizard. After you install Avaya Aura® Contact Center software, you use the Ignition Wizard to configure the initial networking, locale, administration, and licensing solution details.

If you know the contact center solution details, you can run the Ignition Wizard directly after installing the Avaya Aura® Contact Center software. Alternatively, you can install the Avaya Aura® Contact Center software and then defer running the Ignition Wizard until you know the solution details. This gives you the flexibility to install the server software and then, at a later date or different location, configure the solution details.

You must use the Ignition Wizard to initialize Avaya Aura® Contact Center, otherwise Avaya Aura® Contact Center is not operational.

Avaya Aura® Contact Center supports Microsoft Windows Server 2012 R2

Avaya Aura® Contact Center Release 7.0 is supported on the Microsoft Windows Server 2012 R2 operating system. 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.

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.

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 Agent Browser application

Contact Center Release 7.0 includes an Agent Browser application. Voice-only Contact Center agents can use the Agent Browser application to log on to Contact Center and perform basic tasks. The Agent Browser application is supported in SIP-enabled Contact Center solutions only.

Contact Center Manager Administration password expiry

In Contact Center Release 7.0, administrators can configure that the password used for Contact Center Manager Administration (CCMA) expires after a specified duration. By default, the CCMA password expiry feature is disabled.

If administrators enable the password expiry feature, by default the CCMA password expires after 30 days and CCMA also displays a CCMA password expiry warning 14 days prior to password expiry. Administrators can configure both the expiry period and the password expiry warning duration using the CCMA Security Settings dialog.

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.

Contact Center services secured by default

The Contact Center Release 7.0 base build includes a number of services and connections that you can secure using Transport Layer Security (TLS). By default, Contact Center installs commonly used Web services and CTI connections with security enabled. This feature includes enhancements to the Contact Center Certificate Management tool to make it easier to manage server and root certificates.

On a new Contact Center install, the following connections and services use TLS by default:

- Contact Center Manager Administration (CCMA)
- Contact Center Multimedia (CCMM) Administration
- Agent Desktop

- Multimedia Services
- Orchestration Designer
- Outbound Campaign Management Tool
- Contact Center Web Services
- Communication Control Toolkit (CCT) Web Administration

You can turn off Web services security after installation and initial configuration. If you choose to leave Web Services security enabled, replace the Contact Center default security store with a new security store containing a signed server certificate and root certificate from your Certificate Authority (CA).

Crystal Reports replacement with Microsoft SQL Server Reporting Services

In Avaya Aura® Contact Center Release 7.0, Microsoft SQL Server Reporting Services (SSRS) replaces Crystal Reports as the historical reporting presentation engine. Avaya Aura® Contact Center Release 7.0 retains the full set of historical report templates previously available.

Avaya Aura® Contact Center Release 7.0 supports Report Creation Wizard (RCW), and customers can migrate existing RCW generated reports based on Crystal Reports to Avaya Aura® Contact Center Release 7.0 SSRS-based templates.

Custom reports built outside of RCW, for example using Crystal Designer, cannot be migrated to Avaya Aura® Contact Center Release 7.0. You can either manually recreate these custom reports in SSRS format, or use an external Crystal instance, which you provide, with the AACC database views.

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.

Emergency license expiry notification

When an emergency license is provided to a customer, a daily Windows event is generated. The Windows event warns the customer of the number of days left for the emergency license to expire. Customers can then address the situation in which the Avaya customer service representative provided the emergency license, before the emergency license expires. For example, if your Avaya customer service representative activates the emergency license file on your system because the

connection between Contact Center License Manager and Contact Center Manager Server cannot be fixed within the 30-day grace period, then you can use the emergency license to re-establish the connection between Contact Center License Manager and Contact Center Manager Server.

Force password change when users log on to Contact Center Manager Administration for the first time

In Contact Center Release 7.0, administrators can configure a setting, using the CCMA Security Settings dialog, that forces users to change their password when they log on to Contact Center Manager Administration (CCMA) for the first time. In Contact Center Release 7.0, the force password change feature is disabled by default.

For fresh installations of Contact Center Release 7.0 Feature Pack 1, CCMA security settings are enabled by default. If you are upgrading from Contact Center Release 7.0 version, your existing CCMA security settings do not change.

Passwords must not match the previous password and must contain the following:

- Only English and special characters
- 8 to 20 characters
- A number
- An uppercase letter
- A lowercase letter
- No spaces

New Avaya Aura® Contact Center minimum hardware specifications

Avaya Aura® Contact Center Release 7.0 continues to support Platform Vendor Independence (PVI) for physical server hardware deployments. Avaya Aura® Contact Center Release 7.0 defines three new minimum levels of hardware specification; a new Entry-level, a new Mid-range, and a new High-end server hardware specification. For Avaya Aura® Contact Center Release 7.0 installations on physical servers, only the new PVI server hardware specifications are supported.

New Avaya Aura® Contact Center minimum virtual machine specifications

Avaya Aura® Contact Center Release 7.0 continues to support VMware and virtualization. Avaya Aura® Contact Center Release 7.0 defines three new minimum levels of virtual machine specification; a new Entry-level, a new Mid-range, and a new High-end virtual machine specification.

For virtualized Avaya Aura® Contact Center Release 7.0 installations on virtual machines, only the new virtual machine specifications are supported.

Password aging in Contact Center Manager Administration

Password aging protects organizations from malicious users gaining unauthorized access to Contact Center, because a stolen password is useful to the intruder only for a limited time.

Contact Center Release 7.0 contains a setting that implements password aging for Contact Center Manager Administration (CCMA).

In Contact Center Release 7.0, the password aging feature is disabled by default. If administrators enable the password aging feature, by default the maximum password age is set to 30 days. Users must change the passwords for CCMA when the maximum password age is reached. Administrators can configure the maximum password age for CCMA using the CCMA Security Settings dialog.

For new installations of Contact Center Release 7.0 Feature Pack 1, Contact Center Manager Administration (CCMA) security settings are turned on by default. If you are upgrading from Contact Center Release 7.0, your existing CCMA security settings are not modified.

Serviceability enhancements in Contact Center 7.0

The following are the serviceability enhancements in Contact Center 7.0:

- Upgraded third-party controls in Agent Desktop
- Enhanced security in Contact Center Manager Administration
- Prevention of Orchestration Designer flow application changes until all Contact Center services start

Support for adding company images and logos to signatures

Contact Center Release 7.0 supports adding company images and logos to email signatures and automatic email signatures. Automatic signatures are automatically added at the bottom of an outgoing email message.

Support for copying the CLID of a customer using Agent Desktop

In Contact Center Release 7.0, the agents can use the **Copy CLID** button on the Agent Desktop toolbar to copy the Calling Line Identification (CLID) number of a customer to the clipboard. Agents can copy the telephone number of the caller when administrators configure Agent Desktop to display the name of the caller using the contacts directory integration.

For incoming calls, Agent Desktop copies the value of the AD_CLID intrinsic when agents click the **Copy CLID** button. For outgoing calls, Agent Desktop copies the value of the CALLED_NUMBER intrinsic when agents click the **Copy CLID** button.

Note:

Agents can copy the CLID of a customer using Agent Desktop only for voice calls in a SIP-enabled Contact Center.

Support for displaying login history in Contact Center Manager Administration, Agent Desktop, and Security Manager

In Contact Center Release 7.0, Contact Center Manager Administration, Agent Desktop, and Security Manager display the date and time of your last login. Contact Center Manager Administration and Security Manager also displays the number of failed login attempts before a successful login. With the number of failed attempts, users can identify whether a malicious user tried to log in with their credentials after the last successful login.

By default the login history out feature is disabled. Administrators can enable this feature using the CCMA Security Settings dialog.

Support for forced Not Ready reason codes

In Contact Center Release 7.0, administrators can configure a setting that forces agents and supervisor/agents to enter a Not Ready reason code when changing their status to Not Ready.

Note:

The default code or no code applies when Contact Center returns the contact to a queue because the contact has not been answered within the presentation class guidelines set for the agent.

When a logged in agent exits Agent Desktop by clicking X in the Top bar, the agent goes into the Default Not Ready state.

Support for Remote Geographic Node server with no HA at the campus

In SIP solutions on the Avaya Aura® Unified Communications (UC) platform, Contact Center no longer requires High Availability (HA) at the campus to support a Remote Geographic Node (RGN) server. An RGN server on a remote geographic site can shadow a single server at the campus, for data resiliency and disaster recovery.

Support for scripting using CLID and Wild CLID in SIP environments

Contact Center Release 7.0 supports scripting using Calling Line ID (CLID) and Wild CLID intrinsics when creating workflows or scripts for a SIP deployment.

Support for up to 3000 Web chat sessions with EWC

Customers who require large numbers of Web chat sessions can use the Avaya Aura® Contact Center Enterprise Web Chat (EWC) SDK instead of Web Communications. Use EWC if your requirement is greater than the maximum number of supported CCMM Web Communications chat sessions. EWC can support up to 3000 simultaneous Web chat sessions.

Temporary lock out of Contact Center Manager Administration users

In Contact Center Release 7.0, administrators can configure a setting which temporarily locks out Contact Center Manager Administration (CCMA) users, if users incorrectly enter the application password a specified number of times.

In Contact Center Release 7.0, the temporary lock out feature is disabled by default,. If administrators enable the temporary lock out feature, by default users can incorrectly enter the password three times before CCMA locks the user account for three minutes. Administrators can configure both the number of times that the users can enter an incorrect password and the lock out period using the CCMA Security Settings dialog.

For new installations of Contact Center Release 7.0 Feature Pack 1, Contact Center Manager Administration(CCMA) security settings are turned on by default. If you are upgrading from Contact Center Release 7.0 version, your existing CCMA security settings are not modified.

Upgrade to Avaya one-X® Agent Release 2.5.5 in Agent Desktop

Contact Center Release 7.0 upgrades the Avaya one-X® Agent version from Release 2.5 to Release 2.5.5 in Agent Desktop. Agent Desktop uses Avaya one-X® Agent in the *My Computer* mode as an embedded softphone.

Important:

Avaya one-X® Agent Release 2.5.5 does not support Windows 8.1 and Windows 10.

Web Services security enhancements

Release 7.0 includes multiple enhancements to improve the security of Web Services.

Prevent Cross Site Tracing

Contact Center disables the methods that allow Cross Site Tracing, to remove this vulnerability.

Web server version disclosure

Contact Center no longer responds to requests with the Web server version. This prevents a common probe used to determine the Web server version, so that attackers can exploit known vulnerabilities for that server version.

User Interface Redress prevention

It is no longer possible to embed the Contact Center Manager Administration (CCMA) pages in forms, and this reduces the vulnerability to UI Redress attacks. UI Redress attack is a malicious technique that tricks a Web user into clicking something different from what they think they are clicking.

Implement strong cipher support for WebLM service

Contact Center implements only up-to-date strong ciphers for WebLM embedded in the Contact Center Tomcat instance. Obsolete and redundant ciphers are no longer available for secure communications.

Tomcat directory listing disabled

Contact Center disables the directory listing attribute in the Tomcat instance. This prevents the possibility of an attacker traversing the directory structure.

Feature changes in Release 7.0 Feature Pack 1

See the following sections for information about new features in Release 7.0 Feature Pack 1.

Ability to run Avaya one-X® Communicator concurrently with Avaya Agent Desktop

From Release 7.0 Feature Pack 1, Contact Center administrators can disable the Avaya Agent Desktop embedded softphone either on a per agent basis or on a system-wide basis. When the administrators disable the embedded softphone, Avaya one-X® Communicator can run concurrently with Avaya Agent Desktop.

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.

Agent Desktop uses a user directory as the default file browsing directory

From Release 7.0 Feature Pack 1, Contact Center changes the default directory that Agent Desktop uses for file browsing to a user directory instead of a system directory. Browsing files using a user directory ensures that agents cannot browse to a hidden drive such as `C:\` and improves security on a workstation. A user directory is the directory that Agent Desktop opens by default, if an agent has defined a default attachment folder. If an agent has not defined a default attachment folder or if the default attachment folder no longer exists then by default Agent Desktop opens the `Documents` folder on the client computer.

Automated backup of new security store

From Release 7.0 Feature Pack 1, Contact Center automatically backs up a new security store when you create it. This allows you to recover from situations where the store is damaged or deleted before you make a manual backup of the store.

Automatic refreshing of non-staffed skillsets for Real-time Reporting

From Release 7.0 Feature Pack 1, Contact Center Manager Administration Real-Time Reporting automatically refreshes every 20 seconds the list of non-staffed skillsets with the most recent information.

Contact Center implements Transport Layer Security version 1.2 by default

From Release 7.0 Feature Pack 1, Contact Center implements Transport Layer Security (TLS) version 1.2 as the default minimum version negotiated for secure communications. This is to avoid security vulnerabilities that exist in TLS 1.0.

Before migrating to Release 7.0 Feature Pack 1, ensure that the browsers you use for CCMA or Element Manager are configured to use TLS 1.2.

For backward compatibility and inter-operation with third-party or custom applications connecting to Contact Center, Administrators can set lower versions of TLS on certain communication channels. When a lower version of TLS is available, Contact Center still negotiates the highest level of TLS that the other application can support.

Before migrating from a previous Release, or before applying Feature Pack 1 to a Release 7.0 solution, check third-party or custom applications that connected securely to Contact Center, to understand whether you need to change the Contact Center TLS versions.

If you apply Feature Pack 1 to an existing Release 7.0 installation, Contact Center does not apply this change, and retains your Release 7.0 TLS configuration.

Contact Center supports Proactive Outreach Manager integration only with Release 3.0.4

From Release 7.0 Feature Pack 1, Contact Center supports Proactive Outreach Manager integration only with POM Release 3.0.4. The integration with POM is not backward compatible. If you are currently using POM to provide outbound contacts in Contact Center Release 7.0, you must upgrade your POM server to Release 3.0.4 before you apply Feature Pack 1.

Contact Center supports Proactive Outreach Manager in HA and NCC solutions

From Release 7.0 Feature Pack 1, Contact Center supports Proactive Outreach Manager (POM) in Avaya Aura® Contact Center High Availability (HA) and Network Contact Center (NCC) solutions.

Contact Control Service SDK

From Release 7.0 Feature Pack 1, Contact Center includes the Contact Control Service SDK. This SDK builds on the capabilities of existing Contact Center APIs by adding support for outbound voice calls in solutions that integrate Proactive Outreach Manager (POM). The Contact Control Service

SDK supports the Java programming language. You can develop custom clients for Contact Center using the Contact Control Service SDK.

Database Integration Wizard configuration moved to Contact Center database

From Release 7.0 Feature Pack 1, Contact Center stores configuration information for the Database Integration Wizard (DIW) in the Contact Center database. The standard Contact Center backup includes this information, so you no longer back up the DIW configuration separately.

When you migrate from an earlier release of Contact Center, you must back up the Database Integration Service configuration from the registry in the normal way. After you restore this configuration to the registry on the new server, Contact Center automatically copies the configuration into the database on the next restart.

Embedded web browsers in Agent Desktop use the latest version of Internet Explorer installed on the client system

From Release 7.0 Feature Pack 1, Contact Center checks and uses the latest version of Internet Explorer, up to Internet Explorer 11, installed on the client system for embedded web browser in Agent Desktop. Agent Desktop checks the version of Internet explorer installed on your system and forces all embedded browsers used in Agent Desktop to use the installed version up to Internet Explorer 11. Using the latest Internet Explorer version, enables screen pops to render better and you can also take advantage of HTML5.

File extension restrictions for attachments

From Release 7.0 Feature Pack 1, Contact Center administrators can use the Contact Center Multimedia (CCMM) Administration utility to configure the supported list of file extensions that agents can attach to emails. When agents add a file attachment to an email, Agent Desktop displays the configured list of file attachment extensions in the Open dialog box. If the attachment type is not in the configured list, Agent Desktop displays a warning message and does not attach the file to the email.

Improved operational performance for High Availability

From Release 7.0 Feature Pack 1, Contact Center improves the operational performance of High Availability. This results in moving the standby server shadow journal database files to the database journal partition.

This change does not impact the minimum partition size of the database journal drive.

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.

Modify chat transcripts of Enterprise Web Chat

From Release 7.0 Feature Pack 1, Contact Center administrators can modify chat transcripts of Enterprise Web Chat (EWC) before the transcripts are saved to the Multimedia database.

Creating filters is the responsibility of the customers and a sample filter is provided as part of the EWC SDK. Administrators can configure EWC to use a transcript filter created by the customer. The transcript filter can be used to modify the transcript to mask sensitive data such as account details, credit card numbers, or personal identification numbers. The transcripts are associated with the customer record whose email sent the chat request.

New application for installing Feature Packs and Service Packs

From Release 7.0 Feature Pack 1, Contact Center includes a new application, Release Pack Installer (RPI), for installing Feature Packs and Service Packs.

Feature Pack and Service Pack ZIP files include the Release Pack Installer (RPI) executable. The RPI ensures that you do not need to manually un-install software patches before upgrading Contact Center. It also ensures that third party software updates remain consistent, and facilitates roll-back to a previous patch lineup.

Multimedia account passwords must meet minimum complexity criteria

From Release 7.0 Feature Pack 1, Contact Center requires multimedia accounts to meet the minimum password complexity criteria. If you are an agent or supervisor who handles multimedia contacts, Agent Desktop forces you to change your password if you log on using the default password or your password that does not meet the minimum password complexity criteria.

Passwords must fulfill the following complexity criteria:

- Must be between 8 to 20 characters
- Must contain a number
- Must contain at least one uppercase letter and at least one lowercase letter

- Must not contain spaces
- Must not contain any of these characters: \ & : < > |

Agents can change the multimedia account password using the **Preferences** tab in the User Preferences screen. Administrators also can change multimedia account passwords using the Multimedia Administration utility.

Provision of adding a friendly name for a web chat agent

From Release 7.0 Feature Pack 1, Contact Center administrators can add a friendly name or nickname for a web chat agent. If administrators configure the Friendly Name label, the nickname of the web chat agent is displayed in agents' responses to web chat messages. Administrators can also choose that the friendly name is displayed in welcome messages.

Removal of the default Agent Desktop Dashboard password

From Release 7.0 Feature Pack 1, Contact Center has removed the default password that was required to access Agent Desktop Dashboard. You can collect and upload log files or videos to the Contact Center server without entering a password.

Second Avaya WebLM server to support High Availability solutions

From Release 7.0 Feature Pack 1, Contact Center supports implementing a second Avaya WebLM server to improve licensing support in virtualized High Availability (HA) Contact Center solutions.

Release 7.0 customers can currently use a virtualized Avaya WebLM server in non-HA deployments to license multiple Avaya products including AACC. With Feature Pack 1, customers must implement a second Avaya WebLM server to support implementing either a campus HA solution or a Remote Geographic Node (RGN) disaster recovery solution.

Skillset list sorted when creating a billboard display

From Release 7.0 Feature Pack 1, Contact Center sorts the skillset list alphabetically when you create a billboard display. The skillset drop-down list is grouped by contact type and then sorted alphabetically within the contact type group.

Supervisors can change prompts with new Announcement Recorder

From Release 7.0 Feature Pack 1, Contact Center includes a new Announcement Recorder application. The Announcement Recorder is a Telephony User Interface (TUI) that supervisors and supervisor agents can use to change prompts used in Contact Center flows.

This feature requires that you license and configure Agent Greeting. Supervisors and supervisor agents that want to use the application must be enabled for Agent Greeting.

Upgrade to Avaya one-X® Agent Release 2.5.8 in Agent Desktop

Contact Center Release 7.0.1 upgrades the Avaya one-X® Agent version from Release 2.5.5 to Release 2.5.8 in Agent Desktop. Agent Desktop uses Avaya one-X® Agent as an embedded softphone in *My Computer* mode.

Avaya one-X® Agent Release 2.5.8 supports Windows 8.1 and Windows 10.

VMware 6.0 support

From Release 7.0 Feature Pack 1, Contact Center supports virtualized environments on VMware 6.0. There is no change to the virtual server specifications required to run Contact Center on VMware 6.0.

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.

Feature changes in Release 7.0 Feature Pack 2

See the following sections for information about new features in Release 7.0 Feature Pack 2.

Agent Desktop integrated login

From Release 7.0 Feature Pack 2, agents no longer need to login separately to CCMM. Agent Desktop authenticates users based on their Windows session credentials only. If your Windows session credentials do not match your CCT user credentials, Agent Desktop prompts you to authenticate using your CCT user credentials.

Agent skillset assignment guardrails

From Release 7.0 Feature Pack 2, you cannot run the same agent skillset assignment concurrently. You must wait until the assignment completes before you run it again. This prevents a potential CCMA performance impact.

Contact Center supports Proactive Outreach Manager integration with Release 3.0.5 and 3.1

From Release 7.0 Feature Pack 2, Contact Center supports Proactive Outreach Manager integration only with POM Release 3.0.5 or 3.1. The integration with POM is not backward compatible. If you are currently using POM to provide outbound contacts in Contact Center Release 7.0, you must upgrade your POM server to Release 3.0.5 or 3.1 before you apply Feature Pack 2.

Increased CCMM customer contact ratio

From Release 7.0 Feature Pack 2, the customer to contact ratio in Contact Center Multimedia (CCMM) has been increased to 1:1000 (or 1 customer record per 1000 contacts).

Offline Security Store

From Release 7.0 Feature Pack 2, you can create an offline store using Security Manager. This allows you to minimize downtime if you want to replace your current security store. When your offline store is created, you can swap between the active store and the offline store. You can make the offline store the active store at any point using Security Manager. You must stop Contact Center services before making the offline store active.

Remote Desktop Services support for Agent Desktop

From Release 7.0 Feature Pack 2, Contact Center supports using Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop.

Removal of default security configuration

From Release 7.0 Feature Pack 2, for new installations Contact Center no longer provides a default security store and default security certificates. At the installation stage, you can now use the Ignition Wizard to create a security store, generate a Certificate Signing Request (CSR) and import a Certificate Authority root certificate. Alternatively, you can choose to skip security configuration at the installation stage and configure your security certificates later in the commissioning process using Security Manager.

REST API integration

From Release 7.0 Feature Pack 2, Contact Center allows you to invoke REST API in a Contact Center workflow. REST (Representational state transfer) provides efficient scalable services for web communications.

A Contact Center workflow can request data using scripting commands, and the workflow uses the TfeRestService to request and retrieve data from the REST API.

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.

VMware 6.5 support

From Release 7.0 Feature Pack 2, Contact Center supports virtualized environments on VMware 6.5. There is no change to the virtual server specifications required to run Contact Center on VMware 6.5.

Other changes in the Release 7.0 base build

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

Agent Desktop no longer supports deployment as a thick client

From Release 7.0, Contact Center does not support deployment of Agent Desktop as a thick client. You can deploy Agent Desktop using either the click-once deployment or an MSI file.

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.

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® Contact Center Hardware Appliance no longer available

Avaya Aura® Contact Center Release 7.0 is not available as a Hardware Appliance.

You can use the Avaya Aura® Contact Center Release 7.0 DVD to build a variety of contact centers, including the Avaya Aura® Unified Communications based contact center solution formerly implemented by the Hardware Appliance.

Avaya Aura® Contact Center no longer supports AMD processors

Avaya Aura® Contact Center Release 7.0 is not supported on servers or VMware hosts with Advanced Micro Devices (AMD) processors. Avaya Aura® Contact Center Release 7.0 is supported only on servers or VMware hosts with Intel processors.

Avaya Aura® Contact Center OVA file no longer available

Avaya Aura® Contact Center Release 7.0 is not available as an Open Virtual Appliance (OVA) file. You can use the Avaya Aura® Contact Center Release 7.0 DVD or ISO image to build a range of VMware virtual machines. Avaya Aura® Contact Center continues to support VMware virtualization, productivity, efficiency, and flexibility. Avaya Aura® Contact Center Release 7.0 supports integration with the Avaya WebLM Release 7.0 and Avaya Aura® Media Server Release 7.7 OVAs.

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 IQ is no longer supported

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

Avaya Remote Agent Observe is no longer supported

Avaya Communication Server 1000 and AML-based Avaya Aura® Contact Center Release 7.0 does not support Avaya Remote Agent Observe.

SIP-enabled Avaya Aura® Contact Center Release 7.0 and Agent Desktop continue to support the Supervisor Observe feature. The Supervisor Observe feature is integrated into Avaya Aura® Contact Center and Agent Desktop; it does not require additional hardware.

Avaya Voice Portal integration is no longer supported

Avaya Aura® Contact Center Release 7.0 does not support integration with Avaya Voice Portal. Avaya Aura® Contact Center supports integration with Avaya Aura® Experience Portal.

CCMA report formats and options no longer supported

In Avaya Aura® Contact Center Release 7.0, Microsoft SQL Server Reporting Services (SSRS) replaces Crystal Reports as the historical reporting presentation engine. This results in CCMA no longer supporting some report formats and export options.

Ad-hoc report export formats

CCMA no longer supports the following ad-hoc report export formats:

- Crystal Reports (RPT)
- Microsoft Excel Data Only
- Microsoft Word – Editable
- Rich Text Format (RTF)
- XML

Scheduled report export formats

CCMA no longer supports the following scheduled report export formats:

- Crystal Reports Format (*.rpt)
- Excel Data Only Format (*.xls)
- Editable Rich Text Format (*.rtf)
- Rich Text Format (*.rtf)
- XML Format (*.xml)
- Comma Separated Format (*.csv)
- Character Separated Format (*.csv)
- Tab Separated Format (*.tsv)
- Text Format (*.txt)
- HTML Format (*.html)
- HTML 4.0 Format (*.html)
- Record Style Format (*.rs)

Ad-hoc report export page range and number of records

CCMA no longer supports selecting a range of pages when exporting an ad-hoc report. CCMA exports all pages.

CCMA no longer supports ad-hoc reports that pull more than 50,000 records from the database. CCMA blocks such reports. This maximum limit safeguards the memory and CPU usage on the Avaya Aura® Contact Center server. Avaya recommends that you run reports with selection criteria that reduce the amount of data on the report.

Parameter reports

CCMA no longer supports Parameter reports. In previous versions, users can import custom reports as Parameter reports. These reports cannot be scheduled; they allow the user to type or select from a list of available values to filter the report data.

Contact Summary report no longer supports links to Activity Code or Observe and Barge-In data

CCMA no longer supports the ability to click a link on an ad-hoc Contact Summary report to see the Activity Code and Observe and Barge-In data associated with a contact.

Knowledge Worker server type no longer supported

Avaya Aura® Contact Center Release 7.0 does not support the Knowledge Worker server type. Customers with an existing Knowledge Worker solution can migrate to an Avaya Aura® Contact Center Release 7.0 Voice and Multimedia Contact Server or a Voice Contact Server.

Microsoft Exchange Server supported versions

Contact Center Release 7.0 does not support Microsoft Exchange Server 2003. Contact Center Release 7.0 supports only Microsoft Exchange Server 2007, Microsoft Exchange Server 2010, and Microsoft Exchange Server 2013.

Microsoft Internet Explorer releases no longer supported

Contact Center Release 7.0 does not support Microsoft Internet Explorer releases 8.0 or 9.0. Contact Center Release 7.0 supports only Microsoft Internet Explorer 10.0 (32-bit version only), and 11.0 (32-bit version only).

Microsoft Office Communications Server integration is no longer supported

Avaya Aura® Contact Center Release 7.0 does not support integration with Microsoft Office Communications Server (OCS). SIP-enabled Avaya Aura® Contact Center supports integration with Microsoft Lync and Avaya Aura® Presence Services.

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.

Offsite Agent is no longer supported on the Avaya Communication Server 1000 platform

Avaya Aura® Contact Center Release 7.0 does not support Offsite Agent on the Avaya Communication Server 1000 platform.

SIP-enabled Contact Center supports Offsite Agent, using the Avaya Aura® Unified Communication platform Telecommuter mode feature.

Secure Sockets Layer communications is no longer supported

Contact Center Release 7.0 does not support Secure Sockets Layer (SSL) for secure connections. Contact Center supports only Transport Layer Security (TLS). This is to remove security vulnerabilities that exist in SSL.

Third-party or custom applications connecting to Contact Center must support TLS 1.0 or later. Removal of support of SSL can have implications for existing third party or custom applications.

Before migrating from a previous Release, check third-party or custom applications that connected securely to Contact Center, to ensure that these applications support TLS.

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.

SER Predictive Outbound no longer supported

Avaya Aura® Contact Center Release 7.0 does not support integration with SER Predictive Outbound solutions. If your solution requires predictive dialing capabilities, you can integrate Avaya Aura® Contact Center with Avaya Proactive Outreach Manager.

SIP-enabled CS1000 integration is no longer supported

Avaya Aura® Contact Center Release 7.0 does not support integration with SIP-enabled Avaya Communication Server 1000 (CS1000).

You can migrate from SIP-enabled Avaya Communication Server 1000 solutions to Avaya Aura® Contact Center Release 7.0 on the Avaya Aura® Unified Communications voice platform.

Other changes in Release 7.0 Feature Pack 1

See the following sections for information about other changes in Release 7.0 Feature Pack 1.

Avaya Aura® Media Server update

Contact Center Release 7.0 Feature Pack 1 includes an update to Avaya Aura® Media Server. The most recent release includes a change to streaming music, which impacts the configuration when you apply Feature Pack 1.

Contact Center security improvements

From Release 7.0 Feature Pack 1, Contact Center introduces additional security improvements to keep current with the latest standards in the industry. These improvements include restrictions to web services access, locking down of user accounts, and changes to the way Contact Center

manages passwords and keys. Many of these improvements are internal to Contact Center operation and have no impact on end-user operations.

Any security improvement that is visible to end users, or changes the way in which users work with Contact Center, has a separate topic in this section.

iceAdmin Windows account privileges reduced

From Release 7.0 Feature Pack 1, Contact Center reduces the Windows privileges of the CCMA Administration account, iceAdmin. This is to improve security by restricting iceAdmin to the minimum Windows privileges required for managing CCMA.

This reduction in privileges changes the way you configure network printers for CCMA reports.

Server Message Block signing enabled on Windows Server 2012

From Release 7.0 Feature Pack 1, both the Contact Center DVD and the Release Pack installer modify the Windows Server 2012 local group policy to enable Server Message Block (SMB) signing. SMB signing places a digital tag into each server message block, which helps prevent man-in-the-middle attacks on network file sharing.

If you do not want to use SMB signing, you can disable it by modifying the Windows Server 2012 local group policy.

Third-party components updated

Release 7.0 Feature Pack 1 upgrades the Contact Center Tomcat and Java third-party components to recent versions. This improves security and ensures that Contact Center remains current with recent updates.

The Release Pack Installer automatically updates these components.

Other changes in Release 7.0 Feature Pack 2

See the following sections for information about other changes in Release 7.0 Feature Pack 2.

CCMA users must login before changing password

From Release 7.0 Feature Pack 2, CCMA users must login before changing their password. When changing a password in CCMA, users can now change the password of the currently logged in user only.

Installation account for Contact Center install

From Release 7.0 Feature Pack 2, you can use any account with local administrative rights to install Contact Center, provided that you disable the Admin Approval Mode security feature on the Contact Center server. You can also use any account with local administrative rights to upgrade and patch Contact Center; you do not need to always use the same administrative account to perform these tasks.

Third-party components updated

Release 7.0 Feature Pack 2 upgrades a number of third-party components to recent versions, such as Caché, Contact Center Tomcat, and .NET Framework. This improves security and ensures that Contact Center remains current with recent updates.

The Release Pack Installer automatically updates these components.

Part 1: Overview

Chapter 3: Avaya Aura® Contact Center feature description

This section describes Avaya Aura® Contact Center Release 7.0 features, components, servers, and solutions.

Avaya Aura® Contact Center supports the following platforms and solution types:

- SIP-enabled Avaya Aura® Unified Communications platform.
- AML-based Avaya Communication Server 1000. Application Module Link (AML) is an internal protocol used by Avaya Aura® Contact Center to communicate directly with Avaya Communication Server 1000 (CS 1000).

Avaya Aura® Contact Center features the following server types:

Voice and Multimedia Contact Server — Install this server to provide context sensitive and skill-based routing for customer voice and multimedia contacts. This server provides routed contact support for email messages, web communications, voice mail messages, scanned documents, fax messages, and SMS text messages. Each SIP-enabled Voice and Multimedia Contact Server requires one or more Avaya Aura® Media Servers in the contact center solution. Avaya Aura® Media Server supports SIP-enabled voice contact routing, and it provides conference and Agent Greeting capabilities in SIP-enabled contact centers. A Voice and Multimedia Contact Server has the following components:

- Contact Center Manager Server
- Contact Center License Manager
- Contact Center Manager Server Utility
- Contact Center Manager Administration
- Communication Control Toolkit
- Contact Center Multimedia
- Optional Avaya Aura® Media Server Windows version (only in SIP-enabled solutions)

In a small to medium solution using a Voice and Multimedia Contact Server, agents download and install Agent Desktop software from the Voice and Multimedia Contact Server.

Voice Contact Server Only — Install this server to provide context sensitive and skill-based routing for customer voice contacts. Each SIP-enabled Voice Contact Server requires one or more Avaya Aura® Media Servers in the contact center solution. Avaya Aura® Media Server supports SIP-

enabled voice contact routing, and it provides conference and Agent Greeting capabilities in SIP-enabled contact centers. A Voice Contact Server has the following components:

- Contact Center Manager Server
- Contact Center License Manager
- Contact Center Manager Server Utility
- Contact Center Manager Administration
- Communication Control Toolkit

In a solution where agents use Agent Desktop to log on and handle customer calls, each Voice Contact Server requires one Multimedia Contact Server. In a SIP-enabled voice contact center solution, agents must use Agent Desktop to log on and handle customer calls. Therefore each SIP-enabled voice solution using a Voice Contact Server also requires one Multimedia Contact Server. In an Avaya Communication Server 1000 AML-based voice-only solution, where agents use Agent Desktop to log on and handle customer calls, each Voice Contact Server requires one Multimedia Contact Server. In an Avaya Communication Server 1000 AML-based voice-only solution, where agents use their desk phones to log on and handle customer calls, and where the agents do not use Agent Desktop, a Multimedia Contact Server is not required.

Multimedia Contact Server Only — Install this server to increase the number of contact center agents in your enterprise solution. When installed, this server provides the multimedia contact processing capabilities, and the Voice Contact Server processes only voice contacts. In a solution using a Multimedia Contact Server, agents download and install Agent Desktop software from the Multimedia Contact Server. Administrators configure Agent Desktop features and functions using the CCMM Administration utility installed on the Multimedia Contact Server.

A Multimedia Contact Server has the following components:

- Contact Center Multimedia (CCMM)

Network Control Center Server Only — Install this server to add networking, network skill-based routing, and consolidated reporting support for a number of Voice and Multimedia Contact Servers operating as a single distributed contact center. Use this server to configure contact routing between the Voice and Multimedia Contact Server nodes of a distributed contact center solution. A Network Control Center Server has the following components:

- Contact Center Manager Server
- Contact Center License Manager
- Contact Center Manager Administration

Avaya Aura® Media Server on Linux — Install this server to provide additional media processing capabilities, and to support Avaya Aura® Media Server High Availability. Avaya Aura® Media Server supports SIP-enabled voice contact routing, and it provides conference and Agent Greeting capabilities in SIP-enabled contact centers. Avaya Aura® Media Server High Availability is not supported on the Windows operating system. Each SIP-enabled Contact Center requires one or more Avaya Aura® Media Servers. For small to medium contact centers without High Availability, choose a server type with co-resident Avaya Aura® Media Server for Windows. For large contact centers, or contact centers requiring High Availability, install one or more standalone Avaya Aura® Media Server Linux-based servers.

Contact Center components

The Contact Center application suite consists of the following main components:

- Contact Center Manager Server (CCMS)—The core contact center component, which provides intelligent call routing.
- Avaya Aura® Media Server—This is a software based media processing platform for the Contact Center.
- Contact Center Manager Administration (CCMA)—A component that provides browser-based access to the contact center for administrators and supervisors.
- Contact Center License Manager (LM)—A component that provides centralized licensing and control of all Contact Center suite components and features across the Contact Center suite.
- Contact Center Manager Server Utility—A component used to monitor and maintain Contact Center Manager Server activity.
- Network Control Center (NCC) server (optional)—The server in a Contact Center Manager network that manages the Network Skill-Based Routing (NSBR) configuration and communication between servers.
- Communication Control Toolkit (CCT)—A client/server application that helps you implement Computer Telephony Integration for installed and browser-based client integrations.
- Contact Center Multimedia (CCMM) —A contact center application that provides multimedia contact support.
- Orchestration Designer (OD)—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 client components

The Contact Center client components consist of the following components:

- Contact Center Manager Client—Client PCs used to administer the server and to monitor contact center performance using a browser-based interface. The number of these computers is usually proportional to the number of agents in the contact center.
- Avaya Agent Desktop—Agent Desktop is a single-interface client application used by contact center agents to interact with customers. Agent Desktop agents can respond to customer contacts through a variety of media, including phone, outbound contacts, email, Web communication, Fax messages, voice mail messages, scanned documents, SMS text messages, social networking, and instant messaging.
- Agent Browser application—Voice-only Contact Center agents can use the Agent Browser application to log on to Contact Center and perform basic tasks such as logging on or off, changing status, or setting codes.

Installation configurations

The Avaya Aura® Contact Center DVD installer supports a range of server types. Each server type installs a combination of Avaya Aura® Contact Center components suitable for a specific contact center function.

The following table lists the server types supported by each voice platform:

Voice platform	Server type	Components
SIP-enabled Avaya Aura® Unified Communications platform	Voice and Multimedia Contact Server without Avaya Aura® Media Server	• Contact Center Manager Server • Contact Center License Manager • Contact Center Manager Server Utility • Contact Center Manager Administration • Communication Control Toolkit • Contact Center Multimedia
	Voice and Multimedia Contact Server with Avaya Aura® Media Server	• Contact Center Manager Server • Contact Center License Manager • Contact Center Manager Server Utility • Contact Center Manager Administration • Communication Control Toolkit • Contact Center Multimedia • Avaya Aura® Media Server Windows version
	Voice Contact Server Only	• Contact Center Manager Server • Contact Center License Manager • Contact Center Manager Server Utility • Contact Center Manager Administration • Communication Control Toolkit
	Multimedia Contact Server Only	• Contact Center Multimedia
	Avaya Aura® Media Server on Linux	• Avaya Aura® Media Server on Linux
AML-based Avaya Communication Server 1000	Voice and Multimedia Contact Server	• Contact Center Manager Server • Contact Center License Manager • Contact Center Manager Server Utility • Contact Center Manager Administration • Communication Control Toolkit • Contact Center Multimedia

Voice platform	Server type	Components
	Voice Contact Server Only	• Contact Center Manager Server • Contact Center License Manager • Contact Center Manager Server Utility • Contact Center Manager Administration • Communication Control Toolkit
	Multimedia Contact Server Only	• Contact Center Multimedia
All voice platform types	Network Control Center Server Only	• Contact Center Manager Server • Contact Center License Manager • Contact Center Manager Administration

Select the server types appropriate for your voice platform, required features, and required maximum agent count. To use Avaya Aura® Contact Center High Availability, you must install additional Contact Center servers.

Each Avaya Aura® Contact Center server type requires one server. Avaya Aura® Contact Center server types are not supported co-resident with each other on the same server.

Server types and server specifications overview

The following table summarizes the supported Avaya Aura® Contact Center deployments for each server type. The table shows which server specification each Avaya Aura® Contact Center server type requires when installed on a physical server or on a virtual machine.

Table 1: Supported server specifications for each server type

Server type	Voice platform - PABX	Physical server			Virtual machine		
		Entry-level server	Mid-range server	High-end server	Entry-level virtual machine	Mid-range virtual machine	High-end virtual machine
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	No	Yes	Yes	No	No	No
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	No	Yes	Yes	No	Yes	Yes
	CS 1000	No	Yes	Yes	No	Yes	Yes
Voice Contact Server Only	Aura SIP	Yes	Yes	Yes	Yes	Yes	Yes
	CS 1000	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia Contact Server Only	Aura SIP	Yes	Yes	Yes	Yes	Yes	Yes
	CS 1000	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia Contact Server Only – Enterprise Web Chat	Aura SIP	No	Yes	Yes	No	Yes	Yes
Network Control Center Server	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Avaya Aura® Media Server standalone on Linux	Aura SIP	No	Yes	Yes	No	Note 1	Note 1
Avaya Aura® Contact Center software appliance	Aura SIP	N/A	N/A	N/A	No	No	Yes
• **Note 1:** Virtualized Avaya Aura® Media Server is supported only on a 4 vcpu or 8 vcpu virtual machine.							

Installation configurations for Avaya Aura® Unified Communications platform

Each SIP-enabled Avaya Aura® Contact Center solution based on the Avaya Aura® Unified Communications platform must contain the following:

- One Voice and Multimedia Contact Server with Avaya Aura® Media Server. This server type is suitable for small to medium contact centers not using High Availability. [Requires one Contact Center Windows server.]

  OR

- One Voice and Multimedia Contact Server without Avaya Aura® Media Server and one or more Avaya Aura® Media Server on Linux servers. These server types are suitable for small to medium contact centers not currently using High Availability. [Requires one Contact Center Windows server, and one or more Contact Center Linux servers.]

  OR

- Two Voice and Multimedia Contact Servers without Avaya Aura® Media Server and two or more Avaya Aura® Media Server on Linux servers. These server types are suitable for small to medium contact centers using High Availability. [Requires two Contact Center Windows servers, and two or more Contact Center Linux servers.]

  OR

- One Voice Contact Server, one Multimedia Contact Server, and one or more Avaya Aura® Media Server on Linux servers. These server types are suitable for large contact centers not currently using High Availability. [Requires two Contact Center Windows servers, and one or more Contact Center Linux servers.]

  OR

- Two Voice Contact Servers, two Multimedia Contact Servers, and two or more Avaya Aura® Media Server on Linux servers. These server types are suitable for large contact centers using High Availability. [Requires four Contact Center Windows servers, and two or more Contact Center Linux servers.]

The following server type is optional:

- Optional Network Control Center Server Only. [Requires one Contact Center Windows server.]

Supported Avaya Aura® Media Server and Avaya WebLM deployment options

SIP-enabled Avaya Aura® Contact Center requires one or more Avaya Aura® Media Server for media processing. Avaya Aura® Contact Center uses Avaya WebLM for license management.

The following table shows an overview of the Avaya Aura® Media Server and Avaya WebLM deployment options supported by each of the SIP-enabled Avaya Aura® Contact Center server type.

Table 2: Supported Avaya Aura® Media Server and WebLM deployment options

Server type	Platform Support		Avaya Aura® Media Server			Avaya WebLM	
	Physical or virtual	Supported	Co-resident on Windows	Physical Linux	Virtual Linux VMware	Local WebLM license file	VE Avaya WebLM server
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Physical	Yes	Yes	No	No	Yes	Yes
	VMware	No	N/A	N/A	N/A	N/A	N/A
	Hyper-V	No	N/A	N/A	N/A	N/A	N/A
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Physical	Yes	No	Yes	Yes	Yes	Yes
	VMware	Yes	No	Yes	Yes	Yes	Yes
	Hyper-V	Yes	No	Yes	No	No	Yes
Voice Contact Server Only	Physical	Yes	No	Yes	Yes	Yes	Yes
	VMware	Yes	No	Yes	Yes	Yes	Yes
	Hyper-V	Yes	No	Yes	No	No	Yes
Multimedia Contact Server Only	Physical	Yes	N/A	N/A	N/A	N/A	N/A
	VMware	Yes	N/A	N/A	N/A	N/A	N/A
	Hyper-V	Yes	N/A	N/A	N/A	N/A	N/A
Network Control Center Server	Physical	Yes	N/A	N/A	N/A	Yes	Yes
	VMware	Yes	N/A	N/A	N/A	Yes	Yes
	Hyper-V	Yes	N/A	N/A	N/A	No	Yes

- The Multimedia Contact Server obtains licenses from the Voice Contact Server. The Voice Contact Server obtains licenses from the local license file or from a VE Avaya WebLM server.

AML-based Avaya Aura® Contact Center does not require or use Avaya Aura® Media Server or Avaya WebLM.

Installation configurations for Avaya Communication Server 1000 platform

Each AML-based Avaya Aura® Contact Center solution using the Avaya Communication Server 1000 platform must contain the following:

- One Voice and Multimedia Contact Server. This server type is suitable for small to medium contact centers not currently using High Availability. [Requires one Contact Center Windows server.]

  OR
- Two Voice and Multimedia Contact Servers. These server types are suitable for small to medium contact centers using High Availability. [Requires two Contact Center Windows servers.]

  OR
- One Voice Contact Server and one Multimedia Contact Server. These server types are suitable for large contact centers not currently using High Availability. [Requires two Contact Center Windows servers.]

  OR
- Two Voice Contact Servers and two Multimedia Contact Servers. These server types are suitable for large contact centers using High Availability. [Requires four Contact Center Windows servers.]

The following supported server type is optional:

- Optional Network Control Center Server Only. [Requires one Contact Center Windows server.]

Avaya Aura® Contact Center Software Appliance deployment option

Avaya Aura® Contact Center Release 7.0 offers a software appliance package for small to medium sized solutions virtualized using VMware. The Avaya Aura® Contact Center software appliance package consists of the following components:

- Avaya Aura® Contact Center virtual machine
- Avaya Aura® Media Server OVA
- Avaya WebLM OVA

These components integrate with an Avaya Aura® Unified Communications platform to build a SIP-enabled contact center solution.

You can use a single Open Virtual Appliance (OVA) package to distribute a virtual appliance. For example, an Avaya Aura® Media Server OVA package includes all of the Open Virtualization Format (OVF) information required to create an Avaya Aura® Media Server virtual appliance on a VMware

host. A virtual appliance contains a preinstalled, preconfigured operating system and an application stack optimized to provide a specific set of services. The Avaya Aura® Media Server and Avaya WebLM OVAs are prepackaged and ready for deployment.

For the Avaya Aura® Contact Center virtual machine, you build a suitably specified virtual machine and then install *Voice and Multimedia Contact Server without Avaya Aura® Media Server* software from the Avaya Aura® Contact Center DVD or ISO image.

Avaya Aura® Contact Center domain and workgroup support

The following specifies Avaya Aura® Contact Center (AACC) support for Windows (Active Directory) domains and workgroups:

- SIP-enabled AACC solutions require a domain; they are not supported in workgroups. This solution type supports High Availability only in a domain.
- Multimedia-only AACC solutions are supported in a domain or in a workgroup. This solution type supports High Availability only in a domain.
- Avaya Communication Server 1000 AML-based contact center solutions using Communication Control Toolkit, Contact Center Multimedia, or Avaya Agent Desktop are supported in a domain or in a workgroup. This solution type supports High Availability only in a domain.
- Avaya Communication Server 1000 AML-based voice-only solutions not using Communication Control Toolkit, Contact Center Multimedia, and Avaya Agent Desktop are supported in a domain or in a workgroup. This solution type supports High Availability in a workgroup or in a domain.

Avaya Aura® Contact Center domain considerations

Avaya Aura® Contact Center supports only a Windows Server Active Directory domain. Avaya Aura® Contact Center supports a single forest implementation. Avaya Aura® Contact Center supports agent integration within only those domains in the same forest as the Avaya Aura® Contact Center domain. Avaya Aura® Contact Center does not support agent integration across multiple forests, or in domains outside the Avaya Aura® Contact Center forest.

All Avaya Aura® Contact Center servers must be in the same Windows Active Directory domain. All Avaya Aura® Contact Center servers must be registered with the same Windows Active Directory Domain Controller. All Avaya Agent Desktop clients must be registered in this domain, or in domains with a two-way trust relationship with this Avaya Aura® Contact Center server domain.

The Avaya Aura® Contact Center firewall policy defines the services, network ports, and Windows accounts necessary for contact center voice and multimedia functionality. Avaya Aura® Contact Center does not provide or install a group policy. A group policy manages and configures software applications and user settings in a given environment. Avaya Aura® Contact Center cannot be customized to accommodate individual corporate domain structures or group policies, so corporate domains must meet Avaya Aura® Contact Center requirements.

If you plan to apply a corporate or custom group policy to the Avaya Aura® Contact Center (AACC) servers and solution, you must first perform the following:

- Understand the AACC services, ports, and user account requirements as specified by the AACC firewall. For more information, see Microsoft Windows Firewall and Advanced Security on your AACC server to view the inbound/outbound rules.
- Understand the AACC network ports and transport types. For more information, see the Avaya Aura® Contact Center Port Matrix document available at http://support.avaya.com.
- Design or modify your group policy to accommodate these existing AACC services, ports, user accounts, and transport type requirements.
- Domain group policies and security policies can be configured to automate MS Windows updates, server backups, and password expiry rules for local users. These automated features are not supported by AACC. If your group policies or security policies implement these automated features, place the AACC servers in an Active Directory organizational unit (OU) container that protects the servers from these automated features.
- During Avaya Aura® Contact Center commissioning or during a maintenance window, apply and test your group policy. Ensure Avaya Aura® Contact Center call control, administration and maintenance capabilities are preserved. Do not apply an untested group policy to an Avaya Aura® Contact Center production environment. If necessary, modify your group policy to preserve Avaya Aura® Contact Center functionality.
- After successful testing, place AACC back into production, and continue to monitor the contact center for adverse side effects of your group policy.

For more information about the Avaya Aura® Contact Center firewall policy and compatibility with corporate domain group policies, see *Avaya Aura Contact Center Security*.

Avaya Aura® Contact Center server applications (CCMS, CCMA, CCT, CCMM, and LM) do not support Dynamic Host Configuration Protocol (DHCP). All Avaya Aura® Contact Center servers must have a static IP address. Avaya Agent Desktop client computers support both DHCP and static IP addresses.

Avaya Aura® Contact Center firewall considerations

Avaya Aura® Contact Center deploys a customized Windows Firewall Security policy. After you install Avaya Aura® Contact Center, Avaya recommends that you do not make changes to the AACC Firewall Policy.

When you install a Service Pack on your Contact Center server, the Service Pack applies the most recent version of the AACC Firewall Policy; any changes previously made to the AACC Firewall Policy are therefore lost. If you make changes to the AACC Firewall Policy, you must manually track and manage these changes.

Installation process

To check whether a proposed server meets the basic requirements for Platform Vendor Independence, the Contact Center Installer runs a Platform Vendor Independence utility before the software is installed. The Platform Vendor Independence utility generates warnings and suggestions when the proposed server does not satisfy the minimum requirements.

If major problems are detected, the Platform Vendor Independence utility reports a Fail message. The installation cannot proceed until you fix the problems.

The Platform Vendor Independence utility is included in the Contact Center product installation DVD. The utility runs automatically before the software is installed to verify the system.

Common utilities

Avaya Aura® Contact Center includes the following common utilities:

Avaya Contact Center Release Pack Installer

You must use the Release Pack Installer (RPI) for installing Feature Packs and Service Packs.

Feature Pack and Service Pack ZIP files include the Release Pack Installer (RPI) executable. The RPI ensures that you do not need to manually un-install software patches before upgrading Contact Center. It also ensures that third party software updates remain consistent, and facilitates roll-back to a previous patch lineup.

Avaya Contact Center Update Manager

Use Avaya Contact Center Update Manager to view the patches currently on a Contact Center server. You can use Avaya Contact Center Update Manager to install and un-install patches in the correct order. You must install patches for each server application in order of patch number (01, 02, 03).

You cannot use Avaya Contact Center Update Manager to install Feature Packs or Service Packs; you must use the Release Pack Installer (RPI).

System Control and Monitor Utility

The System Control and Monitor Utility is a common utility that you can use on Contact Center servers to monitor the services and shut them down.

The functionality of the utility is split between separate tabs for each installed Contact Center application. In addition, a summary of the progress appears on the main tab.

Database Maintenance

The Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, and Contact Center Multimedia have a common backup and restore utility.

Use this utility to perform the following functions on the Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, or Contact Center Multimedia databases:

- create a backup location on a network drive
- perform an immediate backup
- perform a scheduled backup
- restore the database
- migrate the database to Avaya Aura® Contact Center Release 7.0

You can backup the Contact Center Manager Database, the Contact Center Manager Administration database, the Communication Control Toolkit database, the Contact Center Multimedia database, or the database configuration for backup locations, redundancy paths and schedule information (named ADMIN in the backup utility).

Scheduled backups can occur weekly, monthly, or daily. If two backups are arranged to start at the same time, the larger timeframe backup occurs first. For example, if you have a weekly and a daily backup scheduled at the same time, the weekly backup is performed first, and followed immediately by the daily backup.

When scheduling backups, ensure you configure the backup locations so that separate backup locations are created for each backup. If only one backup location is reserved, all backups are stored in the single location. You can choose the backup location for each scheduled backup.

A database restoration always restores the most recent backup. To restore one of the older backups, you must manually copy files from the old backup to the current location.

High Availability

The High Availability utility provides an interface to configure the modes of each server, IP addresses for each server, notification settings, and settings of the active and standby servers. It is also used to configure and confirm switchovers between the active and standby servers.

For more information, see High Availability fundamentals on page 148.

Grace Period Reset

If a communication error occurs between the Contact Center Manager Server or Communication Control Toolkit and the Contact Center License Manager, normal operation of the Contact Center Manager Server or Communication Control Toolkit runs for the duration of the grace period. Use the Grace Period Reset application to reset the licensing file.

For more information, see Update licensing grace period on page 86.

Trace Control Utility

Trace Control is a utility used to manage traces for the Contact Center servers. The primary function is to provide a common user interface for the administrator to effectively manage trace settings for various services.

A trace logs information provided by a component such as operations or issues and errors.

Automated Log Archiver

With a small number of exceptions (HDC, Toolkit, and Avaya Aura® Media Server), all component logging is now on by default. A circular logging process occurs with a similar file name to configure a number of log files for each server. The user configures the amount of disk space for each component log.

The log files for each component are configured in a circular manner. For each component, you can configure:

- the number of log files for each component
- size limit of each log file

The default log directory on every server is `D:\Avaya\Logs\<product name>`; **<*product name*>** is the name of the component. Each log file uses a standard naming convention: `<product_name>_<component name>_<order number>.log`. The timestamps in the log file follow a consistent format: YYYY-MM-DD hh:mm:ss.sss.

To prevent over-writing or accidental deletion of log files, the Log archiver can archive or store the log files to a common location.

The Automated Log Archiver uses one of two options to archive files:

- Automatic archiving that is always active when the Contact Center Log Archiver service runs on the server.
- The user initiates manual archiving using the Log Archiver utility. All monitored log files are copied to a .zip file.

When you add a watched event manually, you can configure several options to see triggered events (renaming, creating, changing) and the action options (archive the file, archive all files in the directory, or archive the files that match the pattern). You can use wildcard characters to match the log files to monitor.

Use the archiver settings to choose where the archive is to be placed and how much free space you need to configure for the archive on your server.

Upgrades versus migrations

Upgrade: An Avaya Aura® Contact Center software upgrade is done on an existing Avaya Aura® Contact Center server. An upgrade can include installing the most recent Avaya Aura® Contact Center feature pack, service pack, patch, or third-party software.

Migration: An Avaya Aura® Contact Center migration is a move to a new server or virtual guest. Install a new Microsoft Windows 2012 R2 server. Install Avaya Aura® Contact Center Release 7.0 software on the new server and then import or migrate the data from a previous Contact Center server.

Avaya Aura® Contact Center Release 7.0 is supported only on the Microsoft Windows Server 2012 R2 operating system.

Avaya Aura® Contact Center Release 6.x is supported only on the Microsoft Windows Server 2008 R2 operating system. Because the operating system has changed, you cannot upgrade from Avaya Aura® Contact Center Release 6.x to Avaya Aura® Contact Center Release 7.0. You can migrate the agent and statistical information from your existing Avaya Aura® Contact Center Release 6.x solution to Avaya Aura® Contact Center Release 7.0. on a new Windows Server 2012 R2 server. No information is lost in the migration.

Avaya NES Contact Center was supported only on the Microsoft Windows Server 2003 operating system. Because the operating system has changed, you cannot upgrade from Avaya NES Contact Center to Avaya Aura® Contact Center Release 7.0. You can migrate the agent and statistical information from your existing Avaya NES Contact Center solution to Avaya Aura® Contact Center Release 7.0. on a new Windows Server 2012 R2 server. No information is lost in the migration.

Upgrades from Avaya NES Contact Center (on Windows 2003 servers) to Avaya Aura® Contact Center Release 7.0 (on Windows 2012 R2 servers) are not supported.

All Avaya Aura® Contact Center minor releases use patching as the upgrade method. It is important to download and read the patch Release Notes for additional instructions to successfully upgrade Avaya Aura® Contact Center.

For a migration, you install a new Microsoft Windows 2012 R2 server with a fresh version of Contact Center Release 7.0 and import the data from a previous Contact Center server.

The following steps describe the migration process.

1. Backup the database from the existing version of Contact Center to a network location.
2. Install Avaya Aura® Contact Center Release 7.0 on a new Windows 2012 R2 server.
3. Restore the old Contact Center databases to the new Avaya Aura® Contact Center Release 7.0 server, converting the old databases where necessary.
4. Commission Avaya Aura® Contact Center Release 7.0.

The Contact Center migration procedure requires that you migrate all existing co-resident applications at the same time.

Supported migration options

You can migrate the information from previous versions of Avaya NES Contact Center and Avaya Aura® Contact Center to the new Avaya Aura® Contact Center Release 7.0 server types by following the software migration procedures. Migration procedures move all historical, statistical, and configuration information from a previous release of Contact Center to the new release of Contact Center.

The following contact center components and servers can migrate to a Voice and Multimedia Contact Server without Avaya Aura® Media Server:

- Migrate data from an existing Release 6.x co-resident server with Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, and Contact Center Multimedia to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.0.
- Migrate data from an existing Release 6.x Contact Center Manager Server server, Contact Center Manager Administration server, Communication Control Toolkit server, and Contact Center Multimedia server to one new Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.0.
- Migrate data from Avaya NES Contact Center 6.0 or 7.0 to one new Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.0.
- Migrate a Release 7.0 Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server to a new server. For example, to move Voice and Multimedia Contact Server without Avaya Aura® Media Server software from one server to a new larger and faster server.

The following contact center components and servers can migrate to a Voice Contact Server:

- Migrate data from an existing Release 6.x co-resident server with Contact Center Manager Server, Contact Center Manager Administration, and Communication Control Toolkit to a new Avaya Aura® Contact Center Voice Contact Server Release 7.0.
- Migrate data from an existing Release 6.x Contact Center Manager Server server, Contact Center Manager Administration server, and Communication Control Toolkit server to one new Avaya Aura® Contact Center Voice Contact Server Release 7.0.
- Migrate data from Avaya NES Contact Center 6.0 or 7.0 to one new Release 7.0 Voice Contact Server.
- Migrate a Release 7.0 Avaya Aura® Contact Center Voice Contact Server to a new server. For example, to move Voice Contact Server software from one server to a new larger and faster server.

The following contact center components and servers can migrate to a Multimedia Contact Server:

- Migrate data from an existing Release 6.x Contact Center Multimedia server to one new Avaya Aura® Contact Center Multimedia Contact Server Release 7.0.
- Migrate data from Avaya NES Contact Center 6.0 or 7.0 to one new Multimedia Contact Server Release 7.0.
- Migrate a Release 7.0 Avaya Aura® Contact Center Multimedia Contact Server to a new server. For example, to move Multimedia Contact Server software from one server to a new larger and faster server.

The following contact center components and servers can migrate to a Voice and Multimedia Contact Server with Avaya Aura® Media Server:

- Migrate data from an existing Release 6.x single-server with Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, Contact Center Multimedia and Avaya Aura® Media Server to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.0.
- Migrate data from an existing Release 6.x Contact Center Manager Server server, Contact Center Manager Administration server, Communication Control Toolkit server, Contact Center Multimedia server, and Avaya Aura® Media Server server to one new Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.0.
- Migrate a Release 7.0 Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server to a new server. For example, to move Voice and Multimedia Contact Server with Avaya Aura® Media Server software from one server to a new larger and faster server.

The following contact center components or servers can migrate to an Avaya Aura® Contact Center Network Control Center Server:

- Migrate data from an existing Network Control Center Server to a new Avaya Aura® Contact Center Network Control Center Server.
- Migrate data from an Avaya NES Contact Center 6.0 or 7.0 Network Control Center server to an Avaya Aura® Contact Center Network Control Center Server.

- Migrate a Release 7.0 Avaya Aura® Contact Center Network Control Center Server to a new server. For example, to move Network Control Center Server software from one server to a new larger and faster server.

The following Avaya Aura® Media Server migrations are supported:

- Avaya Aura® Media Server on Windows to Avaya Aura® Media Server on Windows
- Avaya Aura® Media Server on Linux to Avaya Aura® Media Server on Linux

Migrating Avaya Aura® Media Server from Windows to Linux is not supported. Migrating Avaya Aura® Media Server from Linux to Windows is not supported. Replacing an Avaya Aura® Media Server Windows server with an Avaya Aura® Media Server Linux server is supported.

Migrating Avaya Aura® Contact Center from an Avaya Communication Server 1000 platform to an Avaya Aura® Unified Communications platform is supported.

Migrating a SIP-enabled Avaya Aura® Contact Center on an Avaya Communication Server 1000 to a SIP-enabled Avaya Aura® Contact Center on an Avaya Aura® Unified Communications platform is supported.

Migrating Avaya Aura® Contact Center from Avaya Aura® Unified Communications platform to Avaya Communication Server 1000 is not supported.

Important:

If you use Avaya NES Contact Center Predictive Dialer, you must contact Avaya to review your migration options. Avaya NES Contact Center Predictive Dialer is end of sale since February 2011. There is no technical upgrade path to Avaya Aura® Contact Center. Outbound dialer options with Avaya Aura® Contact Center include Avaya Proactive Contact and Avaya Proactive Outreach Manager.

Important:

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same, so they attempt to access and control the same resources. Continuing to run the old applications in the Contact Center can result in unpredictable behavior.

Single sign-on deployments

Contact Center supports single-sign on (SSO) deployments, using an identity management mechanism that integrates with a directory services infrastructure (for example Active Directory) for authentication of CCMA users. This helps to reduce administrative costs, and eliminates redundant user information associated with per-application authentication solutions.

Where Contact Center implements SSO, the CCMA Internet Information Server (IIS) redirects new CCMA client requests for the CCMA logon page to a primary security server. The primary security server serves a logon page to the CCMA client and performs the authentication. Following a

successful authentication, the primary security server redirects the original logon request to CCMA with an authentication header. CCMA logs on the CCMA client.

Contact Center supports SSO only using the Avaya Aura® System Manager of the PABX with which Contact Center integrates. This can be the System Manager of either an Avaya Aura® Communication Manager PABX or an Avaya Communication Server 1000 PABX.

You can no longer install a standalone Security Framework server from the Contact Center DVD. You cannot upgrade deployments that use Unified Communications Management (UCM) or Security Framework server as the primary security server. If you are migrating from an earlier version of Contact Center that uses one of these deployments, you must re-configure SSO to use System Manager as the primary security server.

SSO minimizes the necessity for end users to provide the same log on credentials multiple times. SSO using the desktop logon is supported, minimizing the need to authenticate after logging on to the desktop. If you plan to use a single security domain for SSO for multiple applications in your network, you must configure all relevant applications to access the primary security server.

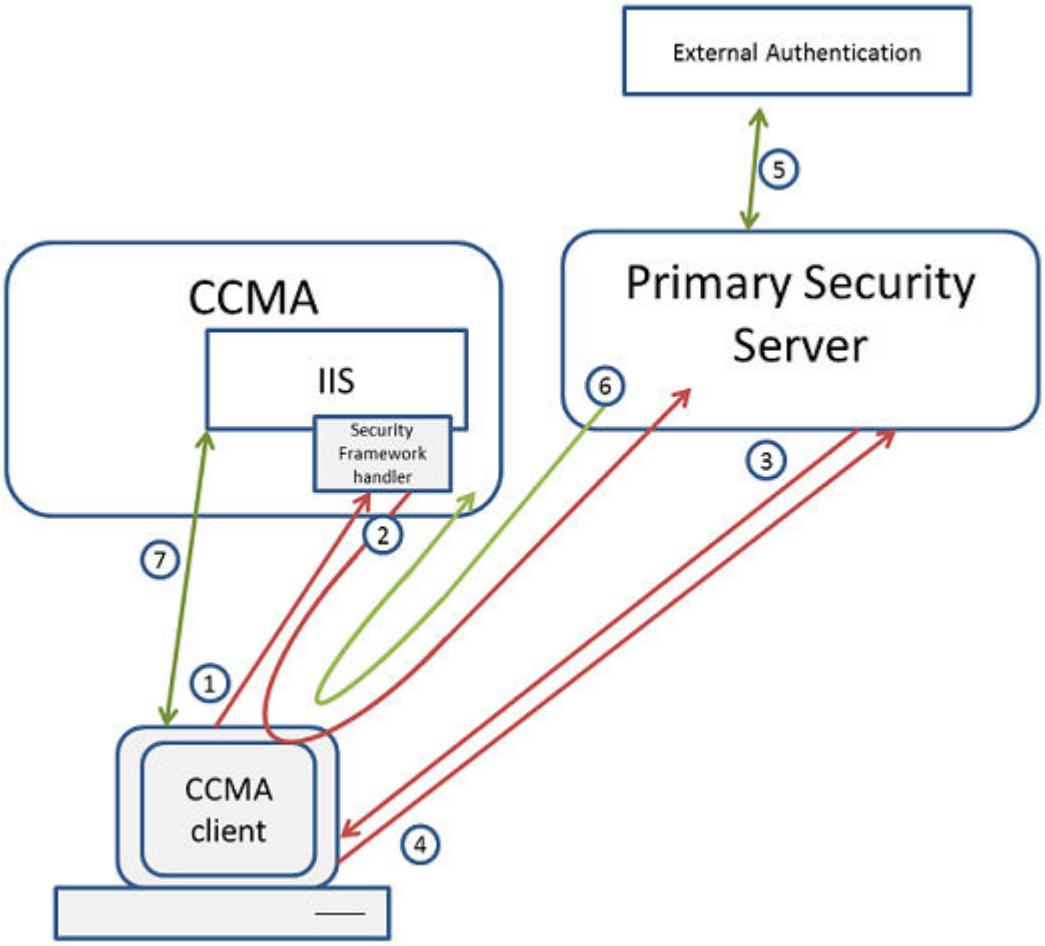


Figure 1: Contact Center Single Sign-On authentication sequence

1.	A CCMA client requests the log on page, but the request does not have an authentication header.
2.	The single sign-on handler redirects the client to the primary security server, System Manager.
3.	System Manager serves a log on page to the CCMA client.
4.	The CCMA client user provides their log on credentials.
5.	System Manager sends the user credentials to External Authentication.
6.	If the user credentials are correct, System Manager redirects the client to the CCMA IIS instance with the authentication header.
7.	CCMA logs on the user and all subsequent requests for this session use the authentication header.

Chapter 4: Routing options

Avaya Aura® Contact Center provides several routing options that depend on the server configuration, voice platform, and licensing.

CDNs and SIP Route Points

In an AML-based contact center, a Controlled Directory Number (CDN) and the associated agents are configured on the Avaya Communication Server 1000 Call Server. A CDN is a special directory number used to queue calls arriving at an Avaya Communication Server 1000 (CS 1000). Contact Center Manager Server (CCMS) controls the CS 1000 CDNs. Use Contact Center Manager Administration (CCMA) to configure which CS 1000 CDNs the CCMS server controls. When CCMS starts up, it acquires the configured CS 1000 CDNs. When a customer call arrives at an acquired CDN, CS 1000 notifies CCMS and waits for routing instructions. The CCMS Task Flow Executor component uses Orchestration Designer flow applications to control, treat, and route the CDN customer call.

SIP-enabled contact centers do not support CDNs. The SIP Route Point is on the CCMS server and not on the PABX or switch. In a SIP-enabled contact center, the CCMS SIP Gateway Manager (SGM) component emulates and controls the SIP Route Points. SIP Route Points are configured in Contact Center Manager Administration using a Uniform Resource Identifier (URI), for example sip: 60000@siptraffic.com. When a customer call arrives at a Route Point, the CCMS Task Flow Executor (TFE) component uses Orchestration Designer flow applications to control, treat, and route that Route Point customer call.

The CDNs used in AML-based solutions and the Route Points used in SIP-enabled solutions perform the same role. They are both logical addresses used by Avaya Aura® Contact Center to accept incoming voice contacts or as a point to which voice contacts are routed. They both enable Avaya Aura® Contact Center to control, queue, treat, and route customer contacts. They are both configured in Contact Center Manager Administration and associated with an application in Orchestration Designer.

Avaya Aura® Contact Center also supports Open Queue Route Points. These Route Point identifiers are used as the entry points for multimedia contacts. Open Queue Route Points are configured in Contact Center Manager Administration.

Contact routing at the switch

When an incoming voice contact is presented to a switch, the switch determines whether it is a contact that requires Contact Center assistance. This determination occurs, for example, by determining the number the customer dialed (DNIS), the customer's trunk group, or a customer choice within an automated attendant application.

Contacts that require Contact Center or agent assistance are routed to the Contact Center through the use of Control Directory Numbers (CDNs). A CDN is a number configured in the switch as the entry point for all voice contacts. One or multiple CDN configurations within the Contact Center offer defined backup parameters. Such parameters include a default agent group (ACD DN), music treatment, and recorded announcements. These definitions are available in a backup scenario if Contact Center is out of service or if the link between the switch and the Contact Center is down.

ACD routing

An administrator can assign a default Automatic Call Distribution (ACD) Queue to an agent. This default ACD Queue is delivered to the switch during agent logon.

The administrator controls moving agents of similar skillsets to the same ACD Queue so that during the default behavior of the switch, agents of similar skillsets receive relevant calls. This feature is supported only on the Avaya Communication Server 1000 (Avaya CS1000) switch platform.

Network ACDN routing works with two Avaya CS1000 switch platforms. The originating server instructs the switch to route the call to the destination site. The originating server provides the configurable dialable DN at which the destination site can be reached. The dialable DN used to route NSBR calls to a destination site must be a CDN configured as a Network CDN on the destination Contact Center Manager Server. The telephony switch uses NACD (the dialing plan) to send the call to the dialable DN at the target site.

Skill-based routing

Contact Center offers the Contact Center Manager Server to provide routing for voice or multimedia contacts that best meets the needs of both the Contact Center and customers.

The skill-based routing capabilities of Contact Center provide efficient contact handling and maximum use of Contact Center resources by presenting contacts to appropriately skilled agents.

A skillset is a label applied to a collection of abilities or knowledge required to process a request, such as language preference, product knowledge, or department knowledge.

In skill-based routing, agents are assigned skillsets, and contacts are presented to available agents who have the skillset to serve the customer request.

Skill-based routing is accomplished using a default or custom-made application you create in the Orchestration Designer (OD).

Contact queuing and presentation

Contact Center facilitates the presentation of contacts to skillsets or queuing functions using one or more of the following criteria:

- Ability—Agents have multiple skills. Each skill is represented by a Contact Center skillset. Contacts can be queued to a skillset, for which the agent who has a particular skill and who is available can respond based on their ability (assigned skillset). Agents can respond to many types of inquiries based on a list of assigned skillsets.
- Personal identification—If a customer needs to speak to a specific representative, you can designate an individual agent to handle a contact. For example, a customer can speak to the same agent as on a previous contact to prevent the customer from having to repeat the situation to a new agent.
- Availability—Agents can be idle because no contacts are presented to them. You can select an agent to receive a customer inquiry because the agent is not busy. You can select an idle agent based on a particular skillset, or choose another agent based on the length of time the agent is idle.
- Priority—Two sets of priorities affect contact presentation to agents:
  - Priority by contact: Contacts with high priority are presented to agents before calls of low priority. Contact priorities range from 1 to 6, with 1 having the highest priority. For example, a contact center can have service level agreements with several customer groups and want to provide a different level of customer service based on those agreements. A customer group with an important service level agreement (such as major corporate accounts) can be assigned a higher priority than a customer group with a lower service level agreement (such as small business accounts).
  - Priority by agent: The agent has a priority for every skillset. Agents with high priorities for the skillset receive contacts for the skillset before agents with low priorities. Agent priorities range from 1 to 48, indicating the level of skill in the skillset. For example, an agent assigned a skillset priority 1 is likely highly proficient in the skill required to effectively handle a customer. An agent assigned a priority of 48 for a skillset can be a new employee learning how to handle customer inquiries for that skillset.

Multiple skillsets

Contacts that simultaneously queue to more than one skillset, are removed from a queue if the call remains unanswered for a specified period of time, or are retrieved from an agent's ringing telephone and queued to another skillset. All options increase the chance of inquiries being answered quickly while maintaining the contact center effectiveness by looking for only appropriately skilled agents.

Open Queue

Open Queue is a licensed feature on Contact Center Manager Server. The primary use of Open Queue is to enable the multimedia Contact Center to receive email messages, Web communications, and instant message contacts, and to send outbound contacts to customers. If you install Contact Center Multimedia, you must enable the Open Queue feature for Contact Center Multimedia/Outbound to route, create, read, and delete the multimedia contacts in Contact Center Manager Server.

The multimedia contacts with Open Queue are handled as voice contacts. They are routed to agents by using the skillset routing features traditionally associated with voice contacts.

The Open Queue feature provides a generic mechanism for third-party software applications to provide access to Contact Center queueing, routing, and reporting for contacts in an integrated manner. The contact management programming interface is Java API. Third-party applications are built with Java libraries supplied by Avaya. The Open Queue specification for contacts supports create, read, and delete operations for contacts. Open Queue also supports a collection of intrinsics associated with the contacts, accesses the values in the intrinsics and uses them to make routing decisions.

The Open Queue feature works with agent licensing to give agents contact handling capability to match the type of contact. Contact Center Multimedia provides a desktop that is integrated with Communication Control Toolkit and that supports multiple contact types. These contact types are configured in Contact Center Manager Server and assigned to agents using Contact Center Manager Administration. For third-party applications, the agent interaction with Open Queue contacts occur through the Communication Control Toolkit, which delivers events relating to Open Queue contacts to desktop applications. Open Queue also delivers contact-control commands (such as answer and close actions), initiated by desktop applications to Contact Center Manager Server contact processing components.

Avaya Callback Assist integration

Avaya Aura® Contact Center (AACC) supports integration with 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.

Network Skill-Based Routing

Network Skill-Based Routing (NSBR) is an optional feature offered with Contact Center Manager. You can use this feature to route voice contacts to various sites on a network.

Agents and skillsets are configured on a Network Control Center (NCC) and propagated to all servers in the network. If a server has a local skillset with the same name as a network skillset, the network skillset replaces the local skillset. For example, the BestAir Toronto server has a skillset named Sales. When the NCC administrator creates a network skillset named Sales, the Sales skillset at BestAir Toronto becomes a network skillset.

Destination sites

A Contact Center Manager network can contain 30 destination sites. However, calls can queue to a maximum of 20 sites.

You can choose a destination site for NSBR using one of the following options:

- First back—The server routes the voice contact to the first site from which it receives an agent available notification. Because the server does not wait for confirmation from slower sites, but queues voice contacts to the site that responds most quickly, contacts are answered more quickly with this method.
- Longest idle agent—The server waits a configured amount of time. During this time, the server examines the agent availability received from the other sites to identify the available agents with the highest priority for the skillset, and to determine which of these high-priority agents is idle for the longest time. The server then routes the voice contact to the site with the longest idle agent. This method helps distribute contact load across the network.
- Average speed of answer—The server waits a configured amount of time. During this time, the server examines the agent availability received from the other sites to identify the available agents with the highest priority for the skillset and to determine which of these agents with the fastest average speed of answer for the skillset is at the site. The server then routes the voice contact to the site with the fastest average speed of answer. This method distributes contacts for a skillset to the most efficient sites in the network.

Chapter 5: Contact Center Manager Server

Contact Center Manager Server is the core Contact Center component that provides the intelligent routing capability for voice and (if licensed) 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.

The Contact Center Manager Server connects to one of the supported switch types:

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

Installation options

The following Avaya Aura® Contact Center server types include a nodal Contact Center Manager Server:

- Voice and Multimedia Contact Server
- Voice Contact Server Only

Each Avaya Aura® Contact Center solution must include one of these server types, therefore every solution contains a nodal Contact Center Manager Server. Contact Center Manager Server is also a component of the Network Control Center Server Only server type.

Components

Contact Center Manager Server has functions distributed among various components:

- Server software—The server software manages functions such as the logic for contact processing, contact treatment, contact handling, contact presentation, and the accumulation of data into historical and real-time databases.

  For more information about the following CCMS utilities, see *Avaya Aura® Contact Center Server Administration*:

  - Database Integration Wizard—A connection between the data within Contact Center Manager Server and an external host database.

  - Feature Report—Easy access to the system attributes of the Contact Center Manager Server such as customer name and company name.
  - Multicast Address and Port Configuration—Change the default data for the optional Real-Time Statistics Multicast (RSM) feature.
  - Multicast Stream Control—Modify the settings for the applications that require real-time statistics to be turned on manually.
  - Server Configuration—Modify or update information from the initial Contact Center Manager Server information.
  - Configuration utility—This interface runs through the Command line prompt only. Use the Configuration utility (nbconfig) to configure local machine settings for Contact Center Manager Server.
- CCMS database—The CCMS database is a Caché database that you configure by using the Contact Center Manager Administration application. The CCMS database stores applications for routing contacts, agents, supervisors, skillsets, and all related assignments, Control Directory Numbers (CDNs), and Dialed Number Identification Service (DNISs).
- Common server utilities—The utilities that are common to all servers in the Contact Center that provide basic monitoring of the software and switch statuses. The common server utilities include the Avaya Contact Center Update Manager, Log Archiver, Process Monitor, System Control and Monitor Utility, and Trace Control.
- Common database utilities—The utilities that are common to all servers in the Contact Center related to database functionality such as backups and restores. The common database utilities are Database Maintenance and High Availability.

Operations performed on the server

The Contact Center Manager Server gathers and routes contacts. See the following sections:

- Process voice and multimedia contacts on page 79
- Contact routing and queuing on page 80
- Multicast communication on page 80
- Network routing on page 81

Process voice and multimedia contacts

Contact Center Manager Server connects to a voice platform (PABX) to collect incoming voice contacts. Contact Center Manager Server provides queuing, routing, reporting, and management of incoming voice contacts.

Contact Center Manager Server can manage multimedia contacts by using the Open Queue feature. The Open Queue is a licensed feature that provides seamless integration between Contact

Center Manager Server, Contact Center Manager Administration, Contact Center Multimedia, and Communication Control Toolkit products. It provides queuing, routing, reporting, and management of outbound voice, Web communications, and email contacts.

Contact Center Manager Server is also used in a SIP-enabled Contact Center, where communication sessions are established over Internet Protocol (IP) networks for interactive communication between two or more entities. SIP enables converged voice and multimedia services, such as instant message and buddy lists.

Contact routing and queuing

Application elements create call routing schemes and treatments. Some examples of elements that you can use to create applications include:

- Queue to Agent—Queues a contact to a specific agent or group of agents.
- Queue to Skillset—Queues a contact to a specific skillset or group of skillsets.
- Give Music—Provides a caller with music from a defined source.
- Give RAN—Provides a recorded announcement to a caller.
- Give Broadcast Announcement—Broadcasts an announcement to multiple callers at the same time (for example, to let the caller know the voice contact can be recorded).
- Give IVR—Provides a caller with an automated way to enter and retrieve information from a voice system while maintaining queue order.
- Collect Digits—Collects information from the caller, such as the reason for the contact or an account number. The collected digits can then be used to route or treat the contact.

For information about configuring contact routing and queuing, see *Using Contact Center Orchestration Designer*.

Multicast communication

IP Multicast communication transmits messages to multiple recipients at the same time. This one-to-many delivery mechanism is similar to broadcasting, except that multicasting transmits to specific groups and broadcasting transmits to everybody. Because IP Multicast transmits only one stream of data to the network on which it is replicated to many receivers, multicasting saves a considerable amount of bandwidth.

IP Multicast provides services such as the delivery of information to multiple destinations with a single transmission and the solicitation of servers by clients.

Unicast communication requires the source to send a copy of information to each recipient: 10 recipients require 10 copies of the data. This method creates two constraints:

- The source system resources are wasted because they duplicate or distribute multiple copies of the same piece of information.

- The combined size of the copies of data sent to recipients cannot be greater than the share of bandwidth available to the source.

A system or router can be a host and can send multicast data to a multicast group if it meets the following conditions:

- The network interface in the system is multicast-capable.
- The system or router is on a network with a local multicast router.
- The internet group management protocol (IGMP) is enabled on the network.

The sender need not be a member of a multicast host group if it sends only multicast data. The sender must be in a multicast host group only if receipt of multicast data is required.

Recipients of IP multicasting data are called host groups. Host groups fall into the following two categories:

- permanent host groups
- transient host groups

IP multicasting specifies multicast host groups using addresses that range from 224.0.0.0 to 239.255.255.255. While IP addresses identify a specific physical location, a multicast IP address identifies a request from a client to a host to join a multicast group.

When you choose IP multicast sending and receiving addresses, note the following restrictions:

- The IP multicast addresses 224.0.0.0 through 224.0.0.255, inclusive are reserved for routing protocols and topology discovery or maintenance protocols.
- The IP multicast addresses 224.0.0.0 through 239.255.255.255, inclusive are reserved for specific applications like Net News.

The following organizations maintain current information about IP multicasting addressing and can provide access to an extensive list of reserved IP multicast addresses. Avaya strongly recommends that you review the information at one or both of these sites before you assign an IP address to a multicast group:

- Internet Engineering Task Force (www.ietf.org)
- Internet Assigned Numbers Authority (www.iana.org)

Network routing

The Network Control Center server is a version of the Contact Center Manager Server that manages the Network Skill-Based Routing (NSBR) configuration and communication between servers in a Contact Center Manager Server network. The Network Control Center server is required when servers in multiple Contact Center Manager Server sites are networked and operating as a single distributed Contact Center. The Network Control Center server runs the Network Control Center software application, a feature of the Contact Center Manager Server software.

Use the Configuration utility (nbconfig) to configure network sites and computer settings for the Contact Center Manager Server network.

Optional configuration tools

Two programming tools are available with Contact Center Manager Server:

- Programming interfaces on page 82
- Web services on page 82

Programming interfaces

Contact Center Manager Server provides a number of open interfaces that third-party developers can use to build applications that work with Contact Center Manager Server:

- Real-Time Statistics Multicast
- Host Data Exchange
- Meridian Link Service Manager

Real-Time Statistics Multicast (RSM) and Real-Time Interface (RTI) provide real-time information to applications such as wall boards.

The Host Data Exchange (HDX) provides an interface for applications to communicate with the call processing script and workflow. This interface ensures the workflow can access information in an external database. With the Open Database Connectivity (ODBC) interface, an application can extract information from the Contact Center Manager Server database.

The Meridian Link Service Manager (MLSM) interface provides messaging and control of resources on the telephony switch.

Programming guides are available for each programming interface.

Web services

The Open Queue Open Interface delivers existing Open Queue functionality to third-party applications by using a Web service. In a controlled fashion, third-party applications can add and remove contacts of a specific type in the Contact Center.

For more details, see the SDK documentation.

The Open Networking Open Interface enables a third-party application to transfer a call between nodes in a network with data associated leaving that call intact. Third-party applications can reserve a Landing Pad on the target node enabling the call to be transferred with data attached. The Web services also provide the functions to cancel the reserving of a Landing Pad freeing it for other calls to be transferred across the network.

For more details, see the SDK documentation.

Chapter 6: License Manager

The License Manager controls the licensing of features within Avaya Aura® Contact Center. The License Manager provides central control and administration of application licensing for all features of Contact Center.

This chapter describes general information about Avaya Aura® Contact Center License Manager.

Installation options

The following Avaya Aura® Contact Center server types include Contact Center License Manager:

- Voice and Multimedia Contact Server
- Voice Contact Server Only
- Network Control Center Server Only

Each Avaya Aura® Contact Center solution must include one of these server types, therefore every solution contains one or more Contact Center License Manager.

User configuration

Use the Contact Center License Manager component to configure Contact Center licensing. Contact Center supports the following license file types:

- local PLIC license file: You can install a suitably configured PLIC license file on the Contact Center server. Contact Center License Manager then uses this PLIC license file to control Contact Center licensed features.
- local WebLM license file: You can install a suitably configured WebLM license file on the Contact Center server. Contact Center License Manager then uses this WebLM license file to control Contact Center licensed features.
- Avaya WebLM server on a virtual guest: Contact Center supports the Virtualized Environment (VE) deployment of Avaya WebLM server. If you already have a VE Avaya WebLM server providing licenses to multiple Avaya products, you can add your Contact Center license to this server. Contact Center License Manager then obtains licenses from the WebLM server, and uses these licenses to control Contact Center licensed features.

  If you use a different deployment of Avaya WebLM server providing licenses to multiple Avaya products, and you want to use Avaya WebLM to license Contact Center as well, you must

change to a VE Avaya WebLM server. This will require re-generating all the licenses you currently have hosted on Avaya WebLM server.

Virtualized deployments of Contact Center can use a VE Avaya WebLM server or a local WebLM license file.

Contact Center deployments that use the Mission Critical High Availability or Remote Geographic Node feature, and use VE Avaya WebLM server licensing, must have two VE Avaya WebLM servers.

For full details on the license file types and license deployment options, see Licensing mechanisms on page 203.

Before installing Contact Center, you must have your license file and know the license type.

Caution:

Do not change the extension of a license file.

Operations performed on the server

The License Manager controls the licensing of features within Avaya Aura® Contact Center. This section contains the following topics:

Configure and view licenses

The License Manager Configuration utility provides the license name, the maximum number of licenses available, the current number of licenses issued, and real-time information regarding license usage.

The License Manager Configuration utility refreshes every five seconds to provide a real-time view of the issued licenses.

Configure license alarms

The License Manager configuration utility generates alarms about license usage. You can change the thresholds at any time.

When the License Manager is co-resident with the Contact Center Manager Server, the Contact Center Manager Server Alarm Monitor is used to monitor alarms.

The following alarm types are available:

- Major alarms—A warning that the license usage is close to hitting the threshold limit configured in the License Manager Configuration utility.
- Critical alarms—A critical alarm that the license usage is likely to be equal to the number of available licenses in your configured system.

Some licensed features have an on (1) or off (0) value. The License Manager configuration utility does not generate alarms for these on/off licenses.

Choose licensing types

Licensing, either Nodal Enterprise or Corporate Enterprise, ensures your contact center can effectively manage the licenses from a single point of contact.

Nodal enterprise licensing

In Nodal enterprise licensing, the license file applies to a single installation of Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, and Contact Center Multimedia. When you choose Nodal licensing, all licensing options for the applications in the Contact Center node are in a single license file that is managed by the License Manager.

Corporate enterprise licensing

You can use Corporate enterprise licensing if more than one occurrence of any product is in the network, to distribute licenses to multiple servers so they can share licenses from a single pool. Products are installed either stand-alone or co-resident. The options in the license file apply to a network of Contact Center Manager Server, Contact Center Manager Administration, Contact Center Multimedia, and Communication Control Toolkit servers.

Manage standby license manager

In a Corporate Licensing environment, you can configure two License Managers: a primary License Manager and a secondary License Manager. Only one License Manager can be active at one time. The primary License Manager actively maintains the licenses. The secondary License Manager runs as a standby License Manager to provide redundancy in a corporate environment.

You can configure the secondary License Manager as the Standby License Manager for the Contact Center License Manager components so that it is not actively used for licenses unless the active License Manager fails.

Configure your preferred active License Manager as the primary License Manager.

For Corporate License applications, you must install the primary License Manager software on the Network Control Center. The server type Network Control Center Server includes a License Manager.

The first license manager to start becomes active even if it is configured as the secondary license manager. The primary license manager is not the active license manager until the secondary license manager stops.

The following conditions apply to the License Manager usage:

- Use the secondary License Manager on any Contact Center Manager Server that does not contain the primary License Manager, including the Network Control Center. You cannot install the primary and secondary License Manager software on the same server.
- You cannot configure a Standby License Manager in a Nodal licensing environment.
- Do not use the Standby License Manager for load balancing issues.
- The active Contact Center server must not use the standby License Manager on the standby Contact Center because the License Manager cannot run as the active License Manager independently of the Contact Center. The active License Manager attempts to write statistics to the standby Contact Center and not the primary Contact Center which can terminate database shadowing.

Update licensing grace period

If a communication error occurs between the Contact Center Manager Server or Communication Control Toolkit and the License Manager, normal operation of the Contact Center Manager Server or Communication Control Toolkit runs during the grace period.

The grace period is 30 days. If a communication problem occurs between the Contact Center Manager Server and the License Manager, 30 days are available for the Contact Center Manager Server to continue normal operation. After you resolve the communication problem, the grace period automatically reverts to 30 days. For example, if the communication problem is resolved in 2 days, the grace period returns to 30 days after 2 days of successful connection to the License Manager.

If, at any stage, the grace period expires, Contact Center Manager Server shuts down and is locked. You cannot restart Contact Center Manager Server without resetting the grace period.

You can reset the grace period to 30 days at any time. When a communication error is detected, an event is logged to the Server Utility detailing that an error occurred, the time already elapsed in the grace period, and a lock code that you must return to Product Support to reset the grace period.

Important:

Avaya Aura® Media Server does not support the grace period.

Chapter 7: Contact Center Manager Administration

Contact Center Manager Administration is a browser-based tool for contact center administrators and supervisors to manipulate the data and reporting for the Contact Center Manager Server database. You can use Contact Center Manager Administration to configure contact center resources, contact flows, components, and activities. You can also use Contact Center Manager Administration to define access levels to data and provide dynamic reporting to fit your enterprise business needs.

Installation options

The following Avaya Aura® Contact Center server types include Contact Center Manager Administration:

- Voice and Multimedia Contact Server
- Voice Contact Server Only
- Network Control Center Server Only

Each Avaya Aura® Contact Center solution must include one of these server types, therefore every solution contains Contact Center Manager Administration software.

The following sections provide the information you need to install Contact Center Manager Administration:

- Default users on page 87
- Components on page 88

Default users

The installation adds default users to the Windows operating system when you install Contact Center Manager Administration (CCMA). You must change your passwords for the Avaya user accounts to protect your system from unauthorized access.

The following user accounts are configured:

- iceAdmin—The iceAdmin account is the CCMA Administration account, used to manage the CCMA server. iceAdmin is a Windows Server 2012 account with only the privileges required to maintain CCMA.
- IUSR_SWC—The IUSR_SWC account replaces the Internet Information Services (IIS) default anonymous user account, usually IUSR_<machinename>, which is well known and is vulnerable to attack. IUSR_SWC is a Windows Server 2012 account, and has the same default password as the iceAdmin password.
- webadmin—A CCMA user that has access to all the CCMA configuration components, including the component to create new users. You must use the webadmin account to configure other administrators. You can then use these new user accounts to manage CCMA, rather than using the webadmin account. The webadmin account is an application level account, it is not a Windows Server 2012 account.

Components

Contact Center Manager Administration has functions distributed among various components. The major components of Contact Center Manager Administration include the following:

- Server software—The server software handles statistical reporting and maintenance for many aspects of the Contact Center.

  For more information about the following CCMA utilities, see *Avaya Aura® Contact Center Client Administration*:

  - Agent Desktop Displays—A client application for monitoring real-time performance of agents in the Contact Center. Configure the communications on the server to manage the client applications.
  - Agent Certificate Configuration—Manage the security for the agent desktops.
  - Configuration—Perform backups and restores, change passwords, configure reporting, and configure the security policies.
- Contact Center Manager Administration application—A Web-based application that administrators can use to perform the following functions:
  - Contact Center Management (see *Avaya Aura® Contact Center Client Administration*)
  - Access and Partition Management (see *Avaya Aura® Contact Center Client Administration*)
  - Configuration (see *Avaya Aura® Contact Center Client Administration*)
  - Scripting (see *Using Contact Center Orchestration Designer*)
  - Multimedia (see *Avaya Aura® Contact Center Client Administration*)
  - Real-Time Reporting (see *Using Avaya Aura® Contact Center Reports and Displays*)
  - Historical Reporting (see *Using Avaya Aura® Contact Center Reports and Displays*)

- Report Creation Wizard (see *Using Avaya Aura® Contact Center Reports and Displays*)
- Prompt Management (see *Avaya Aura® Contact Center Client Administration*)
- Emergency Help (see *Using Avaya Aura® Contact Center Reports and Displays*)
- Audit Trail (see *Avaya Aura® Contact Center Client Administration*)
- Agent Desktop Displays (see Agent Desktop Displays online Help)
- Outbound (see *Avaya Aura® Contact Center Client Administration*)
- Call Recording and Quality Monitoring (see *Avaya Aura® Contact Center Client Administration*)

Operations performed with Contact Center Manager Administration

Contact Center Manager Administration gathers and routes contact and tracking information about the contacts and agents. Contact Center Manager Administration manages the following tasks:

Control access to configuration components

In Access and Partition Management, administrators can grant and restrict access to Contact Center Manager Administration components and data by defining users and access classes.

Use Access and Partition Management to add, edit, view, or delete the following items:

- users
- partitions

- access classes
- report groups for Historical Reporting

For information and procedures to manage users and access in your Contact Center, see *Avaya Aura® Contact Center Client Administration*.

Perform off-line configuration

Use the Configuration component to configure and administer Contact Center Manager Server. You can use the CS1000 Data Extraction Tool to extract configuration data from the CS1000 PBX switch, and then upload that data to the Contact Center Manager Server by using Contact Center Manager Administration Configuration spreadsheets. For more information, see *Avaya Aura® Contact Center Server Administration*. The Avaya Communication Server 1000 Data Extraction Tool is intended for use with the Avaya CS 1000 PBX switch only; it does not support the Avaya CS 1000 Internet Enabled switch.

If you are on site configuring a customer Contact Center, you can upload your Contact Center Manager Configuration Tool spreadsheets by using the Configuration component of the customer Contact Center Manager Administration application.

For information and procedures to configure your Contact Center off line, see *Avaya Aura® Contact Center Client Administration*.

Manage users and skillsets for users

Use Contact Center Manager Administration to add, edit, view, or delete:

- users (agents, supervisors, or supervisor/agents) for Contact Center Manager Server
- agent-to-supervisor assignments
- agent-to-skillset assignments

Supervisors can also use CCMA to log out one or more agents.

For information and procedures to manage users and skillsets in your Contact Center, see *Avaya Aura® Contact Center Client Administration*.

Create script or flow applications

Contact Center uses script or flow applications to route contacts. You can install the Orchestration Designer on a stand-alone client to create applications before you install the remainder of the Contact Center server software. With the Scripting component, you can create, modify, or activate previously composed applications to configure the contact routing instructions for your Contact Center by using the following components:

- Orchestration Designer to create graphical-based applications (flows) or command line applications (scripts)

- Script Variable tool to create variables for the applications

You can apply thresholds or groups of monitored statistics to your applications, and you can edit application threshold classes.

The Orchestration Designer has a built-in validation tool that checks your applications for errors.

If you are configuring a customer Contact Center, you can use the Orchestration Designer component on your client computer to upload your Contact Center Manager applications.

For more information about creating applications in the Orchestration Designer, see *Using Contact Center Orchestration Designer*.

Report real-time data

Use the real-time reporting component to view contact activity information. Real-time displays are available for both single node and multinode sites.

The following standard real-time reporting displays are available in Contact Center Manager Administration:

- six standard real-time displays for a single-node Contact Center Manager Server site
- three standard real-time displays for multinode (or networked) Contact Center Manager Server sites

In addition to viewing current state information on Contact Center, supervisors can log out an agent or toggle an agent's state between Ready and Not Ready from a real time display. To use this feature, supervisors must customize the real time display to display the Force Log Out and Change State buttons.

Contact Center Agent Desktop Displays provides real-time skillset monitoring to agents. You can configure Agent Desktop Displays to inform agents, for example, of the number of calls in queue and the average call wait time.

Agent Desktop Displays is a component of Contact Center Manager Administration installed on the agent workstation. The application is not started or installed from the Contact Center Manager Administration server. A separate piece of client software is installed on the clients to view real-time reports.

For information and procedures to create real-time reports in your Contact Center, see *Using Avaya Aura® Contact Center Reports and Displays*. To understand the fields in the real-time reports, see *Contact Center Performance Management Data Dictionary*.

Review real-time reports in Agent Desktop Display

The Agent Desktop Displays application is a separate Windows-based tool that can run with the Avaya Agent Desktop on clients in your Contact Center to provide real-time skillset monitoring to Contact Center agents.

Agents or supervisors can log on to Agent Desktop Displays using their phone logon ID and view real-time statistics for each skillset to which they belong.

The tabular format appears as a window with several columns. This window can be moved, minimized, resized, closed, or configured to always stay on top of the desktop like a standard Microsoft window.

The application continually verifies that the agent is logged on to the server in Contact Center Manager Server by checking with the Contact Center Manager Administration server once every minute. It also checks the list of skillsets that are assigned to the logged-on agent once every three minutes and updates the display accordingly.

Report historical data

Use Historical Reporting to obtain standard reports about the past performance of the Contact Center, Contact Center configuration data, and Access and Partition Management configuration data of the Contact Center Manager Administration server. The data for historical reports is gathered from primary or standby servers: you configure the destination in the Global settings section of the Contact Center Manager Administration application.

Report Creation Wizard is a reporting feature that you can access through the main Historical Reporting interface. You can use the wizard to create, maintain, and modify custom on-demand reports through a user-friendly interface.

After you create reports by using Report Creation Wizard, you can work with the reports in the Historical Reporting component and use the same access permissions, partitions, and filters features that you can with other reports.

You can use the Historical Reporting interface to schedule reports that you create with the Report Creation Wizard.

You can generate many types of historical reports:

- standard reports, such as agent properties and CDN properties
- summarized historical reports for a specific interval of time
- detailed reports for specific events that occur in the Contact Center
- graphical reports to show service level, contact handling performance, and agent staffing information for skillsets
- Report Creation Wizard reports imported from the Report Creation Wizard component
- User defined reports created from standard reports to run on-demand and scheduled reports
- User created reports imported to Contact Center Manager Administration
- Access and Partition Management configuration reports for the Contact Center Manager Administration server, such as access classes, report groups, users, and user-defined partition reports

Configure Simple Mail Transfer Protocol (SMTP) to send an email notification to report recipients when the Historical Reporting component of Contact Center Manager Administration generates a scheduled report.

Create a shared folder to export historical reports if you want multiple users to access scheduled historical reports from the same folder.

For information and procedures to create historical reports in your Contact Center, see *Using Avaya Aura® Contact Center Reports and Displays*. To understand the fields in the historical reports, see *Contact Center Performance Management Data Dictionary*.

Configure emergency support for agents

The Emergency Help feature is a notification panel on the browser whereby supervisors are alerted when an agent presses the Emergency key on their phone.

Agents press the Emergency key when they require assistance from the supervisor (for example, if a caller is abusive). The Emergency Help panel displays information about the agent, including the agent name and location, and displays the time when the Emergency key was pressed.

To configure emergency help in your Contact Center, see *Avaya Aura® Contact Center Client Administration*.

Monitor configuration changes

Contact Center Manager Administration has an audit trail that records the actions performed in Contact Center Management, Access and Partition Management, Historical Reporting, Prompt Management, Realtime Reporting, Scripting, and Configuration. The Audit Trail also identifies the ID of the user who made the changes.

For information about the audit trail, see *Avaya Aura® Contact Center Client Administration*.

Create outbound campaigns

If you have Contact Center Multimedia installed, you can use the Outbound Campaign Management Tool to create, modify, and monitor outbound campaigns. You can use this tool to define campaign parameters, import and review call data, create agent scripts, and monitor campaign results.

The Agent Desktop interface for outbound runs on the agent desktop during campaigns. This interface presents outbound contacts to agents, provides agents with preview dial capability, displays agent call scripts (if configured), and saves disposition codes and script results.

For information and procedures to configure the outbound contact type, see *Avaya Aura® Contact Center Server Administration*. For information and procedures to create outbound campaigns in your Contact Center, see *Avaya Aura® Contact Center Client Administration*.

Prompt Management

Using Prompt Management, Contact Center Manager Administration (CCMA) users can manage prompts on the Avaya Aura® Media Server (Avaya Aura® MS) server designated the Content Store Master. Prompt Management provides access control and partitioning.

You must configure CCMA as a trusted host in Avaya Aura® MS to configure the prompts. For more information on Prompt Management, see *Avaya Aura® Contact Center Client Administration*.

Optional tools

The Contact Center Manager Administration server includes two optional components:

- Data extraction on page 94
- Logon warning message on page 94

Data extraction

The CS1000 Data Extraction Tool is a software application that extracts information about resources such as Terminal Numbers (TNs), voice ports, Controlled Directory Numbers (CDNs), Interactive Voice Response Automatic Call Distribution DNs (IVR ACD-DNs), and routes from an Avaya Communication Server 1000 switch. The tool saves this information in Excel spreadsheets.

You cannot upload data from the CS1000 Data Extraction Tool spreadsheets directly to Contact Center Manager Administration. You must copy the data from the CS1000 Data Extraction Tool spreadsheet into the Contact Center Manager Administration Configuration Tool spreadsheet and then upload the data.

For more information about Contact Center Manager Administration Configuration Tool spreadsheets, see the Contact Center Manager Administration online Help.

Logon warning message

You can customize a warning message to appear when users attempt to log on to Contact Center Manager Administration. By default, this feature is enabled in Contact Center Manager Administration; however, a message is not visible unless you configure your message title and text in the Local Security Policy tool of Windows Server 2012 R2.

If you have a domain security policy in place with a logon warning message configured, you cannot change the logon warning message. In this case, you must contact your administrator to change the message on the domain server. If you implement Single Sign-On, the warning message on the primary security server (Avaya Aura® System Manager) overrides the logon message.

Chapter 8: Contact Center Server Utility

Use the Server Utility to monitor and maintain Contact Center Manager Server activity. The Server Utility provides tasks that are not available through Contact Center Manager Administration application.

Installation options

The following Avaya Aura® Contact Center server types include Server Utility:

- Voice and Multimedia Contact Server
- Voice Contact Server Only
- Network Control Center Server Only

Each Avaya Aura® Contact Center solution must include one of these server types, therefore every solution contains Server Utility software.

The following sections provide the information you need to install the Server Utility software:

- Components on page 95

Components

Contact Center Server Utility contains the following components:

- Server Utility window—Use the Server Utility window to monitor and maintain the following components:
  - User Administration—Users (desktop) and Access Classes
  - System Configuration—Serial ports, switch resources, Voice Prompt Editor, server settings, and connected sessions
  - Alarms and Events—Alarm monitor, event browser, and event preferences
  - System Performance Monitoring—Service performance monitor
- Provider application—Receive Contact Center script information over the Host Data Exchange (HDX) interface. Additionally, you can configure the Provider application to return information to the Contact Center script.

- Service Monitor—Monitor the status of Contact Center Manager Server services from a stand-alone computer.
- PC Event Browser—View events that occur on the client PC on which the Server Utility runs. You can view help for each event as it appears in the PC Event Browser.

Operations performed on the server

Use the Contact Center Server Utility to configure users and accounts. This section contains the following topics:

Monitor and maintain user permissions

Information vital to companies is transmitted over networks. You must protect these networks so that only authorized users can access, change, or delete information.

The system administrator establishes and maintains system security. The administrator sets up security by assigning logon passwords and access classes to users. By assigning the appropriate access classes to the appropriate users, the administrator can help ensure system security.

For example, to restrict access to certain Server Utility components to senior administrators, perform these tasks:

1. Define access classes.
2. For each access class, select the Contact Center Manager Server functions that members of that class can use in Server Utility.
3. Create desktop user accounts for users who require access to Contact Center Manager Server functions.
4. Assign access classes to user accounts, giving users the privileges they need to perform their jobs.

Configure access classes

An access class is a group of privileges for functions available for Contact Center Manager Server through Server Utility.

Three default access classes are available:

- adminGroup—Users have administrator access to the system and can access all functions.
- Call Center Admin—Users can access User Administration and System Configuration.
- Supervisor—Users can view users in User Administration reporting to them.

Reset passwords

Users are locked from the system if they attempt to log on more than three consecutive times using an invalid password, based on Windows settings configured during the installation. To restore a user's access to the system, an administrator must reset the password retry count to zero.

If the locked-out user is an administrator, another administrator must restore access. If you log on as the system administrator (sysadmin), you are not locked out.

If only one administrator exists, only Avaya customer support staff can reset the account. Therefore, be sure you create at least two users with administrator privileges.

The desktop user password expires after 180 days. Seven days before the expiry of the password, the Server Utility software displays a warning message during the user logon. If the desktop user password expires, the administrator must reset the password.

The sysadmin password does not expire.

Monitor system configuration settings and performance

You can use the Server Utility to view and edit the following system configuration information:

- serial ports

  Serial ports are input/output devices used to connect external equipment, such as DVD drives or modems, to your computer. Serial ports transmit data from these external devices one bit at a time.

  View, print, or edit serial port settings. You can modify a serial port baud rate, data bits, stop bits, parity, and flow control. You can also use the Serial Port Properties page to edit serial port settings.
- switch resources

  Record information about an Avaya Communication Server 1000 after initial software installation. You can record the type, subtype, release number, and the host port assigned to the Avaya Communication Server 1000.

  The Switch Resources option is not available when you connect to an Avaya Aura® Media Server.
- server settings

  View detailed information about the server resources, such as the software release number and the serial number. The information is saved to the server database during installation and

can be retrieved for technical support purposes. You can print the contents of the Server Settings window for future reference. You can also view a list of the services and features installed on your system.

- connected sessions

  View the users logged on to the server and disconnect user sessions. You can print information about connected sessions for future reference.

- system performance

  View the server operating conditions. Determine whether your system has sufficient processor capacity, memory, or storage space. You can also use this information to improve the system efficiency. For example, to improve daytime performance, you can reschedule events to run at night, when the server is not as busy. You can print server performance data for future reference.

Manage alarms and events

The PC Event Browser and Alarm Monitor show events that occur on the server. These programs provide many common features for viewing events.

The main advantages of the Event Browser are

- You can filter events by several categories, including severity and event code range.
- You can limit the display to the most recent events.

To view server events, use the Alarm Monitor. The Alarm Monitor automatically appears in the foreground of the desktop when an event occurs, immediately alerting you to problems. You can specify whether the Alarm Monitor appears in the foreground for only critical events, major and critical events, or all events, or whether it stays in the background.

Events are log entries that record activities in Contact Center Manager Server, such as sending or receiving messages, opening or closing applications, or errors.

In the Alarm Monitor, you can filter events by severity only. The Alarm Monitor does not display information events.

- Minor—A fault condition exists that does not affect service and that you must take corrective action to prevent a more serious fault. For example, a minor event is generated when the file system is 90 percent full.
- Major—A condition exists that affects service and urgent corrective action is required. The event condition can cause severe degradation in server performance, and you must restore full capacity. For example, a major event is generated when the file system is 100 percent full.
- Critical—A condition exists that affects service and immediate corrective action is required. Critical events are reported when a component is completely out of service, and you must take immediate action to restore it. For example, a critical event is generated when the file system crashes.

Table 3: Event Browser versus Alarm Monitor feature

Feature	In PC Event Browser?	In Alarm monitor?
View events	Yes	Yes
View online Help for an event	Yes	Yes
Sort events by category	Yes	Yes
Save a list of events	Yes	No
Print a list of events	Yes	Yes
View minor, major, critical events	Yes	Yes
View information events	Yes	No
Filter events by code, type, severity, latest events	Yes	No
Filter events using Event Preferences	Yes	Yes
Automatically show the graphical user interface in the foreground when an event occurs	No	Yes
Clear an event	No	Yes

Chapter 9: Communication Control Toolkit

Communication Control Toolkit is a client/server application that helps you implement Computer-Telephony Integration (CTI). For switches, the Communication Control Toolkit facilitates the integration of Contact Center with your client applications. In the SIP-enabled Contact Center, the Communication Control Toolkit integrates the Contact Center users within the SIP environment to offer features that enrich the customer experience.

Communication Control Toolkit enhances the skill-based routing ability of Contact Center Manager Server. You can create custom agent applications, such as softphones, agent telephony toolbars with screen pops, and intelligent call management applications. Communication Control Toolkit enables integration with business applications such as CRM systems.

In this environment, Communication Control Toolkit uses Meridian Link Services to communicate with Contact Center Manager Server over the Contact Center subnet. Through Contact Center Manager Server, it communicates with the switch. Optionally, the IVR Service Provider element of Communication Control Toolkit connects to an IVR server on the Contact Center subnet.

When you use Communication Control Toolkit as a telephony application server in a Contact Center environment, Communication Control Toolkit connects to the Contact Center subnet. Contact Center Manager Server connects to the embedded Local Area Network (ELAN) subnet either directly or is routed using the Contact Center subnet.

A direct connection to Contact Center Manager Server links to the ELAN subnet. An additional Contact Center subnet is required in a Contact Center environment to ensure that the TAPI Service Provider (SP) traffic is not affected by non-TAPI data traffic. An Ethernet switch or router provides routing between these Contact Center subnets.

A Contact Center installation supports the following resources:

- CTI-enabled IVR ports
- CTI-enabled agent desktops
- call-attached data sharing between IVR, user-to-user information (UUI) (incoming only), and Communication Control Toolkit clients
- call-attached data networking in a Communication Control Toolkit network
- Host Data Exchange (HDX) and Real-time Statistics Multicast (RSM) supported through CCT-IVR

Installation options

The following Avaya Aura® Contact Center server types include Communication Control Toolkit:

- Voice and Multimedia Contact Server
- Voice Contact Server Only

Each Avaya Aura® Contact Center solution must include one of these server types, therefore every solution contains Communication Control Toolkit.

Components

Communication Control Toolkit has functions distributed among various components. The CCT includes the following major components:

- Server software—The server software handles functions such as assigning resources (for example, users) to groups of users to workstations.

  For more detailed information about the following CCT utilities, see *Avaya Aura® Contact Center Server Administration*.

- CCT database—The CCT database is configured using the CCT Web Administration. The Caché-based CCT database stores the user-to-group assignments, switch information (terminals and addresses), and information about Contact Center mappings.

  Note:

  The Communication Control Toolkit Web Administration application is hosted on an Apache Tomcat server.

- Common server utilities—The utilities that are common to all servers in the Contact Center provide basic software and switch status monitoring. The common server utilities include the Avaya Contact Center Update Manager, Log Archiver, Process Monitor, System Control and Monitor Utility, and Trace Control.
- Common database utilities—The utilities that are common to all servers in the Contact Center related to database functions such as backups, restores, and high availability. The common database utilities are Database Maintenance and High Availability.

Operations performed on the server

The Communication Control Toolkit gathers and handles data for voice and multimedia contacts. This section describes the tasks you perform in Communication Control Toolkit:

- Monitor call data on page 102

- Configure resources on page 102

Monitor call data

Attached data in Communication Control Toolkit use one of three formats: binary, string, and key-value pairs. The string and key-value pair formats contain meta-data (the markup that describes their structure) when they are attached to TAPI as CallData. Because the size limit for TAPI call data is 4096 bytes, when these formats are used on systems that use the TAPI connector, the effective storage capacity of Call Data is reduced by the size of the meta-data.

The formatting meta-data overhead of string (Str) formatted data is 34 bytes, reducing the effective CallData storage capacity in TAPI to 4062 bytes (4061 characters plus the terminating null character). The formatting meta-data overhead of the key-value pair (KVP) formatted data is 34 bytes for each key-value pair.

For example, for a 5-character key and a 5-character value, the actual data that is attached to TAPI is:

34 (base formatting)
+ 16 (1 key-value pair)
+ 10 (the key and the value)
+ 1 (terminating null character)
= 61.

Adding a second similar key-value pair increases the number of bytes by 26 (16 for the key-value pair + 10 for the key and the value). Attached data stored in the binary (bin) format is stored in TAPI CallData without formatting meta-data. The full 4096 bytes of TAPI CallData is used.

Configure resources

The following resources are used by Communication Control Toolkit in AML-based Avaya Communication Server 1000 contact center solutions:

- Windows user—Users who are logged on to one or more communication terminals.
- Windows user group—A logical group of Windows users (for example, a sales group or a support group) that have a common property.
- Agents—Users configured in the Contact Center database on Contact Center Manager Server with a designated role in the Contact Center such as a supervisor or an agent to received queued contacts.
- Agent group—A logical group of Contact Center users (for example, agents or supervisors) that have a common property.
- Terminal—A physical (including software applications) communications endpoint such as an email client or an IVR line.
- Terminal group—A logical group of terminals (for example, local office, support office) that have a common property.

- Address—A logical communications endpoint such as an email address or telephone number. An address can be one of three types:
  - Basic—A basic address (SCR key) is an address that has an associated terminal (physical endpoint). The basic address is used by Communication Control Toolkit users to answer and make calls.
  - Route Point—A route point address (CDN) is an address to a terminal that is not associated with a line. The Route Point address is used by the Telephony Service Provider to accept incoming contacts or as a point to which contacts are routed.
  - Agent—A position ID (ACD key) for the Avaya Communication Server 1000 switch.
- Address group—A logical group of addresses that have a common property.
- Workstation—A computer used by Communication Control Toolkit client on the same domain as the Communication Control Toolkit server.
- Provider—A switch interface service provider to connect telephony devices to the Communication Control Toolkit server.

Resource Assigning

Assignments use the following principles:

- When a terminal is assigned to an agent, CCT automatically assigns the addresses associated with that terminal to the agent. When the agent logs on, CCT verifies changes to the agent's configuration. New addresses assigned to the terminal are automatically assigned to the agent. Also, unassigned addresses are automatically removed from the respective agents. For specialized CCT behavior, an administrator can assign route point addresses to agents.
- Assignments are distributed using groups. If you assign one resource to a second resource that is a group, and the second resource to a third, then the first resource is also assigned to the third. For example, if you assign two users to a user group, and then assign the user group to an address, then the users are assigned to the address. Or, if you assign a user to a user group, the user inherits the user group terminals and addresses.
- Resources cannot be assigned to resources of the same type. For example, you cannot assign a user to a user, or a terminal to a terminal. Grouped resources cannot be assigned to resources that are closely related. For example, you cannot assign a terminal group to an address group because both resources are types of end points.
- Only terminals are assigned to workstations.
- You do not assign route point addresses to terminals; route point addresses do not have associated terminals.

Table 4: Supported resource-to-resource assignments

Resource	Assignment
User	Terminals, Terminal Groups, and Address Groups can be assigned to a User.
User group	Users can be assigned to User Groups.

Resource	Assignment
Terminal	Addresses and Workstations can be assigned to Terminals.
Terminal group	Terminals can be assigned to Terminal Groups.
Address	No resources can be assigned to an Address.
Address group	Address can be assigned to Address Groups.
Workstation	No resources can be assigned to a Workstation.

Importing resources

Use the Communication Control Toolkit Web Administration to manage the resources in the database. You can configure the resources manually or automatically by using the Bulk Provisioning tool of the Communication Control Toolkit Snap-in.

For more information about importing resources, see *Avaya Aura® Contact Center Server Administration*.

Communication Control Toolkit API

Communication Control Toolkit is software for installed and browser-based client integrations. Communication Control Toolkit delivers a cross-portfolio multichannel Application Programming Interface (API) that facilitates the integration of self-service and Contact Center solutions for your client applications.

The Application programming interface (API) is published as Microsoft .NET types and is distributed as a Windows assembly, which is referenced by application developers.

You can use Communication Control Toolkit as the next generation of computer telephony integration (CTI) middleware and CTI toolkit. On the client, the API provides a group of interfaces, collectively known as the Communication Control Toolkit API.

The Communication Control Toolkit API provides easy access to a subset of Communication Control Toolkit functions, which you can use for CTI functionality without low-level CTI knowledge for the basic development of powerful integrations and applications such as:

- desktop applications (for example, Call Control Toolbar) server
- applications (for example, Call Recording, Work Force Management)
- screen-pop utilities
- business application or Computer Resource Management (CRM) connectors

For more information about using the Communication Control Toolkit API, see the Avaya Communication Control SDK Programmers Reference Guide. This guide is a help file that accompanies the Software Development Kit. You must join the developer partner program and purchase the Communication Control Toolkit SDK to download the documentation from http://support.avaya.com.

Avaya Agent Desktop is an example of a client application that uses the Communication Control Toolkit API.

Contact Control Service SDK

The Contact Control Service SDK builds on the capabilities of existing Contact Center APIs by adding support for outbound voice calls in solutions that integrate Proactive Outreach Manager (POM).

The Contact Control Service SDK uses the Integration Portal module, which consolidates Contact Center APIs to simplify custom client development. The Integration Portal module exposes a wide range of features and capabilities to developers of custom applications. It automatically inherits the CCT and CCMM configuration data, and requires no further user configuration. The Integration Portal uses the Industry standard HTTPS port 443 on the Contact Center server.

The Contact Control Service SDK supports the Java programming language. You can develop custom clients for Contact Center using the Contact Control Service SDK. The Contact Control Service SDK supports the following:

- Inbound voice calls.
- Outbound voice calls, when Proactive Outreach Manager is part of the Contact Center solution.

When using the outbound contact type, an agent cannot use both Agent Desktop and a custom client developed using the Contact Control Service SDK at the same time.

For more information on developing Contact Control Service SDK custom clients, see the Contact Control Service SDK documentation on the Avaya DevConnect site http://www.devconnectprogram.com.

Chapter 10: Contact Center Multimedia

Contact Center Multimedia provides support for inbound multimedia contacts. Contact Center Multimedia also facilitates outbound contact types, which you can use to create and manage outbound campaigns; for example, marketing or sales campaigns.

Contact Center Multimedia supports the following contact types:

- Email
- Instant Message (IM)
- Web communications
- Outbound
- SMS text
- Faxed document
- Scanned document
- Social Networking
- Voice mail

All multimedia contact types are subject to Contact Center routing and prioritization. Administrators can create specific treatments through applications developed in the Orchestration Designer. Administrators and supervisors can review a full range of historical reports and real-time displays to track volume and completion statistics.

You must have licenses for Contact Center Multimedia, Open Queue, and one or more Internet contact types before you can install Contact Center Multimedia.

Installation options

The following Avaya Aura® Contact Center server types include Contact Center Multimedia:

- Voice and Multimedia Contact Server
- Multimedia Contact Server Only

Each Avaya Aura® Contact Center solution must include one of these server types, therefore every contact center solution contains Contact Center Multimedia software.

The following sections provide the information you need to install Contact Center Multimedia:

Default users

The installation adds default users to the Windows operating system when you install Contact Center Multimedia:

- IUSR_<servername>: An Internet Information Services (IIS) account used for all communication between the Multimedia server and the Agent Desktop over HTTP.

Folder structure

The Contact Center Multimedia install creates two folders on the same hard drive on which you install the database:

- `Avaya/Contact Center/Email Attachments/inbound`
- `Avaya/Contact Center/Email Attachments/outbound`

These two folders are locations for the attachments sent or received by your contact center. You must configure these two folders to allow share and NTFS folder permissions.

Components

Contact Center Multimedia contains several major components:

- Server software: The server software handles multimedia contacts.

  For more information about the following CCMM utilities, see *Avaya Aura® Contact Center Server Administration*.
- Multimedia Administration: The Multimedia Administrator application is installed with Contact Center Multimedia, but runs from the Contact Center Manager Administration application. Use the Multimedia Administrator to configure and maintain all aspects of CCMM, other than outbound campaigns.
- OCMT: The Outbound Campaign Management Tool (OCMT) is installed with Contact Center Multimedia, but runs from the Contact Center Manager Administration application. Use the OCMT to create outbound campaigns for your Contact Center.
- Avaya Agent Desktop: The Agent Desktop is installed by default on the Contact Center Multimedia server. Agents in your contact center can download this client application from the CCMM server and use the softphone and multimedia interface to handle all types of contacts from a single window.

- Common server utilities: Utilities that are common to all servers in the Contact Center and provide basic monitoring of software and switch status. The common server utilities include the Avaya Contact Center Update Manager, Log Archiver, Process Monitor, System Control and Monitor Utility, and Trace Control.
- Common database utilities: Utilities that are common to all servers in the Contact Center and are related to database functions such as backups and restores. The common database utilities are Database Maintenance and High Availability.
- CCMM database: The CCMM database contains all information about the multimedia contacts such as customer names, contact information, and contact content (if the content is text-based).

Contact Center Multimedia components

Contact Center Multimedia is part of the Contact Center Manager suite of applications. Contact Center Multimedia provides outbound, email, and Web communication features for the contact center.

Contact Center Multimedia consists of the following components:

- Contact Center Multimedia database—This component is installed on the Contact Center Multimedia server and is an InterSystems Caché database that stores all contact center activity. All incoming email, Web requests, and associated responses are stored in a structured format within the database. Information about Outbound campaigns are also stored in this database.
- Email Manager—This component is installed on the Contact Center Multimedia server. The Email Manager connects to the email server at regular intervals. During each connection, all configured mailboxes are accessed. Email from the customer is read from the email server, processed, and stored in the database. Outgoing email, generated from the email responses stored in the database, is sent to the email server.
- Outbound Campaign Management Tool—This component is installed on the Contact Center Multimedia server and is accessed using the Contact Center Manager Administration application. The Outbound Campaign Management Tool is used to create, modify, and monitor outbound campaigns. An outbound campaign is a series of outbound calls for one specific purpose, for example, a customer survey, or a sales promotion. Use the Outbound Campaign Management Tool for the following activities:
  - define campaign parameters
  - import and review call data
  - create agent call scripts
  - monitor campaign results
  - export campaign data

The Contact Center Manager Administration report tool provides information about agent and skillset states in real-time displays and historical reports.

- Web communications—The Web communications component includes a set of Web Services on the Contact Center Multimedia server for communication between the agent and the customer. A set of sample Web pages are installed on the Contact Center website showing how Web Services are used to implement Web pages to provide Web Chat (click to chat) and Scheduled Callback (click to talk) features.
- Agent Desktop interface—This component is installed on the Contact Center Multimedia server. Agents use Internet Explorer to connect to the Contact Center Multimedia server to retrieve the Agent Desktop interface. The Communication Control Toolkit pushes email, Web requests, outbound contacts, and voice calls to the Agent Desktop interface. The Agent Desktop interface uses Web services to retrieve email, Web requests, outbound campaign information, and customer details and history from the Contact Center Multimedia database. Web services are also used to send email replies and save outbound call details in the Contact Center Multimedia database.

  Email contacts are presented to agents through the Agent Desktop interface, where agents can;

  - verify customer information
  - access historical email to and from the customer
  - create responses to customer inquiries
  - provide a closed reason (if configured)

    When an outbound campaign is running, contacts are presented to agents through the Agent Desktop interface, where the agents can;
  - preview contact information
  - review call scripts (if configured)
  - save scripts
  - select a disposition code
- Contact Center Multimedia Administrator—This component is installed on the Contact Center Multimedia server. The Contact Center Manager Administration provides administrative and management capabilities.

Multimedia contacts processing

Contact Center receives multimedia contacts through two external interface points: the email server and the External Web server.

Email server contacts

Email server contacts are retrieved from a POP3 or IMAP capable email server using the Inbound Message Handler (IMH). The IMH runs at regular intervals. You can configure the settings for the IMH (such as the time between intervals and the number of email retrieved from each mailbox during each run) using Contact Center Manager Administration.

The IMH logs on to the mailboxes on the email server as listed in the Email Manager. It parses email in the mailboxes and stores them in the Contact Center Multimedia database. Any attachments

associated with an email are stored in the Inbound attachment folder, as specified in Contact Center Manager Administration. After an email is successfully stored in the Contact Center Multimedia database, it is deleted from the email server.

The IMH passes a received email to the Contact Center Multimedia rules engine, which applies rules relevant to the email based on the To address, and invokes the Outbound Message Handler (OMH) to send automatic responses, if any.

Contact Center Release 7.0 does not support Microsoft Exchange Server 2003.

Contact Center Release 7.0 supports only the following versions of Microsoft Exchange Server:

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013

External Web server transactions

Contact Center Multimedia receives contacts from the External Web server through the Contact Center Multimedia Web services. The Web services provide a Java API. This enables contacts to be written into the Contact Center Multimedia database, retrieved from the database, and have their status queried.

Contacts received through the Web services do not pass through the Rules Engine. The External Web server determines the skillset and priority assigned to the contact.

A set of sample pages is distributed through DevConnect to provide examples of how a Web server can access the Web services. You must create your own Web pages, with customized look, feel, and business logic.

Integration with Contact Center Manager Server

The Contact Center Multimedia system is integrated directly with Contact Center Manager Server through the OAM interface and through Open Queue. The OAM interface enables Contact Center Multimedia to access the information in Contact Center Manager Server about configured agents, supervisors, skillsets, and mapping these users to skillsets.

Contact Center Manager Server supports Open Queue. 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.

Enterprise Web Chat

Customers who require large numbers of Web chat sessions can use the Avaya Aura® Contact Center Enterprise Web Chat (EWC) SDK instead of Web Communications. If the customer requirement exceeds the maximum number of supported CCMM Web Communications simultaneous chat sessions, the customer should use EWC.

Contact Center supports EWC only on a standalone Multimedia Contact Server in a Unified Communications integration. Customers must develop an external Web chat server, using Avaya Solution Development Kits (SDKs). Agents handling EWC contacts can use Agent Desktop or a custom desktop. Customers must develop agent documentation and training to support any custom agent client they develop. Agents handling EWC contacts cannot use the Agent Browser application.

In CCMM, customers configure and license agents in the same way for both Web Communications and Enterprise Web Chat. Both solutions implement the same contact type.

EWC is a licensed feature. If Contact Center has an EWC license, CCMM implements only EWC for WC contacts. If Contact Center does not have an EWC license, CCMM implements only Web Communications for WC contacts. For Agent Desktop to handle EWC contacts, administrators must enable a setting on the Contact Center Multimedia (CCMM) Administration utility.

For more information on developing EWC solutions, see the EWC SDK documentation on the Avaya DevConnect site www.avaya.com/devconnect.

High Availability in an EWC solution

Contact Center supports High Availability (HA) in an EWC solution. The CCMM components use the normal HA switchover mechanisms. In addition, the EWC component uses an ejabberd cluster. In an EWC solution, a failure in the EWC component causes a switchover of the Multimedia Contact Server.

Operations performed on the server

In a multimedia Contact Center, Contact Center Multimedia collects contacts and assigns them to skillsets based on the rules the administrator configured. The Contact Center Manager server routes the contacts to the most appropriate available agent by using the applications scripted through Orchestration Designer. For the multimedia Contact Center to work efficiently for a contact type, you configure settings on both CCMS and CCMM.

For more detail about the relevant procedures, see *Avaya Aura® Contact Center Server Administration*.

This section contains the following topics:

- Handle contacts on page 122
- View and update customer information on page 124
- Create callbacks on page 124
- Report multimedia data on page 124
- Purge archived Multimedia contacts on page 125

Configure email settings

The email contact type is a licensed feature of the Contact Center. You must purchase email agent licenses to use this feature.

The Email Manager, built into the Contact Center Multimedia Administrator, regularly connects to the email server. During each connection, the Email Manager accesses all configured mailboxes, reads the message, routes the message according to the rules, and then stores the email information in the database. Outgoing email messages, generated from the email responses stored in the database, are sent to the email server.

Email is a text-based communication with clients using an email client such as Microsoft Exchange.

To configure email routing, you must create or configure the following items:

- Route points: Assign a route point to each email skillset (denoted by EM_). A route point is a location in the open queue that enables incoming contacts to be queued and treated by the application on CCMS.
- Inbound and outbound email servers: Configure the names and email transfer protocol for the email servers in your organization.
- Inbound email settings: Configure how frequently your Multimedia server scans the corporate server for new messages, and where email attachments are stored.
- Outbound email settings: Configure the outgoing email address or contact information when an email message is sent from your Contact Center. You can configure the signature by skillset.
- Language settings: Configure the characters (including Asian characters) used for outgoing messages. Some exceptions exist to the languages for your email messages; some components of the message, such as automatic responses and automatic signatures, are not converted to the sender's character set.
- Recipient mailboxes: Configure the mailbox details on your email server that you use to receive inbound email messages intended for the Contact Center.
- Email rules and rule groups: email rules determine how an email contact is routed based on information in or about the email message. Rules can review the recipient mailbox and route the contact based on where it was received (recipient mailbox), route contacts based on who sent the email (sender groups), apply treatments based on the time it was received (office hours and holidays), or route the contact based on particular words or phrases (keywords). One or more rules must be included in a rule group and attached to a recipient mailbox.

- System rules: Two system rules, a System Delivery Failure Rule and the Default Rule, are used for all recipient mailboxes to route contacts that are not otherwise handled by your administrator-created rules.
- Optional message treatments: You can configure email rules to send automatic responses based on the information in the email contact. The Email Manager automatically sends the response to the customer without routing the contact to an agent.
- Suggested message responses: You can configure email rules to present suggested responses to the agent who receives the contact. If you find that agents frequently use a particular suggested response to respond to an email that satisfies one rule, you can promote the suggested response to an automatic response for the rule.
- Barred addresses: Configure email addresses to which your Contact Center environment does not respond.
- Automatic phrases: You can create templates containing text that agents commonly use in email messages. These are shortcuts so that agents need not type large blocks of commonly used text. Agents can configure the template responses based on the contacts they receive.

For information about configuring the administration settings for email contacts, see *Avaya Aura® Contact Center Server Administration*.

If you use Microsoft Exchange 2007 or later on your email server, configure authentication settings. For more information, see *Avaya Aura® Contact Center Server Administration*.

Configure IM settings

In a SIP-enabled contact center environment, you can configure the settings for instant messages received in your Contact Center.

The automatic text for an instant message includes a welcome message for customers who initiate a session, and a disconnect message for the customer in the text-based conversation. You can configure default instant messages for individual skillsets.

To configure instant message routing, you must create or configure the following items:

- Route points: Assign a route point to each instant message contact type skillset (denoted with IM_). A route point is a location in the open queue for incoming contacts to be queued and processed by the application on CCMS.
- Default conversation text: The default conversation text includes a welcome message (based on the skillset chosen) and labels for the agent and customer in the text conversation.
- Message timers: Provide indicators to an agent and customer that no new action occurred in the current instant message conversation.
- Conversation log: Configure a log report of the conversation to send to the customer by email after the chat session is complete.
- Automatic phrases: You can create templates containing text that agents commonly use in instant messages. These are shortcuts so that agents need not type large blocks of commonly used text.

For information about configuring the administration settings for instant message contacts, see *Avaya Aura® Contact Center Server Administration*.

Configure Web communications settings

Use the Web Communications Manager to communicate with customers over the Internet. Agents and customers directly communicate in real-time in a two-way conversation by exchanging text messages using Javascript and frame-compliant Web browsers.

To configure Web communications routing, you must create or configure the following items:

- Route points: Assign a route point to each Web communication skillset (denoted by WC_). A route point is a location in the open queue that enables incoming contacts to be queued and run through the application on CCMS.
- Test and production Web servers: Configure the names and transfer protocol for the test Web server to perform trials for the new customer website, and the production Web server for the active Contact Center in your organization.
- Default conversation text: The default conversation text includes a welcome message (based on the skillset chosen) and labels for the agent and customer in the text conversation.
- Message timers: Provide indicators to an agent and customer that no new action occurred in the current Web communications conversation.
- Conversation log: Configure a log report of the conversation to send to the customer by email after the chat session is complete.
- Create multimedia presentations: Create multimedia presentations or groups of sites for customers who wait for an agent to respond. This feature, called Web On Hold, is configured in Contact Center Manager Administration.
- Automatic phrases: You can create templates containing text that agents commonly use in Web communications. These are shortcuts so that agents need not type large blocks of commonly used text.

For information about configuring the administration settings for Web communications contacts, see *Avaya Aura® Contact Center Server Administration*.

Configure outbound settings

The outbound contact type is a licensed feature of the Contact Center; you must purchase outbound agent licenses to use this feature. Outbound contacts are voice contacts made from the Contact Center to connect agents to customers; for example, for sales or marketing surveys. The Outbound Campaign Management Tool uses CCMS skillset routing to select an available agent and route the outbound contact to them. Agent Desktop provides the agent with outbound contact details and features such as call scripts, and uses CTI to initiate the outbound voice call.

In the CCMM Administration application on the Contact Center Multimedia server, you can configure the following items for outbound contacts:

- Route points: Assign a route point to each outbound skillset (denoted by OB_). A route point is a location in the open queue for contacts to be queued and treated by applications on CCMS.
- Campaign scheduler: The campaign scheduler determines when to queue contacts from the outbound campaign. When scheduling campaigns you must comply with all laws about if and when you can contact the customer.

For information about configuring the administration settings for outbound contacts, see *Avaya Aura® Contact Center Server Administration*.

The Outbound Campaign Management Tool (OCMT) is installed on the Contact Center Multimedia server and accessed using the Contact Center Manager Administration application. Administrators use the Outbound Campaign Management Tool to create, modify, and monitor outbound campaigns. Use the Outbound Campaign Management Tool to:

- define campaign parameters
- import and review call data
- create agent call scripts
- monitor campaign progress
- export campaign data

For more information about configuring the Outbound Campaign Management Tool, see *Avaya Aura® Contact Center Client Administration*.

Configure Social Network settings

Contact Center includes a new contact type, called a Social Networking contact, which provides closer integration with Avaya Social Media Manager (SMM) Release 6.2.11 or later. Previous releases of Contact Center integrated with SMM using a standard email contact.

Social Media Manager allows organizations to search through social networks to look for content relevant to their business. For example, a company might want to find positive comments about their products and services, so they can proactively reward customers who give them good feedback, or search for customer suggestions to improve their offerings. Social Media Manager can filter these social network entries, and determine which of these are relevant and actionable by an agent. SMM can then forward them to Contact Center for direct action by agents.

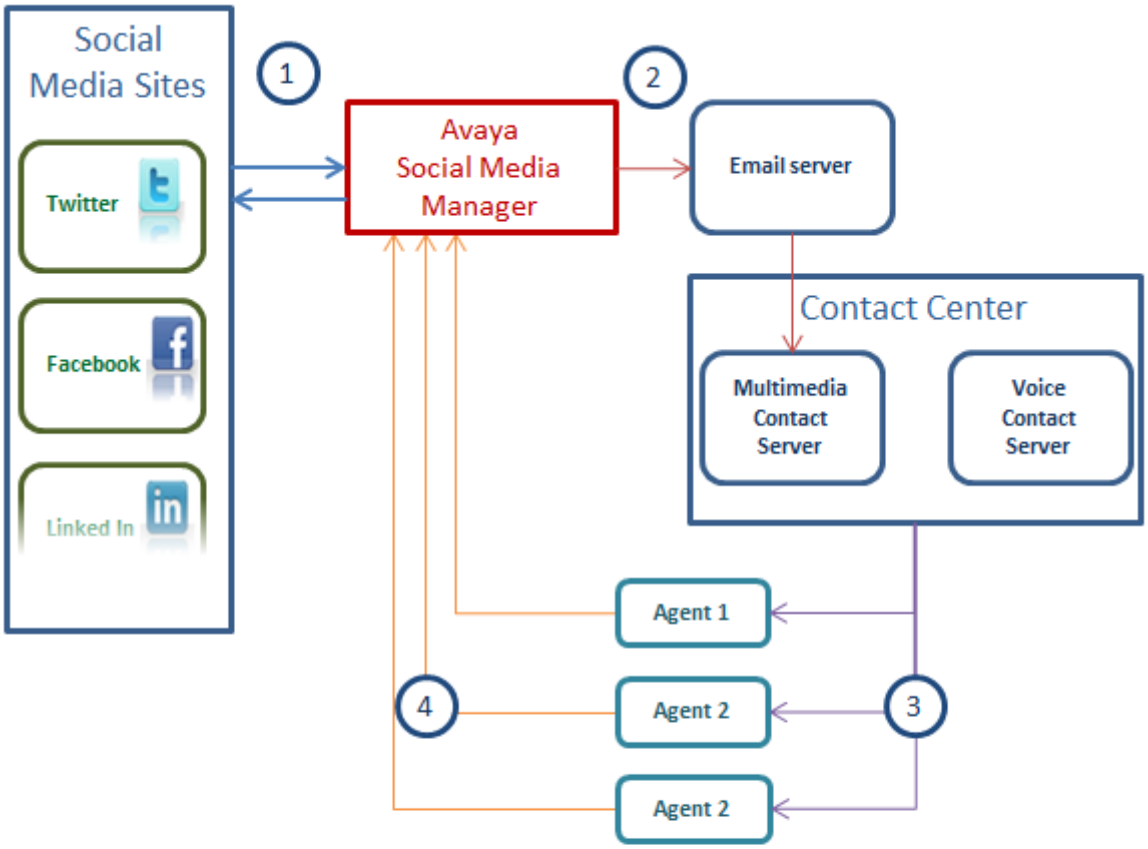
Social Media Manager forwards contacts to Contact Center by sending an email to a mailbox monitored by the CCMM Email Manager. The email that SMM sends contains the social networking content, and additional information. This information includes headers that Contact Center can use for routing, such as Language, Channel, Sentiment, and Relevance. There are also invisible headers such as a URL for the contact on SMM, which AD can use to pop the record.

Contact Center caters for routing the Social Networking contact type, so that Contact Center can provide improved reporting on Social Networking contacts. It also picks up information included with the social networking contact. The Multimedia Administration client includes all the settings required

to allow an administrator to configure Social Networking contacts and routing. The CCMM dashboard includes tracking of the Social Networking type.

Social Media Manager forwards actionable items by email to a one of more defined mailboxes. These mailboxes must be dedicated to emails from SMM, because Email Manager uses the mailbox as the only determinant of whether a contact is a Social Networking type. In Contact Center, in the Multimedia Administration tool, the administrator links this mailbox to a social networking skillset (SN_).

When the agent accepts the SN contact, they receive a pop up that allows them to log on to the SMM response interface so they can respond to the social contact directly from SMM.



1	Social Media feeds
2	Avaya SMM emails
3	Social Networking contacts
4	Avaya SMM response interface actions

Figure 2: Example of the Social Network contact flow

As a result of this contact workflow, Contact Center saves and reports on Social Networking contact routing details, but the details of the agents' responses are available only in SMM. Also, when processing a Social Networking contact, an agent must close the contact in SMM, and then separately close the SN contact in Agent Desktop.

An agent cannot transfer or conference an SN contact, nor can a supervisor/agent observe or barge in on an SN contact.

Social Media Analytics

Social Media Analytics is a cloud-based solution that monitors the social media feeds you select, searches for keywords you identify, and tracks conversations that matter to you. It pinpoints positive and negative posts about your products, your company, and your brand and then delivers them directly to your contact center. Social Media Analytics can convert relevant social media messages into email messages and route them to a mailbox monitored by Avaya Aura® Contact Center. Avaya Aura® Contact Center then applies email rules and routes these social media related email messages to skillsets and agents that are trained to process them. Agent responses are delivered using email to the Social Media Analytics mail store from where they are delivered to the appropriate social media gateway, such as Twitter or Facebook.

Agents use Agent Desktop software to process and respond to social media related email messages. The agents responses must conform to the standards of the original social media message. For example, the responses must remain within the 140 character limit of Twitter.

You can use Avaya Aura® Contact Center keyword analysis on the social media generated email messages to determine the skillset assignments and priority. You can also use the other email processing features such as *Supervisor Approva*l to process responses to social media.

Avaya recommends that you keep social media based email messages on separate skillsets from the regular email traffic. This approach allows granular reporting by targeting only the social media email skillsets.

Configure voice mail settings

Voice mail contacts use a feature on many voice mail systems that can convert a voice mail into a Wave file and attach it to an email message which it sends to a mailbox. The mail recipient can listen to the voice mail on their desktop PC.

In Contact Center Multimedia, the email messages generated by the voice mail system arrive in a mailbox monitored by the Email Manager, which converts them to contacts. An agent receiving a voice mail contact can listen to the voice mail and then choose how to respond to the customer—by voice call, email response, or Web chat.

The voice mail contact type is a licensed feature of the Contact Center. You must purchase voice mail agent licenses to use this feature.

To enable voice mail contacts, you must create or configure the following items:

- Voice mail skillset: Create at least one voice mail skillset for routing voice mail contact types. The CCMS installer automatically creates a default voice mail skillset (denoted by VM_ in the skillset name). You can use this or create new ones according to the needs of your Contact Center. You create voice mail skillsets in Contact Center Manager Administration (CCMA).
- Route points: Assign a route point to each voice mail skillset (denoted by VM_). A route point is a location in the open queue for incoming contacts to be queued and processed by the application on CCMS.
- Mailbox settings: Configure the names and email transfer protocol for the mailbox from which Email Manager takes the voice mail contacts. You must ensure that the voice mail server is configured to forward voice mail messages to a mailbox.
- Sender address settings: Parse the voice mail contact sender address to extract the telephone number of the customer who left the voice mail. This allows the agent receiving the contact to call the customer directly using Agent Desktop CTI controls.

For information about configuring the administration settings for scanned document contacts, see *Avaya Aura® Contact Center Server Administration*.

If you use Microsoft Exchange 2007 or later on your email server, configure authentication settings. For more information, see *Avaya Aura® Contact Center Server Administration*.

Configure scanned document settings

Combined with Contact Center Multimedia, the email messages generated by the document imaging servers arrive in a mailbox monitored by the Email Manager, which converts them to contacts. An agent receiving a scanned document contact can view the content of the document and then choose how to respond to the customer—by voice call, email response, Web chat, or a response through the document imaging server. To respond through the document imaging server, the agent uses an email editor to compose the response, and the Email Manager forwards this to the document imaging server for the customer.

The scanned document contact type is a licensed feature of the Contact Center. You must purchase scanned document agent licenses to use this feature.

To enable scanned document contacts, you must create or configure the following items:

- Scanned document skillset: Create at least one scanned document skillset to route scanned document contact types. The CCMS installer automatically creates a default scanned document skillset (denoted by SD_ in the skillset name). You can use this or create new ones according to the needs of your Contact Center. You create scanned document skillsets in Contact Center Manager Administration (CCMA).
- Route points: Assign a route point to each scanned document skillset (denoted by SD_). A route point is a location in the open queue for incoming contacts to be queued and processed by CCMS.

- Mailbox settings: Configure the names and email transfer protocol for the mailbox from which the Email Manager takes the scanned document contacts. You must ensure that the document imaging server is configured to forward scanned document messages to this mailbox.
- Reply address settings: Specify the mailbox that Contact Center Multimedia uses to send a reply if the agent creates a text response to the scanned document contact. The document imaging server picks up this email response and converts it to an image file. The document imaging server must be configured to monitor this mailbox for responses to convert.

For information about configuring the administration settings for scanned document contacts, see *Avaya Aura® Contact Center Server Administration*.

If you use Microsoft Exchange 2007 or later on your email server, configure authentication settings. For more information, see *Avaya Aura® Contact Center Server Administration*.

Configure SMS text settings

To handle SMS text contacts, Contact Center Multimedia operates with an SMS-email gateway. The gateway converts SMS messages into email messages and forwards these to a mailbox. The Email Manager monitors the mailbox and picks up the email messages, and converts them to SMS contacts. An agent receiving an SMS contact can view the content of the SMS message, and then choose how to respond to the customer—by voice call, email response, web chat, or SMS response. For an SMS message, the agent uses an email editor to compose the text, and the Email Manager forwards this to the gateway to send to the customer.

The SMS contact type is a licensed feature of the Contact Center. You must purchase SMS agent licenses to use this feature.

To configure SMS contacts, you must create or configure the following items:

- SMS skillset: Create at least one SMS skillset to route SMS contact types. The CCMS installer automatically creates a default SMS skillset (denoted by SM_ in the skillset name). You can use this or create new ones according to the needs of your Contact Center. You create SMS skillsets in Contact Center Manager Administration (CCMA).
- Route points: Assign a route point to each SMS skillset (denoted by SMS_). A route point is a location in the open queue for incoming contacts to be queued and processed by CCMS.
- Mailbox settings: Configure the names and email transfer protocol for the mailbox from which Email Manager takes the SMS contacts. You must ensure that the SMS gateway is configured to forward SMS messages to this mailbox.
- Sender address settings: Parse the SMS contact sender address to extract the telephone number of the customer who sent the SMS. This allows the agent receiving the contact to call the customer directly using Agent Desktop CTI controls.
- Reply address settings: Specify the mailbox that Contact Center Multimedia uses to send a reply if the agent creates a text response to the SMS contact. The SMS gateway picks up this email response and converts it to an SMS message. The SMS gateway must be configured to monitor this mailbox for responses to convert.

For information about configuring the administration settings for SMS text contacts, see *Avaya Aura® Contact Center Server Administration*.

If you use Microsoft Exchange 2007 or later on your email server, configure authentication settings. For more information, see *Avaya Aura® Contact Center Server Administration*.

Configure faxed document settings

Fax contacts use a feature on many fax servers to convert a fax into an image file and attach it to an email message, which it sends to a mailbox. The mail recipient can view the fax content on their desktop PC.

Combined with Contact Center Multimedia, the email messages generated by the fax server arrive in a mailbox monitored by the Email Manager, which converts them to contacts. An agent receiving a faxed document contact can view the content of the fax and then choose how to respond to the customer—by voice call, email response, Web chat, or fax. If they respond with a fax, the agent uses an email editor to compose the fax message, and the Email Manager forwards this to the fax system to send to the customer.

The faxed document contact type is a licensed feature of the Contact Center. You must purchase fax agent licenses to use this feature.

To enable faxed document contacts, you must create or configure the following items:

- Fax skillset: Create at least one fax skillset to route fax contact types. The CCMS installer automatically creates a default fax skillset (denoted by FX_ in the skillset name). You can use this or create new ones according to the needs of your Contact Center. You create fax skillsets in Contact Center Manager Administration (CCMA).
- Route points: Assign a route point to each fax skillset (denoted by FX_). A route point is a location in the open queue for incoming contacts to be queued to and processed by the application on CCMS.
- Mailbox settings: Configure the names and email transfer protocol for the mailbox from which Email Manager takes the fax contacts. You must ensure that the fax server is configured to forward faxes to this mailbox.
- Sender address settings: Parse the fax contact sender address to extract the fax number of the customer who sent the fax. This number can be used to fax a reply to the customer.
- Reply address settings: Specify the mailbox that Contact Center Multimedia uses to send a reply if the agent creates an email response to the fax contact. The fax server picks up this email response and converts it to a fax. The fax server must be configured to monitor this mailbox for email messages to convert.

For information about configuring the administration settings for faxed document contacts, see *Avaya Aura® Contact Center Server Administration*.

If you use Microsoft Exchange 2007 or later on your email server, configure authentication settings. For more information, see *Avaya Aura® Contact Center Server Administration*.

Configure Agent Desktop settings

Use the CCMM Administration component of Contact Center Manager Administration to configure how Agent Desktop presents and handles contacts.

You can configure the following properties:

- View the current agent details, such as first name and last name and change their passwords.
- Configure maximum open duration: the time in hours and minutes for a contact to remain open on a desktop without activity. When this time expires, Contact Center places the contact into the New state. The default setting is one hour, the minimum is 10 minutes, and the maximum is 12 hours. Maximum open duration does not apply to voice or Web Chat (Web Communications) contacts.
- Configure hot desking, the function in your Contact Center where an agent can sit at a different desk for each shift and log on to Agent Desktop. With hot desking enabled and properly configured, when agents start Agent Desktop, they automatically map to the relevant terminal and addresses without user intervention. When you configure hot desking for a Citrix environment, agents are challenged with a dialog box asking them to identify their workstation.
- Configure the Callback time, the default time in days, hours, and minutes, to wait before re-presenting a pending contact to agents. Agents place contacts into the pending state when they wait for more information to complete the contact. The default range provides the limits for the callback time. Agents choose the actual value in the Agent Desktop application when they reschedule the contact.
- Specify the maximum size of the attachments (including inline attachments) that an agent can attach to an email response.
- Configure whether the Agent Desktop is brought to front, or given focus, when a new contact arrives. If Bring to Front is enabled, the Agent Desktop is brought to the front upon arrival of a new contact. If Bring to Front is disabled, the Agent Desktop plays a warning sound and the toolbar flashes, but it is not brought to the front. You can also configure the Agent Desktop to have focus (the Agent Desktop window is the active window) when it is brought to the front.
- Configure your Agent Desktop so that agents hear a beep when a contact arrives at their desktop. To use this feature, each agent workstation must have a sound card installed.
- In AML-based solutions, choose to have the agent terminal either left in an idle state (so that the agent can still receive incoming DN calls) or in a busy state when logged off. By default, Logoff Terminal State is assigned to Idle.
- When you enable Agent Skillset Partitioning, an agent searching for contacts sees matching contacts only in the in-service skillsets that the agent is assigned to. If Agent Skillset Partitioning is enabled, agents see only the in-service skillsets assigned to them. For a skillset to be in-service, at least one agent must be logged in and not using standby priority. If Agent Skillset Partitioning is disabled, agents see all skillsets in Contact Center.
- Configure Agent Desktop Resources to create specific reason codes for Multimedia contact types.

For information about configuring the administration settings for Agent Desktop for multimedia contacts, see *Avaya Aura® Contact Center Server Administration*.

Configure General settings

Use the CCMM Administration component of Contact Center Manager Administration to configure general settings for your Multimedia Contact Center.

You can configure the following properties:

- Server settings: Change server ports (if required), and add servers to the solution. The core Contact Center servers automatically appear in this window. You can add some server types such as LDAP, Customer Interface, or Standby servers.
- Skillset settings: Configure a route point for each skillset, and optionally create automatic signature text for email (EM_) type skillsets.
- Administration settings: Create administrator accounts for custom Web Communications applications.
- Agent settings: Change agent passwords for the Agent Desktop, and specify whether agents can delete text from text based-contacts. (For example, agents can delete credit card details from email contacts.)
- General settings: Specify your Contact Center license type and change the password for the mmReport user. (The mmReport user is configured in the Multimedia database and has access to data within that database to pass reporting information to Contact Center Manager Administration. If you change the password here you must update the password on the CCMM server record in CCMA.)
- Contact Center Hours: Create templates for Contact Center opening hours. You apply a template to a skillset to define when the Contact Center is open for contacts to arrive to that skillset. Specifying open hours ensures accurate reporting of Service Level Agreements for multimedia contact types, because CCMM now subtracts closed hours from the contact queueing duration.

For information about configuring the general settings for multimedia contacts, see *Avaya Aura® Contact Center Server Administration*.

Handle contacts

Agents use the Agent Desktop application to process email, Web communications, instant message, outbound, SMS text, scanned document, faxed document, voice mail, and POM contacts, depending on the applications your Contact Center is licensed to handle.

For more information about the Agent Desktop, see *Using Agent Desktop for Avaya Aura® Contact Center* .

For voice contacts, the agent can handle the incoming contacts, such as accepting the incoming contact, transferring the contact to another agent, and performing required duties to complete a contact.

For multimedia contacts, the agent can handle the incoming and outgoing contacts including accepting the incoming contact, dealing with the contact, such as talking to the customer, or sending them information in a text format, and performing other duties required to complete the contact.

Using the Multiplicity feature, an agent can work on any of the following contacts simultaneously:

- Voice call
- Email
- Fax
- Instant Message
- OpenQ, contact center multimedia generic contact
- Scanned Document
- SMS
- Social Networking
- Web Communications
- Voice mail

Multiplicity is configured and assigned to agents using Multiplicity Presentation Class (MPC) in Contact Center Manager Administration (CCMA). A MPC is a collection of multiplicity configuration options. Every agent must be assigned an MPC. A default MPC is not modifiable and allows an agent handle a single contact.

MPC configuration options include the following:

- maximum number of concurrent multimedia contacts the agent can handle
- time to wait before presenting the next contact to the agent
- check box to allow presentation of a voice call while working on multimedia contacts
- check box to allow presentation of multimedia contact while active on a voice call
- maximum number of contacts that can be presented for each contact type
- maximum number of contacts that can be presented for individual skillsets

The maximum number of concurrent multimedia or non-voice contacts that an agent can be assigned is five. The consumption of agent licenses in not affected by multiplicity. An agent continues to consume agent licenses at logon for each contact type assigned to the agent. The maximum number of contacts processed simultaneously is limited to 3000 to ensure agent engineering limits are not exceeded.

If a multiplicity-enabled agent is handling multiple contacts and their multiplicity privileges are disabled, no new contacts are presented to the agent until the agent has released all of their existing contacts. Contacts are not dropped or automatically released. If a voice contact is released before the multimedia contacts, agents are reported as "on break" on Real Time Displays (RTD). Agents

remain in this state until the last multimedia contact is released. After the last multimedia contact is released the agent is set to idle after the break time.

When multiplicity is enabled, a voice contact is always presented first to an agent even if it arrives with a priority lower than a multimedia contact. A multiplicity–enabled agent handles the voice contact first because it is a real-time contact. For example, if all the agents are busy and a high priority multimedia contact arrives, and if a lower priority voice contact arrives before the multimedia contact is handled, then the voice contact is presented to the first available agent.

If a blended agent is notified with a multimedia contact, the voice queue position remains unchanged, but the first 10 seconds after the contact is assigned, the blended agent is marked as busy in the voice queue. After the 10–second interval, the agent is marked as idle in the voice queue, but marked as busy in the multimedia queue. This ensures that the agent is not assigned a multimedia contact and a voice contact at the same time.

If your Contact Center solution is configured for routed IM contacts, Avaya recommends that you enable multiplicity to ensure accurate real-time reporting.

View and update customer information

In addition to handling multimedia contacts, agents can also use the Agent Desktop application to update customer information for existing customers, create new customers based on information received during a contact, and track the details of all previous contacts with a particular customer.

For more information about the Agent Desktop, see *Using Agent Desktop for Avaya Aura® Contact Center* .

Create callbacks

By using the Agent Desktop, agents can create a callback record to contact a customer later based on the information received during a different type of contact, such as the time the customer is available and the telephone number to call.

For more information about the Agent Desktop, see *Using Agent Desktop for Avaya Aura® Contact Center* .

Report multimedia data

You can use the Real-Time Reporting and Historical Reporting features of Contact Center Manager Administration to create and run real-time and historical reports for all multimedia contact types.

In addition, the new Contact Center Multimedia Administration tool includes summary reports for each contact type.

You can view real-time reports using the Agent Desktop Displays application where you can view the following items:

- six nodal real-time displays for single Contact Center Manager Server sites
- three network consolidated real-time displays for a network of Contact Center Manager Server sites

You can view historical reporting on the Contact Center Manager Administration server. You must configure the reporting server name and password in the Multimedia Administrator application.

The Standard Agent Real-Time Display (RTD) provides a tabular display of logged-on agents. For a multiplicity-enabled agent, a separate row appears for each contact the agent handles. If the agent is not working at full capacity, an additional row indicates idle capability as the agent awaits more contacts. Blended agents have special representation in the agent RTD. The voice row is always present and represents the activity of the voice terminal. All other rows for the agent represent multimedia activity. Only one multimedia row is active to represent the contact that currently has focus in the agent desktop. All other rows show the state as Held. New agent efficiency and contact summary reports are available to report on multiplicity operation. Using these reports, administrators can review the efficiency of the multiplicity configuration.

Multimedia data management and purging

Avaya Aura® Contact Center includes two databases for multimedia contacts, the MULTIMEDIA database and the OFFLINE database. The MULTIMEDIA database contains all active contacts. The OFFLINE database maintains an archive of contacts from the MULTIMEDIA database. This includes contacts both currently in and cleared from the MULTIMEDIA database.

A CCMM background offline synchronization task updates the OFFLINE database. Every night, the offline synchronization task automatically copies modified contacts from the MULTIMEDIA database to the OFFLINE database. It is a background task in the Caché database, and administrators do not configure it. The synchronization task keeps the OFFLINE database closely synchronized with the MULTIMEDIA database for contacts that have not changed, such as contacts in a Closed state. This enables administrators to keep the MULTIMEDIA database efficient by regularly clearing it of closed contacts.

Administrators create rules and schedules to clear closed contacts from the MULTIMEDIA database. This keeps the MULTIMEDIA database small, while also allowing for historical reporting across all the contacts in both the MULTIMEDIA and the OFFLINE databases. The MULTIMEDIA database contains all the new contacts and contacts on which agents are working. The OFFLINE database contains the archived multimedia contacts. It is accessible for custom reporting, but is not accessible to agents, standard reporting, or screen pop applications. Custom reporting on the OFFLINE database must use an ODBC DSN referencing the OFFLINE namespace.

Administrators can create scheduled cleanup tasks to clear records from the MULTIMEDIA database. Each cleanup task uses a rule, defined by the administrator, to select the contacts to clear. A scheduled cleanup task checks whether each contact matching the rule is archived in the OFFLINE database. If the contact is archived, the task clears it from the MULTIMEDIA database. If

the contact is not archived, the cleanup task copies the contact to the OFFLINE database and then clears it from the MULTIMEDIA database.

The Multimedia Data Management utility includes a Restore function. The Restore function allows administrators to see all the scheduled cleanup tasks previously performed. Administrators can restore the contacts cleared by a scheduled cleanup task. The restore is not selective: it restores all the contacts that the scheduled cleanup task cleared.

Multimedia Database sizing and limits

The MULTIMEDIA database supports a maximum of 1,000,000 contacts. Administrators must regularly cleanup contacts from the MULTIMEDIA database to stay below this limit. The maximum size of the OFFLINE database is 70% of the Multimedia database drive size. If the OFFLINE database fills up, administrators can either increase the Multimedia database disk space, or change the OFFLINE database purge interval.

Administrators can check the current sizes of the MULTIMEDIA and OFFLINE databases in the CCMM Data Management tool.

When the OFFLINE database reaches 75% of the maximum size, CCMM logs this event to the log file. When the Offline database grows above 90% of the maximum size, CCMM logs events to the event viewer. If the Offline database exceeds 95% of the maximum size, CCMM stops automatically synchronizing contacts from the MULTIMEDIA database, and prevents administrators from running manual or scheduled cleanups.

Administrators can purge contacts from the OFFLINE database to reduce the database size. Administrators specify the age at which AACC purges closed contacts. AACC runs a purge task every day, and purges contacts that meet the age criteria. Administrators cannot recover a purged contact other than by restoring a backed-up OFFLINE database.

Database changes for upgrades from Release 6.3

Contact Center added the OFFLINE database in Release 6.4. Contact Center solutions installed before this Release have only a single multimedia contact database, the MULTIMEDIA database, with a different purging and archiving mechanism.

When you upgrade Contact Center from Release 6.3 or earlier (either by migrating the contact center or applying Service Pack 12), Contact Center installs the OFFLINE database and the associated Data Management tasks and tools. This impacts the disk space usage on the multimedia database drive until scheduled cleanups and purging are running effectively on the upgraded system.

For example, if you upgrade Contact Center, and do not set up any scheduled cleanup tasks, on the first night after the upgrade the disk space usage doubles. This is because the CCMM Offline Synch task copies all the contacts from the MULTIMEDIA database to the OFFLINE database.

To prevent excess disk space usage on a system upgraded from Release 6.3 or earlier:

- Archive contacts from the Release 6.3 MULTIMEDIA database before starting the upgrade, to reduce the size of the database.
- After the upgrade, use the CCMM Data Management tool to check the database usage on the upgraded system.
- Configure cleanup rules and scheduled tasks in the CCMM Data Management tool so that CCMM can start clearing closed contacts from the MULTIMEDIA database.

Backing up and restoring the OFFLINE database

For scheduled backups, Contact Center automatically backs up the OFFLINE database. However, Contact Center stores the OFFLINE database in a separate file to the other application databases. Ensure that you include the OFFLINE database backup files for long term storage in your data retention policy.

For manual backups, Contact Center allows you to include or exclude the OFFLINE database. Excluding the OFFLINE database reduces the backup duration, and is useful where you do not need to back up the OFFLINE database for storage. For example, if you are backing up the database before patching Contact Center, you can exclude the OFFLINE database.

If you restore an OFFLINE database, it can contain contacts that CCMM purged since the date of the backup. In such cases, CCMM purges the contacts again when the background purge task runs. If you restored an OFFLINE database to access a purged contact you must restore the contact to the MULTIMEDIA database. Then reopen the contact you want to access so that a scheduled cleanup task does not clear it from the MULTIMEDIA database.

Archives from previous Releases

You can restore an archive from a previous release if you want to recover an old contact. Use the legacy Multimedia Archive/Restore Utility to restore old archives. Do not use the legacy utility for any other data management operation.

Attachment storage

For email contacts stored in the MULTIMEDIA database, CCMM stores attachments in the email attachments folders on the server hard disk. When the CCMM Offline Synch task copies a contact to the OFFLINE database, CCMM stores any associated attachments in a binary object in the OFFLINE database. As a result, when a contact exists in both the MULTIMEDIA and the OFFLINE databases, CCMM stores the attachment twice.

Avaya recommends that you enforce a limit on the incoming attachment size on your email servers, based on your business requirements. This helps prevent the use of storage on the CCMM server by SPAM email messages with large attachments.

High Availability

In a High Availability solution, the active and standby servers have a MULTIMEDIA and an OFFLINE database. Contact Center shadows the MULTIMEDIA database only. On the standby server, the CCMM Offline Synch task synchronizes the OFFLINE database with the replicated MULTIMEDIA database.

In all High Availability procedures that require backing up and restoring databases, include the OFFLINE database in the backup and the restore.

Hot Patching:

If you are applying a Contact Center patch that supports Hot Patching, the following considerations apply:

- If you are going to patch the active and standby servers within 24 hours of each other, exclude the OFFLINE database in the backup and restore procedures.
- If you are going to patch the active and standby servers more than 24 hours apart from each other, include the OFFLINE database in the backup and restore procedures.

Optional configuration tools

You can install optional components on the Contact Center Multimedia server. The following topics describe the purpose of each component:

- Contact Center Standby server on page 128
- Web services on page 128
- Open interfaces for email on page 128

Contact Center standby server

You can install a standby server to shadow the Caché database and provide a quick recovery if the active Contact Center Multimedia server fails. All multimedia services are disabled on the standby server until it is required to run as the active server. If the server implements Enterprise Web Chat (EWC), some services remain running. For more information about the standby servers, see High Availability fundamentals on page 148.

Web services

The Outbound Open Interfaces provide an open interface to integrate third-party applications with Outbound Campaigns. The open interfaces provide the following functions for external applications:

- ability to add contacts to an existing campaign
- ability to close contacts created as part of a campaign before they are complete

For more details, see the SDK documentation.

Open interfaces for email

You can develop a custom Web service that the Email Manager can call when an email message is processed. The custom Web service can perform custom tasks such as manipulating the originating email and modifying the rule routing options.

The Email Manager retrieves the email from the mailbox and performs keyword analysis on the contents of the email. The keyword analysis sets a particular rule. The rule sets a number of properties such as auto-response, skillset, priority. While configuring the rule, you can choose a Web service to be associated with the rule. This custom Web service allows users to provide their own customizations to email messages and their associated properties based on their business needs. You can use the custom Web service to manipulate both the content and the routing of the email message.

You can use C# or Java to develop a custom Web service. The custom Web service must conform to Web Service Description Language (WSDL) standards.

Note:

You must not host the custom Web service on the Avaya Aura® Contact Center server.

For more information on configuring open interfaces for email, see *Avaya Aura® Contact Center Server Administration*.

Chapter 11: Avaya Aura® Media Server

Avaya Aura® Contact Center uses the media processing capabilities of Avaya Aura® Media Server to:

- Conference customer and agent speech paths with media treatments.
- Conference additional parties, or features, with customer or agent calls.
- Play locale-specific media files for announcements and treatments.
- Play locale-specific media files for signaling tones, such as ringback and busy.
- Play notification tones for features such as barge-in and agent observe.
- Play streamed music into contact center calls.
- Play scripted music into contact center calls.
- Support Agent Greeting.
- Support SIP Call Recording.
- Collect DTMF digits.

Avaya Aura® Media Server is the termination and origination point for Real-time Transport Protocol (RTP) and Secure Real-time Transport Protocol (SRTP) streams between the customer, media treatments, and the agent.

Avaya Aura® Contact Center requires a license for each Avaya Aura® Media Server instance in the solution. An Avaya Aura® Media Server High Availability pair of server requires two instance licenses.

Avaya Aura® Contact Center integrates with Avaya Aura® Media Server using Media Server Markup Language (MSML) based communication. Avaya Aura® Contact Center and Avaya Aura® Media Server use the MSML XML language 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.

Avaya Aura® Media Server provides a MSML-based service type named ACC_APP_ID. Configure Avaya Aura® Media Server instances, and the ACC_APP_ID service type, in Contact Center Manager Administration (CCMA).

Avaya Aura® Media Server on Linux automatically installs Access Security Gateway support for new and upgraded systems. Access Security Gateway (ASG) provides a mechanism for Avaya support personnel to access customer servers without needing the customer or business partner to supply log on credentials. Authorized Avaya support personnel can use Access Security Gateway in conjunction with Avaya Secure Access Link (SAL) to remotely access Avaya Aura® Media Server on Linux.

Avaya Aura® Media Server is supported on the Windows Server 2012 R2 operating system when installed coresident with Avaya Aura® Contact Center. Standalone Avaya Aura® Media Server is not supported on the Windows Server operating system.

Standalone Avaya Aura® Media Server is supported on the Red Hat Enterprise Linux 6.x 64-bit operating systems.

Standalone Avaya Aura® Media Server for Avaya Aura® Contact Center is also available as a VMware Open Virtual Appliance (OVA). The Avaya Aura® Media Server OVA creates and configures a virtual machine containing Avaya Aura® Media Server software. The virtual machine contains a Linux operating system, hard disk drive, third-party components, system configuration, firewall settings, and Avaya Aura® Media Server application software.

The Avaya Aura® Media Server software uses the host server's on-board CPUs to perform the media processing.

Avaya Aura® Media Server media files and media management

Avaya Aura® Media Server media files are WAV audio files that contain speech, music, feature tones, or signaling tones. Avaya Aura® Media Server supports custom (customer generated) media files and default (canned) media files.

Use Contact Center Manager Administration (CCMA) *Prompt Management* to configure the media files for the following:

- Locale-specific voice announcement and prompt files
- Scripted music files
- Barge-in notification tone
- Observation notification tone
- Call Force Answer Zip notification tone
- Custom Zip notification tones
- Whisper Skillset announcement

Avaya Aura® Media Server provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. Create your Avaya Aura® Media Server media files using this encoding.

Content Store

The Avaya Aura® Media Server Content Store provides a persistent storage capability for configuration data and media files. You use the Contact Center Manager Administration (CCMA) *Prompt Management* interface to configure and manage the contents of the Content Store. If you have more than one Avaya Aura® Media Server, you can designate one server to be the primary Avaya Aura® Media Server. You can then configure the other Avaya Aura® Media Servers to replicate (copy) the configuration data and media files from the Content Store on the primary Avaya

Aura® Media Server. This configures all of the Avaya Aura® Media Servers with the same media files and allows them to provide a pool of common media processing resources. Content Store replication also provides storage resiliency, if one Avaya Aura® Media Server fails the remaining Avaya Aura® Media Servers are configured correctly and can continue processing media and contact center calls.

Custom media

Avaya Aura® Media Server stores (customer generated) custom media files in a media Content Store. Typically, you record your own announcements and using CCMA *Prompt Management*, store the WAV media file recordings in the Avaya Aura® Media Server Content Store.

The music media files used to provide scripted music in Orchestration Designer applications are another example of custom media.

In an Avaya Aura® Media Server cluster-based solution, you configure your custom media files only on the primary Avaya Aura® Media Server Content Store. The custom media files are automatically replicated to all other Avaya Aura® Media Servers in the cluster.

In Avaya Aura® Media Server Mission Critical High Availability-based solutions, you configure your custom media files only on the primary server of the Avaya Aura® Media Server Content Store Master Pair. The custom media files are automatically replicated to the backup Avaya Aura® Media Server, and to all other Avaya Aura® Media Server High Availability pairs configured in the solution.

Custom media organization

Avaya Aura® Media Server organizes custom media in the Content Store within a content namespace. A content namespace is a logical area in the Content Store. The content namespace name must match the contact center SIP domain name; that is, the Local SIP Subscriber Domain Name in Contact Center Manager Server – Server Configuration.

Within the content namespace you use content groups to subdivide the media into logical groups. You can create locale-specific content groups for treatments such as RAN.

Avaya Aura® Media Server supports the following locales:

Locale	Language	Country
de_de	German	Germany
en_ca	English	Canada
en_gb	English	United Kingdom
en_ie	English	Ireland
en_in	English	India
en_us	English	United States
es_es	Spanish	Spain
es_mx	Spanish	Mexico
fr_ca	French	Canada
fr_fr	French	France
it_it	Italian	Italy

Locale	Language	Country
ja_jp	Japanese	Japan
ko_kr	Korean	Korea
pt_br	Portuguese	Brazil
ru_ru	Russian	Russia
zh_cn	Chinese (Simplified)	China
zh_tw	Chinese (Simplified)	Taiwan

To use treatments in Orchestration Designer (OD) flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the media files in the Avaya Aura® Media Server locale-specific content group. The OD flow applications or scripts reference these routes to access the treatment files on the Avaya Aura® Media Server.

Music media organization

Avaya Aura® Media Server stores music media files in content groups in a reserved namespace, named *streamsource*, in the Content Store. These content groups can be collections of music files of a specific genre, pop, rock, or classical for example, or any other group classification. To use scripted music in OD flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to one of the Avaya Aura® Media Server streamsource content groups. The OD flow applications or scripts reference these routes to access the scripted music provided by Avaya Aura® Media Server.

Default media files

Avaya Aura® Media Server contains a set of country and language specific default media files for all supported locales. The default media files contain numerical values, busy tones and ring-back tones. You can use these default “canned” media files in your Contact Center solution, or you can replace them with your own recordings.

The following are examples of the Avaya Aura® Media Server default or canned locale specific media files:

- Single digit playback (zero.wav, one.wav, two.wav ... nine.wav)
- Busy tone wav file (busy.wav)
- Ringback wav file (ringback.wav)

The default media files are stored in the *prompts* section of the Avaya Aura® Media Server Content Store. The canned media files are stored in Linear 16-bit PCM recording format. You use Avaya Aura® Media Server Element Manager to replace the existing default “canned” media files with your own files.

Default media files are stored in the Avaya Aura® Media Server Content Store and are therefore replicated to other Avaya Aura® Media Servers in resilient or clustered solutions.

The following languages use different WAV file names for the following numbers:

	Zero	One	Two	Three	Four	Five	Six	Seven	Eight	Nine
ja_jp Japanese	zero	ichi	ni	san	yo	go	roku	nana	hatchi	kyu
ko_kr Korean	young	il	yi	sam	sa	o	yuk	chil	pal	gu
zh_cn & zh_tw Chinese	ling	yi	er	san	si	wu	liu	qi	ba	jiu
ru_ru Russian	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9

All audio media files must have a .wav file name extension, for example hatchi.wav, jiu.wav, and seven.wav. The extension is removed when you upload the file using Element Manager.

Network configurations

You can configure Avaya Aura® Media Server in a number of ways, depending on the requirements of your contact center. The different configurations affect the number of servers required, the operating system required, and the media Content Store configuration.

Contact Center supports the following Avaya Aura® Media Server network configurations:

- Co-resident with Contact Center software on a Microsoft Windows 2012 R2 server.
- Standalone Avaya Aura® Media Server, for lower capacity contact centers.
- Standard Avaya Aura® Media Server cluster, for higher capacity contact centers, and for providing load sharing with content replication.
- Standalone Avaya Aura® Media Server High Availability pair, for call protection in a Contact Center HA environment.
- Multiple Avaya Aura® Media Server High Availability pairs, for call protection with higher capacity and content replication in a Contact Center HA environment.
- Standard Avaya Aura® Media Server cluster or a HA pair at a Remote Geographic Node (RGN), to support Mission Critical HA solutions with RGN.

You cannot combine these network configurations in a single contact center solution.

Standalone Avaya Aura® Media Server

Standalone Avaya Aura® Media Server is supported only on the Linux operating systems. You cannot install other applications on the Avaya Aura® Media Server Linux server.

In Contact Center Manager Administration, you configure the Avaya Aura® Media Server as a media server and assign it to provide media services. When you configure a Media Server in Contact

Center Manager Administration, Contact Center License Manager pushes license keys to that Avaya Aura® Media Server. When Avaya Aura® Contact Center uses WebLM licensing, Avaya Aura® Media Server does not require a license file or any specific licensing configuration.

Avaya Aura® Media Server cluster

An Avaya Aura® Media Server cluster is a collection of Avaya Aura® Media Server nodes that work closely together. Avaya Aura® Media Server clusters offer improved redundancy. An Avaya Aura® Media Server cluster shares the following resources:

- Cluster Primary and Secondary Nodes
- Persistent Content Storage
- Redundant License Servers

The cluster performs automatic Content Store replication of system and application configuration data, as well as media content, so you must configure the same media applications on all Avaya Aura® Media Server servers in the same cluster.

An Avaya Aura® Media Server cluster has:

- One Avaya Aura® Media Server designated as the primary Avaya Aura® Media Server
- One Avaya Aura® Media Server designated as the secondary Avaya Aura® Media Server
- Up to six Avaya Aura® Media Servers, each designated as a standard Avaya Aura® Media Server

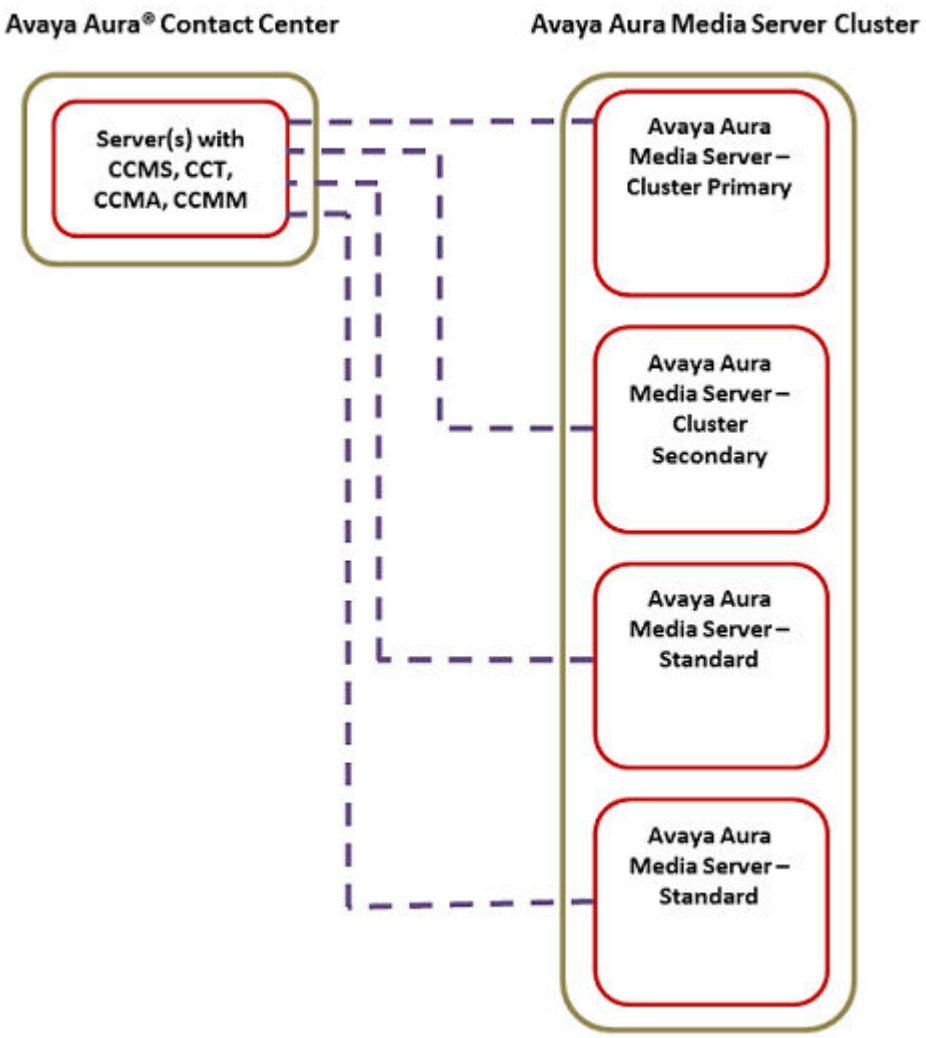


Figure 3: Avaya Aura® Media Server cluster

In this deployment, you configure the Avaya Aura® Media Server servers in a cluster. This allows you to perform configuration on the Primary server only, and the configuration automatically replicates to the other Avaya Aura® Media Servers in the cluster deployment.

In Contact Center Manager Administration, you must still configure each Avaya Aura® Media Server separately as a media server, and assign it to handle media services.

Licensing

Contact Center License Manager pushes license keys to all Avaya Aura® Media Server servers configured as Media Servers in Contact Center Manager Administration. When Avaya Aura® Contact Center uses WebLM licensing, Avaya Aura® Media Server does not require a license file or any specific licensing configuration. Each Avaya Aura® Media Server in the cluster requires one VALUE_CCTR_AMS_INSTANCE license.

Avaya Aura® Media Server Cluster Operating Systems

The servers in an Avaya Aura® Media Server cluster must all have the same operating system. All the servers in an Avaya Aura® Media Server cluster must use the Red Hat Enterprise Linux Release 6.x 64-bit operating system. Avaya Aura® Media Server is supported only when Red Hat Enterprise Linux is installed with English Language selected. Avaya Aura® Media Server does not support clusters with mixed operating systems. You cannot install other applications on the Avaya Aura® Media Server.

Avaya Aura® Media Server improved cluster redundancy

Each Avaya Aura® Media Server supports up to 1000 concurrent agents. When using an Avaya Aura® Media Server cluster, in Contact Center Manager Administration, you must configure each Avaya Aura® Media Server in the cluster separately as a media server, and assign it to handle media services. Avaya Aura Contact Center then distributes its media processing requirements across all configured Avaya Aura® Media Servers.

If your contact center requires 2400 concurrent agents, your solution requires three Avaya Aura® Media Servers: one primary Avaya Aura® Media Server, one secondary Avaya Aura® Media Server, and one standard Avaya Aura® Media Server. If one of these three Avaya Aura® Media Servers fails, potentially one third of calls might be lost. The remaining two Avaya Aura® Media Servers can support only 2000 concurrent agents.

For improved redundancy, you can install up to eight Avaya Aura® Media Servers, one primary Avaya Aura® Media Server, one secondary Avaya Aura® Media Server, and up to six standard Avaya Aura® Media Servers. If any of the eight Avaya Aura® Media Servers in the cluster fail, fewer (one eight) of the calls are lost, and the remaining seven Avaya Aura® Media Servers can continue to process the phone calls for all agents.

Avaya Aura® Media Server requires either primary or secondary server to play custom media

Either the Primary or Secondary server must remain in service for the cluster to remain operational. Cluster service is lost if the Primary and Secondary servers are out-of-service at the same time.

Avaya Aura® Media Server cluster configuration

Avaya Aura® Media Server supports custom (customer generated) media files and default (canned) media files.

In an Avaya Aura® Media Server cluster-based solution, you use Contact Center Manager Administration (CCMA) *Prompt Management* to configure your custom media files in the Content Store of the primary Avaya Aura® Media Server. The Content Store contents, including custom media files, are automatically replicated to all other Avaya Aura® Media Servers in the cluster.

In an Avaya Aura® Media Server cluster-based solution, you use Element Manager to modify the default “canned” media files of the primary Avaya Aura® Media Server. The Content Store contents, including the updated media files, are automatically replicated to all other Avaya Aura® Media Servers in the cluster.

Configure the following Avaya Aura® Media Server resources and settings only on the primary Avaya Aura® Media Server:

- Locale and Content Namespace
- Trusted Avaya Aura® Contact Center (CCMS) servers
- Custom media files (WAV) for announcements (stored in a Content namespace in the Content Store)

- Custom music media files (stored in a *streamsource* namespace in the Content Store)
- Default “canned” media files
- Streamed music source (Really Simple Syndication or SHOUTCast)
- Media Processing and Security

Configure the following Avaya Aura® Media Server resources and settings on every Avaya Aura® Media Server in the cluster:

- Cluster Configuration.

Avaya Aura® Media Server High Availability pair

The Avaya Aura® Media Server High Availability feature ensures uninterrupted availability of media processing and reduces loss of processing data when a switchover occurs. In a High Availability deployment, you configure a redundant pair of Avaya Aura® Media Server servers. The High Availability feature uses two Avaya Aura® Media Server operating in an active-standby configuration. Both the servers have identical configuration and provide full media processing capabilities. Administrators configure the High Availability feature by designating one Avaya Aura® Media Server as the primary server and the other as the backup server. Both servers communicate with each other using a heartbeat mechanism. Interruptions in the heartbeat between servers triggers a switchover, and the standby server becomes active. Because both the primary and backup servers are identical in functionality and configuration, the switchover is seamless.

Important:

Avaya Aura® Media Server supports High Availability only on a Linux operating system.

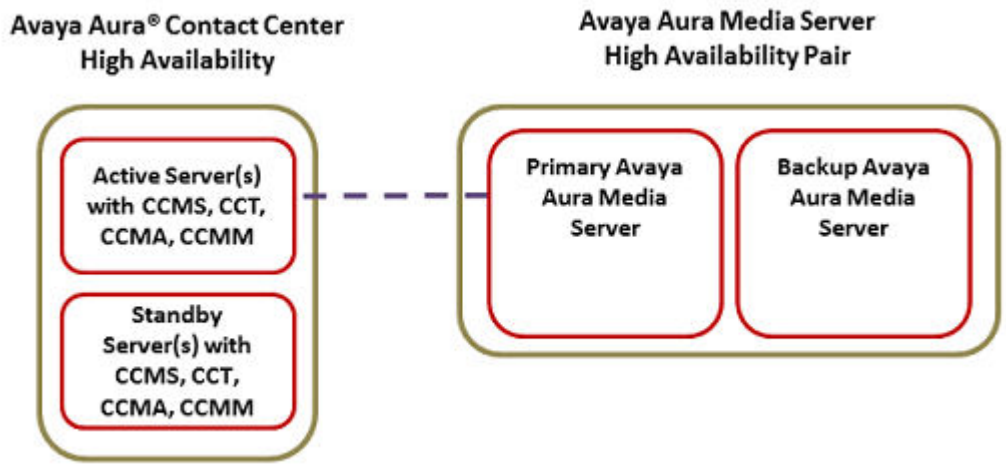


Figure 4: Avaya Aura® Media Server High Availability pair

In Contact Center Manager Administration (CCMA), you configure the Avaya Aura® Media Server High Availability pair as the media server, using the managed IP address of the HA pair, and assign it to handle conference media services.

Licensing

In Contact Center Manager Administration (CCMA), add the Avaya Aura® Media Server HA pair as a single Media Server and enter the Managed IP address of the pair as the IP address of that single Media Server. Avaya Aura® Contact Center then uses the HA pair as a single media processor. If one Avaya Aura® Media Server fails, the other Avaya Aura® Media Server takes over media processing.

When Avaya Aura® Contact Center uses WebLM licensing, Contact Center License Manager pushes license keys to all Avaya Aura® Media Servers configured as Media Servers in CCMA. Contact Center License Manager pushes license keys to both Avaya Aura® Media Servers of the High Availability pair. When Avaya Aura® Contact Center uses WebLM licensing, Avaya Aura® Media Server does not require a license file or any specific licensing configuration.

Each Avaya Aura® Media Server in the HA pair requires one VALUE_CCTR_AMS_INSTANCE license. An Avaya Aura® Media Server HA pair requires two VALUE_CCTR_AMS_INSTANCE licenses.

Avaya Aura® Media Server High Availability configuration

Avaya Aura® Media Server supports custom (customer generated) media files and default (canned) media files.

You update and configure the custom media files using Contact Center Manager Administration (CCMA) *Prompt Management*. In Avaya Aura® Media Server High Availability-based solutions, you configure your custom media files only on the primary Avaya Aura® Media Server. The custom media files are stored in the Content Store and they are automatically replicated to the backup Avaya Aura® Media Server.

In Avaya Aura® Media Server High Availability-based solutions, you use Element Manager to modify the default “canned” media files of the primary Avaya Aura® Media Server. The Content Store contents, including the updated media files, are automatically replicated to the backup Avaya Aura® Media Server.

Configure the following Avaya Aura® Media Server resources and settings only on the primary Avaya Aura® Media Server:

- Locale and Content Namespace
- Trusted Avaya Aura® Contact Center (CCMS) servers
- Custom media files (WAV) for announcements (stored in a Content Namespace in the Content Store)
- Custom music media files (stored in a *streamsource* namespace in the Content Store)
- Default “canned” media files
- Streamed music source (Really Simple Syndication or SHOUTCast)
- Media Processing and Security

Configure the following Avaya Aura® Media Server resources and settings on every Avaya Aura® Media Server in the cluster:

- High Availability configuration

Multiple Avaya Aura® Media Server High Availability pairs

For increased agent capacity in a High Availability deployment, you configure multiple redundant pairs of Avaya Aura® Media Server servers. The Avaya Aura® Media Server High Availability feature ensures uninterrupted availability of media processing and reduces loss of processing data when switchover occurs.

Important:

Avaya Aura® Media Server supports High Availability only on a Linux operating system.

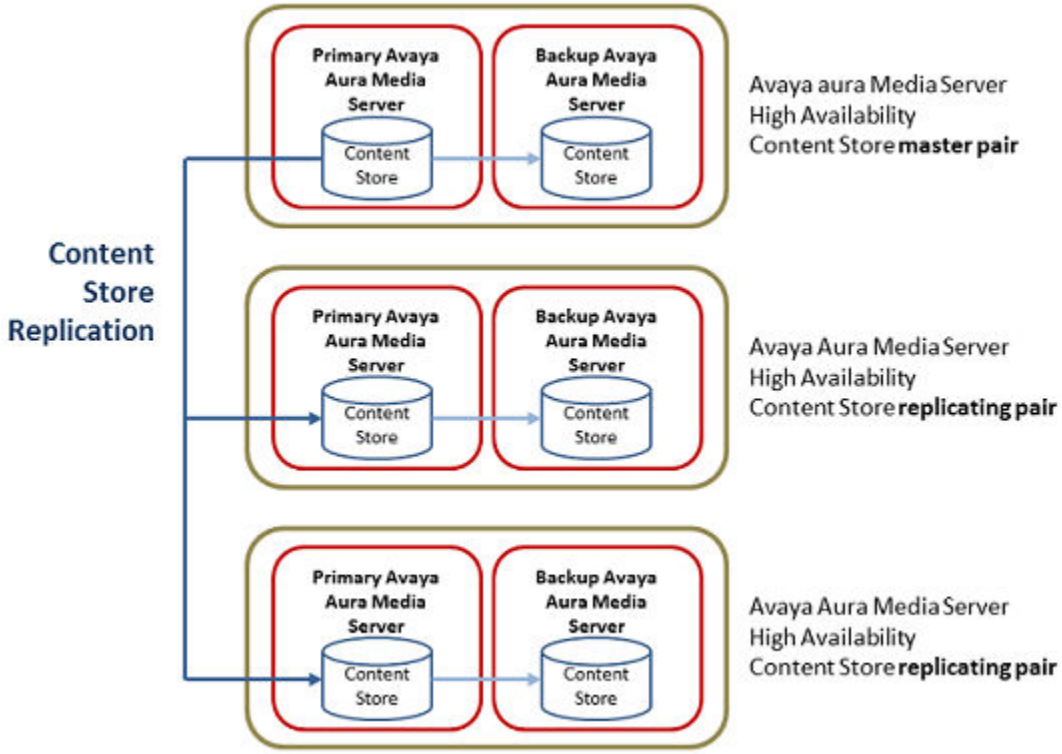


Figure 5: Content Store replication between multiple Avaya Aura® Media Servers with High Availability

In this configuration, you designate one Avaya Aura® Media Server HA pair as the "Master Pair" and the Primary server in the "Master Pair" is designated: "Master Cluster Primary AAMS". The IP address of this Master Cluster Primary AAMS is configured on all other Primary AAMS servers in all of the other HA pairs.

In Contact Center Manager Administration, you configure each Avaya Aura® Media Server HA pair as a media server, using the managed IP address, and assign it to handle conference media services.

Licensing

In Contact Center Manager Administration (CCMA), add each Avaya Aura® Media Server HA pair as a single Media Server and enter the Managed IP address of each pair as the IP address of that single Media Server. Avaya Aura® Contact Center then uses each HA pair as a single media processor. If one Avaya Aura® Media Server fails, the other Avaya Aura® Media Server in that pair takes over media processing.

When Avaya Aura® Contact Center uses WebLM licensing, Contact Center License Manager pushes license keys to all Avaya Aura® Media Servers configured as Media Servers in CCMA. Contact Center License Manager pushes license keys to both Avaya Aura® Media Servers of each High Availability pair. When Avaya Aura® Contact Center uses WebLM licensing, Avaya Aura® Media Server does not require a license file or any specific licensing configuration.

Each Avaya Aura® Media Server HA pair requires two VALUE_CCTR_AMS_INSTANCE licenses.

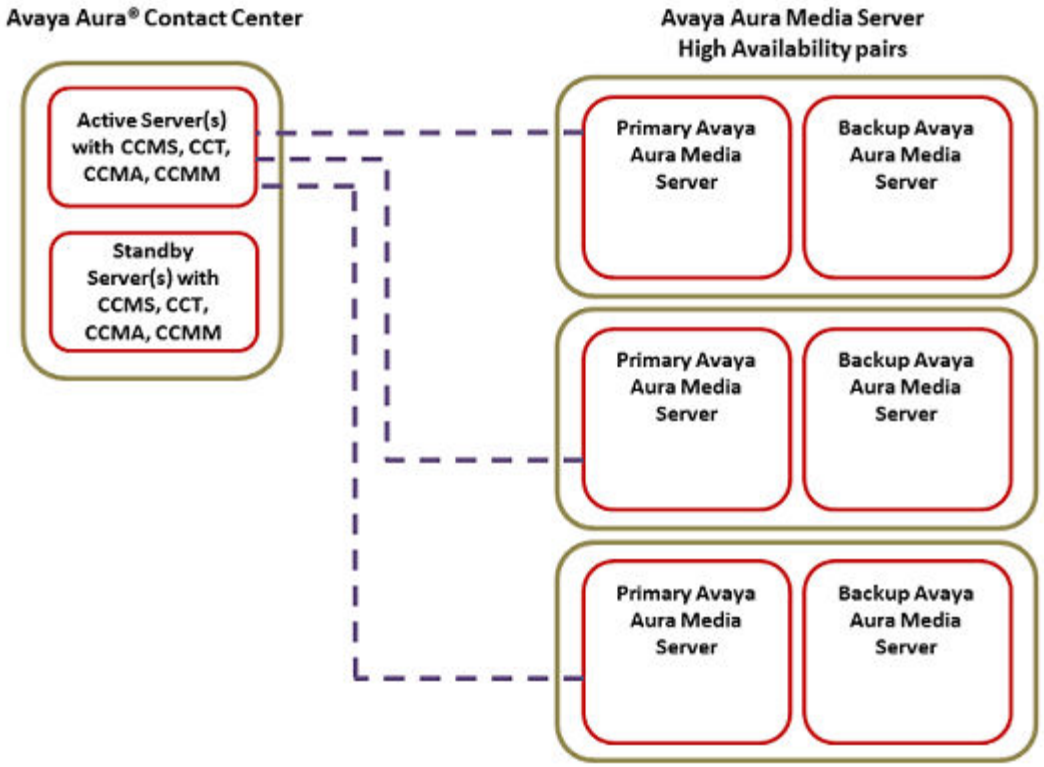


Figure 6: Avaya Aura® Media Servers with High Availability and WebLM licensing

Multiple High Availability pair configuration

Avaya Aura® Media Server supports custom (customer generated) media files and default (canned) media files. You update and configure the custom media files using Contact Center Manager Administration (CCMA) *Prompt Management*. Use Element Manager to modify the default “canned” media files of the primary Avaya Aura® Media Server.

Configure the following Avaya Aura® Media Server resources and settings on the primary server of the Avaya Aura® Media Server High Availability Content Store master pair:

- Locale and Content Namespace

- Custom media files (WAV) for announcements (stored in a Content Namespace in the Content Store)
- Custom music media files (stored in a *streamsource* namespace in the Content Store)
- Default “canned” media files

Configure the following Avaya Aura® Media Server resources and settings on each primary Avaya Aura® Media Server:

- Locale
- Streamed music source (Really Simple Syndication or SHOUTCast)
- Trusted Contact Center Manager Server (CCMS) servers
- Media Processing and Security

Configure the following Avaya Aura® Media Server resources and settings on every Avaya Aura® Media Server in the cluster:

- High Availability configuration.

Avaya Aura® Media Server Remote Geographic Node deployment

Where the contact center deploys High Availability with a Remote Geographic Node, implement a single Avaya Aura® Media Server server, an Avaya Aura® Media Server cluster, or an Avaya Aura® Media Server HA pair at the remote site.

A Remote Geographic Node site supports the following Avaya Aura® Media Server deployments:

- A single primary Avaya Aura® Media Server. The single primary Avaya Aura® Media Server replicates data from the primary Avaya Aura® Media Server at the campus site.
- An Avaya Aura® Media Server cluster. The primary Avaya Aura® Media Server of the cluster replicates data from the primary Avaya Aura® Media Server at the campus site. The other Avaya Aura® Media Servers in the remote cluster replicate data from the primary Avaya Aura® Media Server of the remote cluster.
- An Avaya Aura® Media Server High Availability pair. The primary Avaya Aura® Media Server of the HA pair replicates data from the primary Avaya Aura® Media Server at the campus site. The backup Avaya Aura® Media Server at the remote site replicates data from the primary Avaya Aura® Media Server at the remote cluster.

Configure one remote Avaya Aura® Media Server primary server to replicate from the primary Avaya Aura® Media Server at the campus site. Then configure all other Avaya Aura® Media Servers at the remote site to replicate from the primary Avaya Aura® Media Server at the remote site.

The Avaya Aura® Media Server servers at the remote site obtain licenses from the Avaya Aura® Contact Center servers at that remote site.

In Remote Geographic Node deployments, configure Content Store replication between the primary server of the remote site and the primary server on the campus site. This allows Content Store configuration on only a single primary server on the campus, and the Content Store configuration

automatically replicates to the primary server at the remote side, and from that server to the other Avaya Aura® Media Server servers in the remote site cluster.

Avaya Aura® Contact Center supports the deployment of Avaya Aura® Media Server High Availability pairs at a Remote Geographic Node site. You can also deploy Avaya Aura® Media Server High Availability pairs at multiple remote sites in your solution.

Prompt Management in a geographic redundancy environment

If a failover occurs to the Remote Geographic Node (RGN) site, you must update the Master Content Store setting to point to your local Master Content Store node at the RGN site. When you update this setting, you can use Contact Center Manager Administration for prompt management at the RGN site.

Avaya Aura® Media Server Zoning

Avaya Aura® Media Server (Avaya Aura® MS) Zoning allows contact center administrators to target a specific Avaya Aura® MS instance or prioritized list of instances when anchoring incoming contact center calls. The administrator chooses the preferred Avaya Aura® MS instance on which to anchor the contact center call using a new scripting command in Avaya Aura® Orchestration Designer (OD). The preferred Avaya Aura® MS instance can be selected based on a number of parameters (for example CDN, CLID). These parameters are chosen by the administrator in OD. If no Avaya Aura® MS instance is explicitly selected in the OD script, Avaya Aura® Contact Center (AACC) falls back to its current round-robin selection of an Avaya Aura® MS instance from the available pool. If no Avaya Aura® MS instances in the supplied list are reachable, AACC falls back to its round-robin algorithm to anchor on any other available Avaya Aura® MS.

The existing AACC call handling model, prior to Avaya Aura® MS Zoning, saw incoming customer calls anchored on an available Avaya Aura® MS instance immediately upon arrival into Contact Center. AACC then gives control of these calls to the scripting engine. The mechanism used to select the Avaya Aura® MS instance is a round-robin algorithm, which means you cannot reliably predict the specific Avaya Aura® MS instance to be used for any given call. In this case, Avaya Aura® MS instances must be co-located in a single data center to avoid random distribution of voice media traffic across a customer's Wide Area Network (WAN).

By controlling the Avaya Aura® MS selection process, administrators can optimize WAN bandwidth utilization by distributing Avaya Aura® MS instances to be in close proximity to call ingress points across the contact center network. Calls are then anchored locally at those points. This ensures all voice media traffic to and from the customer is retained within a single location.

Note:

Avaya Aura® Contact Center supports a maximum of six sites in any Avaya Aura® MS Zoning solution. Each zone can include up to five Avaya Aura® MS servers at each site.

The following diagrams show the differences between solutions with and without Avaya Aura® MS Zoning.

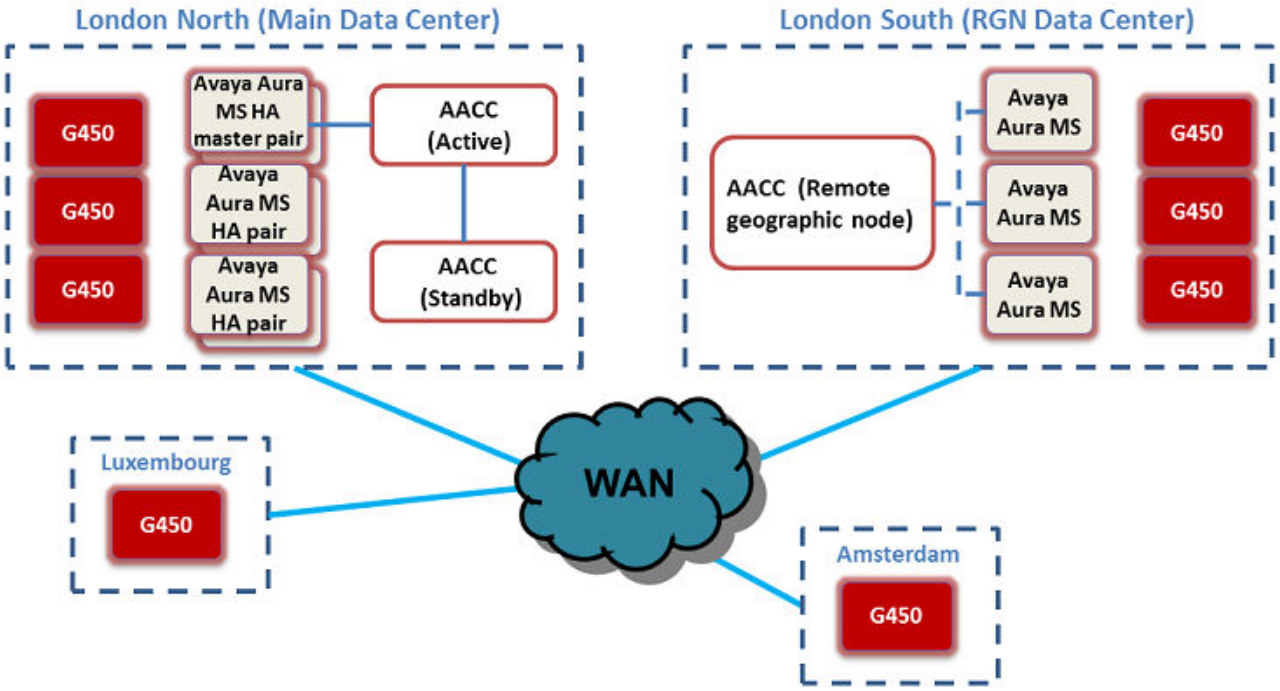


Figure 7: AACC solution without Avaya Aura® MS Zoning

The diagram above describes a Mission Critical HA solution with a Remote Geographic Node site. In this example call ingress points are distributed across four locations (London North, London South, Luxembourg, Amsterdam), but the active Avaya Aura® MS instances must be co-located with their AACC servers. This means that all voice traffic is backhauled to the currently active data center (London North). The Avaya Aura® MS instances at the RGN site are single Avaya Aura® MS servers – Avaya Aura® MS High Availability pairs at RGN sites were previously not supported in Avaya Aura® Contact Center solutions.

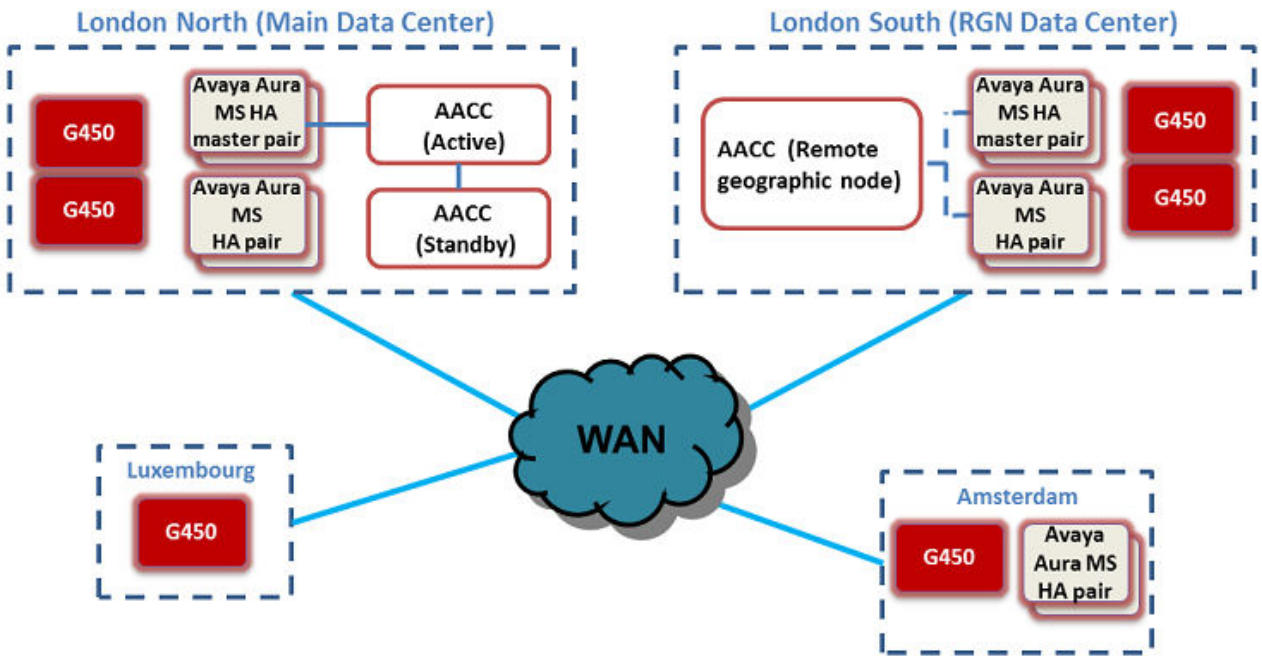


Figure 8: AACC solution with Avaya Aura® MS Zoning

The diagram above also describes a Mission Critical HA solution with a Remote Geographic Node site. In this example, an Avaya Aura® MS High Availability pair is co-located with a call ingress point at the Amsterdam location. The Luxembourg site still contains no Avaya Aura® MS instances. This example might be relevant where a low level of call traffic is arriving at the Luxembourg location and is considered to be close enough (from a WAN traversal perspective) to another location where Avaya Aura® MS instances are deployed. In this example, calls arriving from Luxembourg can be anchored on the Avaya Aura® MS in Amsterdam by default, with a suitably provisioned WAN link between those two sites to handle the customer call leg media traffic.

This example includes Avaya Aura® MS High Availability pairs located at the RGN site with G450 Media Gateways. With Avaya Aura® MS Zoning, it is now possible for the Main Data Center to use the Avaya Aura® MS servers and gateways located at the RGN site. It is also possible for the non-HA AACC server to use Avaya Aura® MS High Availability pairs at the RGN site.

You enable the Avaya Aura® MS Zoning feature on the CCMA Global Settings page. You must have a license that supports Avaya Aura® MS Zoning — you cannot enable Avaya Aura® MS Zoning without a license. The feature is disabled by default. Once the feature is enabled, you must configure your OD flow applications to perform the required Avaya Aura® MS selection logic. If no selection logic is configured in OD, the existing round-robin algorithm is applied for incoming calls.

Agent selection considerations

Administrators can optimize WAN bandwidth utilization by distributing Avaya Aura® MS instances to be in close proximity to call ingress points across the contact center network; however the location of the agent on the customer call also impacts the WAN bandwidth usage. This is because there is an agent call leg established between the Avaya Aura® MS instance and the agent for each customer call. An agent in close proximity to the Avaya Aura® MS instance improves bandwidth usage.

There are options available to the administrator to ensure that each agent on a customer call is located near to the Avaya Aura® MS instance that the call is anchored on. Avaya recommends that administrators define location-specific skillsets. If the solution uses location-specific skillsets, the QUEUE TO SKILLSET script command can identify the preferred location of an agent to choose for each customer call. Assigning these skillsets with a high priority to agents in the applicable locations, and with lower priority to agents in other locations, ensures that Contact Center chooses agents in closer proximity to the AMS instance in preference to other agents with the same basic skillset. Consider the following example:

- The Contact Center solution includes call ingress points in Dublin and London.
- There are Contact Center agents located in both Dublin and London.
- For calls related to sales, create skillsets named Sales_Dublin and Sales_London.
- Assign the Sales_Dublin skillset to sales agents located in Dublin with a high priority and, optionally, assign these agents to the Sales_London skillset with a lower priority.
- Assign the Sales_London skillset to sales agents located in London with a high priority and, optionally, assign these agents to the Sales_Dublin skillset with a lower priority.

There are periods in the course of a customer call that the agent-end media originates from, or is terminated at, a Communication Manager gateway rather than the agent phoneset. Avaya Aura® Contact Center does not support the selection of gateways to use for agent call legs. This is an engineering consideration that must be taken into account by administrators of any solution using Avaya Aura® MS Zoning.

For more information on how to configure Avaya Aura® MS Zoning, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.

WAN requirements

The following is a list of Wide Area Network (WAN) requirements for Avaya Aura® MS Zoning:

- Network jitter must be under 20 milliseconds (ms). Avaya recommends that this figure is less than 10 ms.
- Avaya recommends that packet loss is 1% or less.
- For low loss, jitter, and latency traffic characteristics, by default Avaya Aura® MS marks voice packets with Differentiated Services Code Point (DSCP) - Expedited Forwarding (EF). These characteristics are suitable for real-time voice services and help to prioritize the audio traffic. You can configure the value to suit your network and solution.
- Bandwidth requirements depend on how many channels are running across each WAN segment, and on the codec used:
  - G.711 (using 20 ms packetization intervals) requires 80 kbps per stream including IP/UDP/RTP. Adding Layer 2 over Multilink Point-to-Point Protocol (MLP) gives a total of 86kbps per stream.
  - G.729A (using 20-ms packetization intervals) requires 24 kbps per stream including IP/UDP/RTP. Adding Layer 2 over MLP gives a total of 30kbps per stream.
- Consider the following for ITU G.115:
  - One-way delay is acceptable up to 150 ms (this is mouth to ear, including network, audio codec, and framing for example). 150 ms – 250 ms is acceptable in certain environments.

- Minimize network delay to avoid impacting quality. Distance impacts this number and is unavoidable. Avaya recommends that network delay is 80 ms (one-way) or less.

Chapter 12: High Availability fundamentals

This chapter describes High Availability concepts and features that are common to all High Availability solutions.

Avaya Aura® Contact Center supports High Availability for fault tolerant and mission critical contact centers. Contact Center supports the following levels of campus high availability:

- Mission Critical High Availability for SIP-enabled Contact Centers
- Hot-standby High Availability for AML-based Contact Centers

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. Contact Center also supports geographic data resiliency and disaster recovery.

Campus High Availability

Campus High Availability caters for Contact Center application or server failures, and offers resiliency for local network failures. In a campus High Availability environment the standby and active servers are in the same physical location. The active and standby servers have different static IP addresses, but share a common virtual Managed IP address.

Managed IP address

Contact Center supports the active/standby High Availability model. The active server processes contacts. The standby server takes over if the active server fails or is shut down for maintenance.

A Managed IP address is a virtual IP address that is attached to a Network Interface Controller (NIC) on the active server.

Each High Availability application server has a static IP address. The active server attaches the Managed IP address to its network interface. The Managed IP address is assigned only to the active server. All other contact center applications and clients connect to the active server and applications using the Managed IP address. If the standby server takes over processing and becomes active, it attaches the Managed IP address to its network interface. When an active server stops being the active server, it stops hosting the Managed IP address.

If your High Availability-enabled active Contact Center server has two network interfaces and is configured to support an embedded LAN (ELAN), then the Contact Center server supports two Managed IP addresses; one Managed IP address for the CLAN and one Managed IP address for the ELAN. Contact Center supports an embedded LAN only in CS1000 AML-based solutions.

The Managed IP address of the High Availability pair, the IP address of the active server, and the IP address of the standby server must all be in the same network subnet IP address range. For example, with a subnet mask of 255.255.255.0, if the active server IP address is 172.1.1.X and the standby server IP address is 172.1.1.Y, then the Managed IP address for the HA pair must be 172.1.1.Z.

Managed name

Administrators can configure a Managed name that maps to the Managed IP address. The configuration of this Managed name can be on a Domain Name System (DNS) or in the hosts files on the servers that connect to the High Availability servers.

Applications and servers connecting to a High Availability-enabled Contact Center must use the Managed IP address or Managed name, not the physical names or IP addresses of the active and standby servers. For example, Agent Desktop must use the Managed IP address or Managed name to connect to Contact Center in a High Availability solution.

Campus switchover

In a campus environment, a switchover from the active server to the standby server appears as a server restart to external applications that are using the Managed IP address.

You can manually initiate a switchover or you can configure Contact Center to trigger a switchover automatically when the servers lose communication or if a service or hardware fails on the active server. For a switchover to occur, the standby server must be shadowing the active server and switchover must be enabled on both servers.

The main advantages of campus High Availability are:

- Automatic switchover
- Short switchover time
- Minimal switchover steps
- Third-party applications using the Managed IP address or Managed name experience continued service

Email notification of switchover

You can configure Contact Center to send email notifications automatically when a switchover occurs, to alert the Contact Center administrator. The email notifications provide switchover information to a configured recipient email address. This switchover information includes:

- A description of the switchover type; whether the switchover is manual, is automatic due to a critical service failure, or is automatic due to network communication failure.
- For automatic switchovers, additional information on the critical service or network failures. This information can include event IDs and the switchover time.

In the case of automatic switchovers due to service or network failures, Contact Center sends two emails. The first email informs the administrator that a switchover is imminent, and the second email confirms the successful completion of the switchover.

Contact Center application geographic redundancy

The Avaya Aura® Contact Center High Availability feature supports geographic redundancy for data resiliency and disaster recovery. In geographic Wide Area Network (WAN) solutions, the standby server on the remote geographic site is called a Remote Geographic Node (RGN) server. Contact Center geographic High Availability supports data resiliency and disaster recovery.

The Remote Geographic Node (RGN) server on the remote site shadows the server on the campus site, maintaining a near real-time local copy of the active server databases. Therefore, the RGN server is configured with the most recent data and it can take over if the campus site fails. Where the campus site has High Availability, the RGN server shadows the active server on the campus site, using the Managed IP address. This means that following a Contact Center switchover on the campus site, the RGN continues to shadow data from the same IP address.

The RGN server must have the same Contact Center applications installed as the active server. For example, if the active server is a Voice and Multimedia Contact Server, then the RGN server must be a Voice and Multimedia Contact Server. If the campus site has a Voice Contact server and a Multimedia Contact server, the remote site must have a Voice Contact server and a Multimedia Contact server.

You must use a backup Domain Controller in geographic Wide Area Network (WAN) Contact Center solutions. The Remote Geographic Node (RGN) servers must be able to communicate with the backup Domain Controller after a failure at the campus site. The Remote Geographic Node servers use the backup Domain Controller to authenticate users if the administrator brings the RGN server online.

Database shadowing

The following Avaya Aura® Contact Center components store information in a Caché database:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)

This Caché database technology supports database shadowing for fault tolerant and mission critical solutions such as Avaya Aura® Contact Center. To use Caché database shadowing, you must have two of each resilient application, an active application server and a corresponding standby application server.

The standby server constantly retrieves logical records of database updates from the active server, so that the standby server always has a near real-time copy of the active database. This process is called database shadowing: the standby server is shadowing the active server database.

Therefore, the standby server has the most recent configuration and data, and it can take over from the active server if necessary.

Trusted IP address

The active and standby servers use a Trusted IP address to verify network connectivity. If one HA server cannot communicate with the other HA server, it checks the connection to the Trusted IP address. Each HA server uses this mechanism to validate whether it has lost the connection to the network or lost the connection to the other server.

If the active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the active server stops processing contacts and shuts down. The standby server starts processing contacts if it cannot communicate with the active server but can communicate with the Trusted IP address.

If an active server cannot connect to the Trusted IP address on startup, then no Contact Center services start on that server.

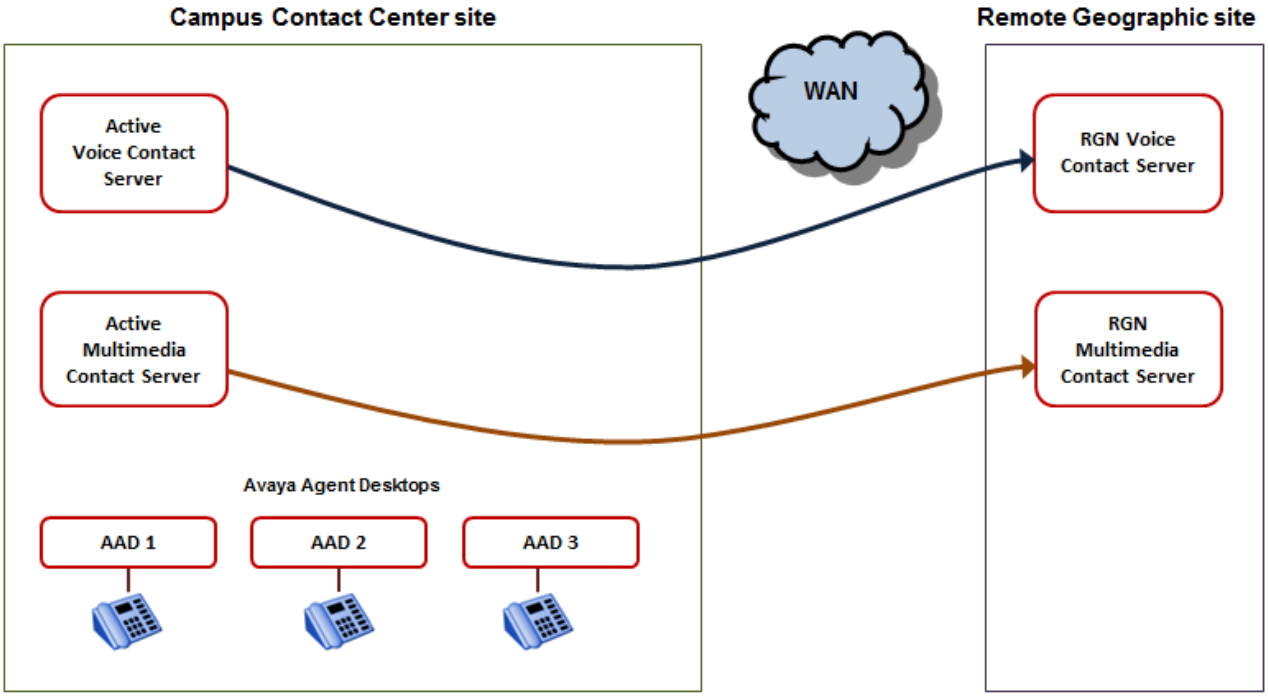
You must use the IP address of some reliable part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

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 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)

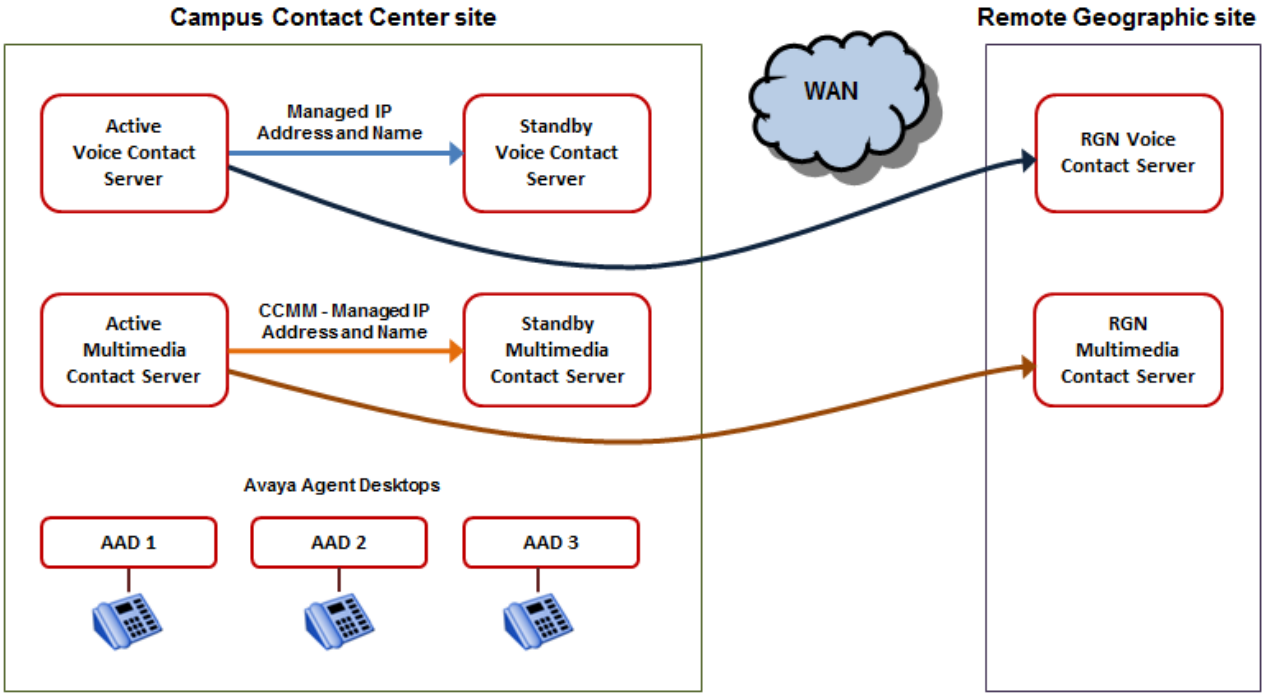
Multimedia Contact Server includes Contact Center Multimedia (CCMM)

AAD Avaya Agent Desktop

RGN Remote Geographic Node

Figure 9: 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 10: 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.

- Avaya Communication Server 1000 AML-based solution, with campus active and standby Contact Center servers, and Contact Center Remote Geographic Node server(s) for data resiliency and disaster recovery.
- Avaya Communication Server 1000 AML-based solution, with a campus active Contact Center server(s), and Contact Center Remote Geographic Node server(s) for data resiliency and disaster recovery.

Contact Center Application High Availability

In a campus solution, each application (CCMS, CCMA, CCT, and CCMM) on the active server processes contacts. Each application (CCMS, CCMA, CCT, and CCMM) on the standby server monitors and shadows the corresponding active application.

Most failures of any active application cause a server switchover from the active server to the standby server.

- CCMS: CCMS service, database, network, or hardware failure
- CCT: CCT service, database, network, or hardware failure
- CCMM: database, network, or hardware failure.

  Generally, if a critical CCMM service fails, Windows Service Monitor automatically restarts the service. However, for High Availability solutions that use Enterprise Web Chat (EWC), a failure of the CCMMWebChatService on the active server causes a switchover.

In a Remote Geographic HA solution, each application (CCMS, CCMA, CCT, and CCMM) on the RGN server monitors and shadows the corresponding active application on the active campus server. However, a failure of one of the applications on the active site does not cause a switchover to the RGN server.

Avaya Aura® Media Server

The Avaya Aura® Media Server High Availability feature ensures uninterrupted availability of media processing and reduces loss of processing data when an Avaya Aura® Media Server fails. The High Availability feature uses two Media Servers. Both the servers have identical configuration and provide full media processing capabilities.

Administrators configure the High Availability feature by designating one server as the primary server and the other as the backup server. Either of these servers can be the active server, with the other being the standby. Both servers communicate with each other using a heartbeat mechanism.

Interruptions in the heartbeat from the active server trigger a switchover to the standby server. The standby server becomes the active server. Because both the active and standby servers are identical in functionality and configuration, the switchover is seamless.

After a switchover, if both servers are still running, the Avaya Aura® Media Server HA pair continues to provide full redundancy and call protection. For example, if a temporary network fault causes a switchover, the HA pair is functional after the network recovers. You do not need to manually intervene to reinstate the HA pair. If both servers are running and can communicate a heartbeat after a switchover, the HA pair continues to support switchovers. However, if a fault on the active server causes a switchover, and the failed server is no longer running, Avaya Aura® Media Server does not provide redundancy or call protection. You must fix the failed server and manually reinstate HA.

Limitations:

- You can configure High Availability only in a 1+1 configuration.
- Avaya Aura® Media Server supports High Availability only on a Linux operating system.

Avaya Aura® Media Server High Availability pair

In a High Availability deployment, configure a redundant pair of Avaya Aura® Media Server servers. Configure a High Availability primary Avaya Aura® Media Server and a High Availability backup Avaya Aura® Media Server on two separate servers. In Contact Center Manager Administration, you configure the Avaya Aura® Media Server High Availability pair as the media server, using the managed IP address of the cluster, and assign it to handle conference media services.

When you configure an Avaya Aura® Media Server as a Media Server in Contact Center Manager Administration, Contact Center License Manager pushes licenses to that Avaya Aura® Media Server. You must restart Contact Center License Manager to push the licenses to Avaya Aura® Media Server.

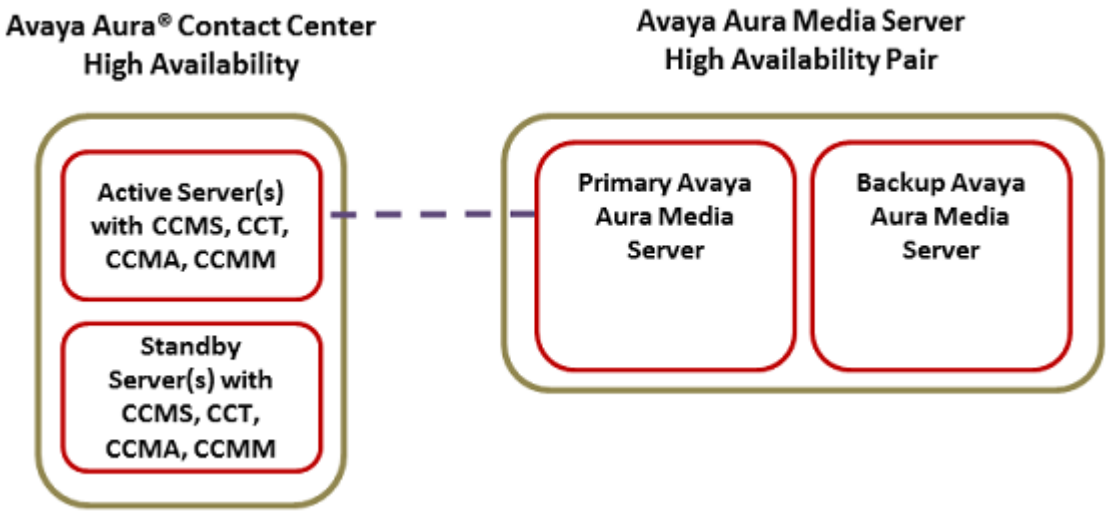


Figure 11: Single Avaya Aura® Media Server with High Availability

Avaya Aura® Media Server server High Availability pairs

For increased agent capacity in a High Availability deployment, you configure multiple redundant pairs of Avaya Aura® Media Server servers. The Avaya Aura® Media Server High Availability feature ensures uninterrupted availability of media processing and reduces loss of processing data when switchover occurs.

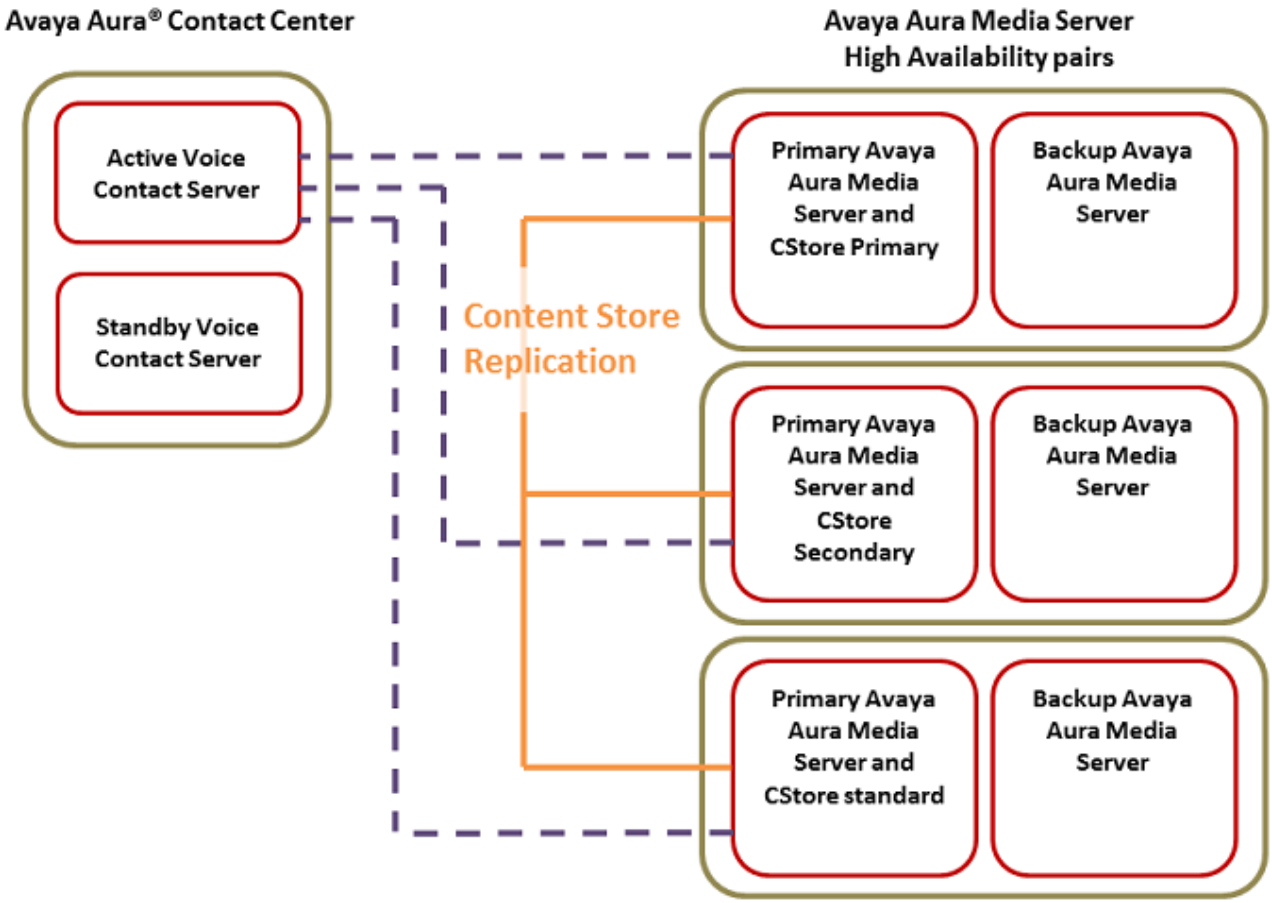


Figure 12: Multiple Avaya Aura® Media Servers with High Availability

In this deployment, you configure Content Store (CStore) replication across the Avaya Aura® Media Server Primary servers. This allows you to perform configuration on a single primary server only, and the configuration automatically replicates to the other Avaya Aura® Media Server servers in the network configuration.

In Contact Center Manager Administration, you configure each Avaya Aura® Media Server redundant pair as a separate media server, using the managed IP address, and assign it to handle conference media services. Contact Center License Manager pushes licenses to the Avaya Aura® Media Servers. You must restart Contact Center License Manager to push the licenses to the Avaya Aura® Media Servers.

Avaya Aura® Media Server Remote Geographic Node deployment

Where the contact center deploys High Availability with a Remote Geographic Node, implement an Avaya Aura® Media Server cluster or HA pair at the remote site. The Avaya Aura® Media Server servers at the remote site obtain licenses from the Avaya Aura® Contact Center servers at that remote site.

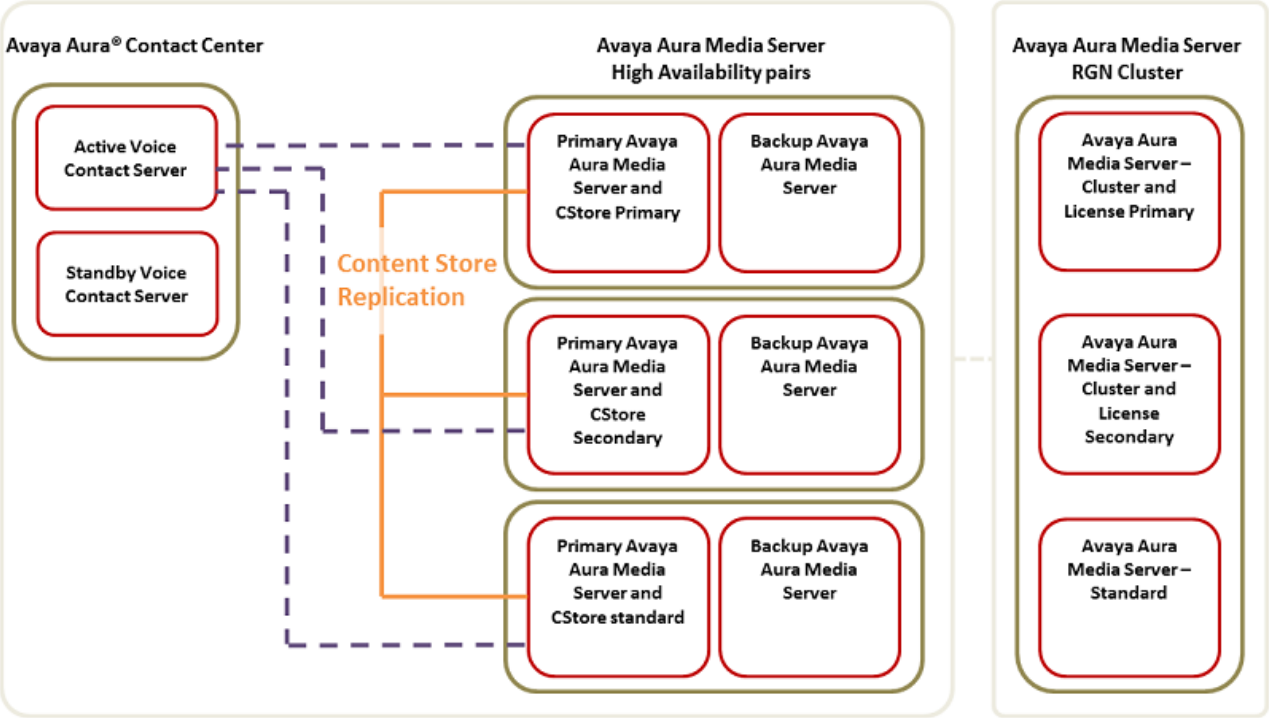


Figure 13: Multiple Avaya Aura® Media Servers in a Remote Geographic node configuration

In this deployment, you configure Content Store (CStore) replication between the primary server of the remote cluster and the primary configuration server on the campus. This allows configuration on only a single primary server on the campus, and the configuration automatically replicates to the primary at the remote side, and from that server to the other Avaya Aura® Media Server servers in the remote site cluster.

Note:

Avaya Aura® Contact Center supports the deployment of Avaya Aura® Media Server High Availability pairs at a Remote Geographic Node site. You can also deploy Avaya Aura® Media Server High Availability pairs at multiple remote sites in your solution.

Standby server hardware requirements

The standby server must match the active server. The standby server must have the exact same hard disk partitions, the same amount of memory and the same CPU type. The standby server must have the Contact Center software installed on the same partitions as the active server. The active and standby servers must have the same patch level and the same operating system updates.

Note:

In a SIP-enabled Contact Center using an Avaya Aura® Unified Communications platform and High Availability resiliency, the active and standby CCMS servers must both have TLS certificates in

place to communicate securely with the Application Enablement Services server and to support High Availability switchover.

Campus network configuration

Contact Center uses a managed IP address for campus High Availability. A managed IP address is a virtual IP address hosted on the NIC of the currently active server. Both the active and standby servers also have a static IP address. You configure the static IP address of each server in the Windows operating system. You configure the Managed IP address in the Contact Center High Availability configuration interface.

To eliminate network points of failure in the Contact Center solution, you must use Link Aggregation Control Protocol (LACP), NIC Teaming, and Virtual Router Redundancy Protocol (VRRP).

Dynamic Host Configuration Protocol (DHCP):

Contact Center server applications do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Link Aggregation Control Protocol:

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

NIC teaming:

NIC teaming is the process of grouping together several physical NICs into one single logical NIC, which can be used for network fault tolerance and transmit load balancing. By teaming more than one physical NIC to a logical NIC, high availability is maximized. Even if one NIC fails, the network connection does not cease and continues to operate on other NICs.

Virtual Router Redundancy Protocol (VRRP):

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. Two or more physical routers, such as Avaya ERS 5520, can be configured to stand for a virtual router. If one physical router fails, another physical router automatically replaces it.

Campus High Availability supports LAN environments where the round trip delay is less than 80ms, with less than 0.5% packet loss.

Remote Geographic Node server requirements

The Remote Geographic Node server must match the campus server. The Remote Geographic Node server must have the same Contact Center application, the exact same hard disk partitions,

the same amount of memory, the same CPU type, and the exact same Operating System patches. The Remote Geographic Node server must have the Contact Center software installed on the same partitions as the campus server, and it must be patched to the same level. The campus and Remote Geographic Node servers must have the same patch level and the same operating system updates.

Geographic network configuration

If you have Contact Center HA at the campus, configure the Remote Geographic Node to communicate with the Managed IP address at the campus site.

To eliminate network points of failure in the contact center solution, you must use Link Aggregation Control Protocol (LACP), NIC Teaming and Virtual Router Redundancy Protocol (VRRP).

Dynamic Host Configuration Protocol (DHCP):

Contact Center server applications do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Link Aggregation Control Protocol:

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

NIC teaming:

NIC teaming is the process of grouping together several physical NICs into one single logical NIC, which can be used for network fault tolerance and transmit load balancing. By teaming more than one physical NIC to a logical NIC, high availability is maximized. Even if one NIC fails, the network connection does not cease and continues to operate on other NICs.

Virtual Router Redundancy Protocol (VRRP):

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. Two or more physical routers, such as Avaya ERS 5520, can be configured to stand for a virtual router. If one physical router fails, another physical router automatically replaces it.

Geographic High Availability supports WAN environments where the round trip delay is less than 80ms, with less than 0.5% packet loss.

Simple Network Management Protocol

You can configure Contact Center applications to alert any Avaya or third-party applications that connect to the server whether the primary server is active, is performing a switchover, or is inactive.

These alerts include Windows events, Simple Network Management Protocol (SNMP) alarms, and email messages.

Licensing

High Availability (HA) is a licensed feature. Contact Center enables HA when you purchase a standby server license.

High Availability with license files

For campus HA, the license file is based on two MAC addresses, the MAC address of the active server and the MAC address of the standby server. The license file, containing the active and standby MAC addresses, is installed on both servers. If a switchover occurs, the standby server processes calls. The standby server has a HA license, and does not use the grace period mechanism.

For geographic HA, the license file is based on two MAC addresses, the MAC address of the active server and the MAC address of the Remote Geographic Node server. The license file, containing the active and Remote Geographic Node server MAC addresses, is installed on the active server and on the Remote Geographic Node server.

If Contact Center has HA at the campus, when a campus switchover occurs, the standby campus server takes over call processing. The standby server uses the licensing grace period mechanism. This gives the Contact Center Administrator 30 days grace to figure out why the switchover occurred and to reinstate the active server.

High Availability with Avaya WebLM server

In a HA deployment you can use two Virtualized Environment (VE) Avaya WebLM servers, or two local WebLM instances. For campus HA, both Avaya WebLM servers can be in the campus. For geographic HA, one Avaya WebLM server must be in the campus and one must be at the remote site.

For campus HA, the license file is based on the Host IDs of both Avaya WebLM servers. Install the license file, containing both Host IDs, on both Avaya WebLM servers. The active server references one Avaya WebLM server, and the standby server references the other Avaya WebLM server. If a switchover occurs, the standby server processes calls. The standby server gets a HA license from the Avaya WebLM server for which it is configured, and does not use the grace period mechanism.

For geographic HA, the license file is based on the Host IDs of both Avaya WebLM servers. Install the license file, containing both Host IDs, on both Avaya WebLM servers. The active server references one Avaya WebLM server, and the Remote Geographic Node server references the other Avaya WebLM server. In a failover to the remote site, the Remote Geographic Node server gets a HA license from the Avaya WebLM server for which it is configured.

In a geographic HA deployment, if Contact Center has HA at the campus, when a campus switchover occurs, the standby campus server takes over call processing. The standby server uses the licensing grace period mechanism. This gives the Contact Center Administrator 30 days to investigate why the switchover occurred and to reinstate the active server.

Hot patching

Microsoft Windows Server 2012 R2 does not support the patching of running applications. You must stop a Windows Server 2012 R2 application to patch it. Avaya Aura® Contact Center is supported on the Microsoft Windows Server 2012 R2 operating system. The Contact Center High Availability feature supports Hot Patching. In a Contact Center using the High Availability feature, two sets of Contact Center applications run, but only the active set processes contacts. The standby applications do not process contacts and can therefore be stopped and patched without shutting down the Contact Center.

A small number of Contact Center patches or service packs might not support Hot Patching, and these updates can require a maintenance window. Read the patch or service pack Readme file to determine if it supports Hot Patching.

If your Contact Center is licensed for active and standby servers, you can patch software to minimize down time during the patching process. You must ensure that you patch both the active and standby servers to the same level of patch.

For more information about Hot Patching the active and standby servers, see *Upgrading and patching Avaya Aura® Contact Center*.

More information

- For information on Mission Critical High Availability see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Solution Description*.
- For information on Hot-standby High Availability, see *Avaya Aura® Contact Center and Avaya Communication Server 1000 Solution Description*.

Chapter 13: 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 Communication Server 1000 AML-based solution, Avaya Aura® Contact Center supports Landing Pads for integration with Avaya Aura® Experience Portal. AML-based solutions do not support SIP header Information or Contact Intrinsics as call attached data.

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

The following table shows the call transfer mechanism supported by each platform type:

Transfer method	CS 1000 AML-based Contact Center	Avaya Aura SIP-enabled Contact Center
Landing Pads	Yes	Yes
UUI SIP header	No	Yes
P-Intrinsic SIP header	No	Yes
SIP INFO message using Context Creation	No	Yes

The following table shows the additional licensing requirements for each Avaya Aura® Contact Center and Avaya Aura® Experience Portal integration type:

Solution type	CS 1000 AML-based Contact Center	Avaya Aura SIP-enabled Contact Center
Landing Pads	OI Open Queue and OI Universal Networking.	OI Open Queue and OI Universal Networking.
Front-end Avaya Aura® Experience Portal	N/A	No additional licenses required.
Back-end Avaya Aura® Experience Portal	N/A	No additional licenses required.
SIP INFO message using Context Creation	N/A	No additional licenses required.

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. • 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.

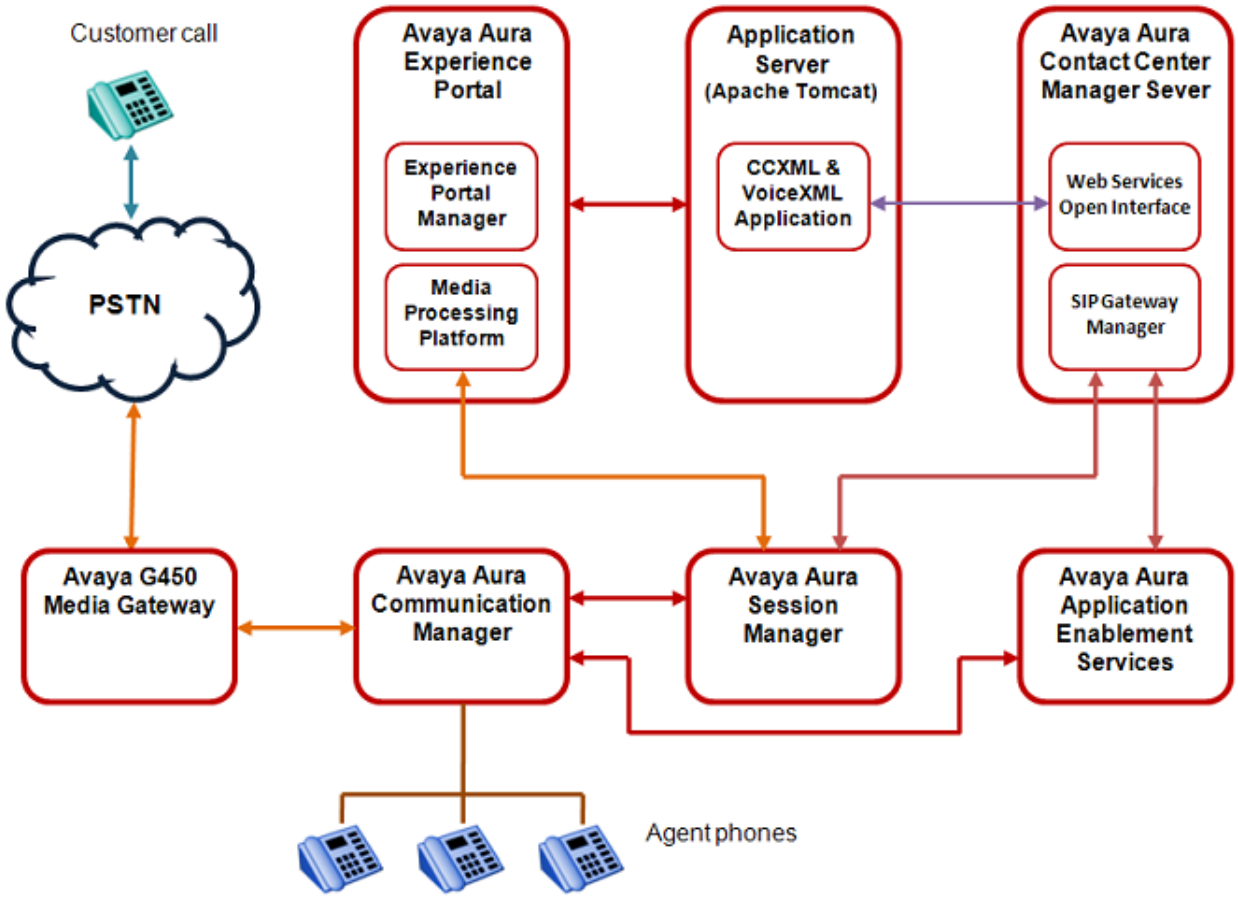


Figure 14: Example of front-end Avaya Aura® Experience Portal using Contact Center Web Service Open Interfaces

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.

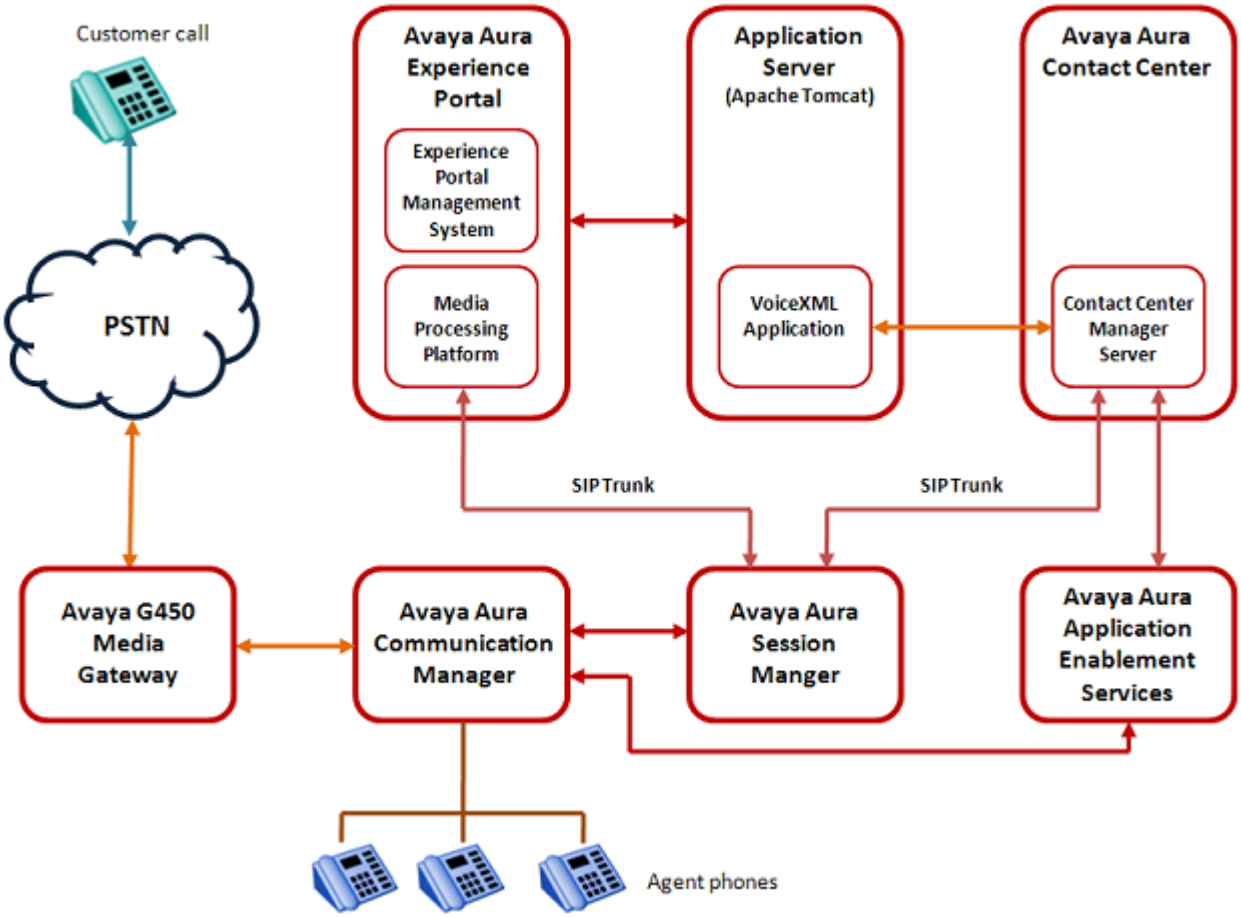


Figure 15: Example of front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

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.

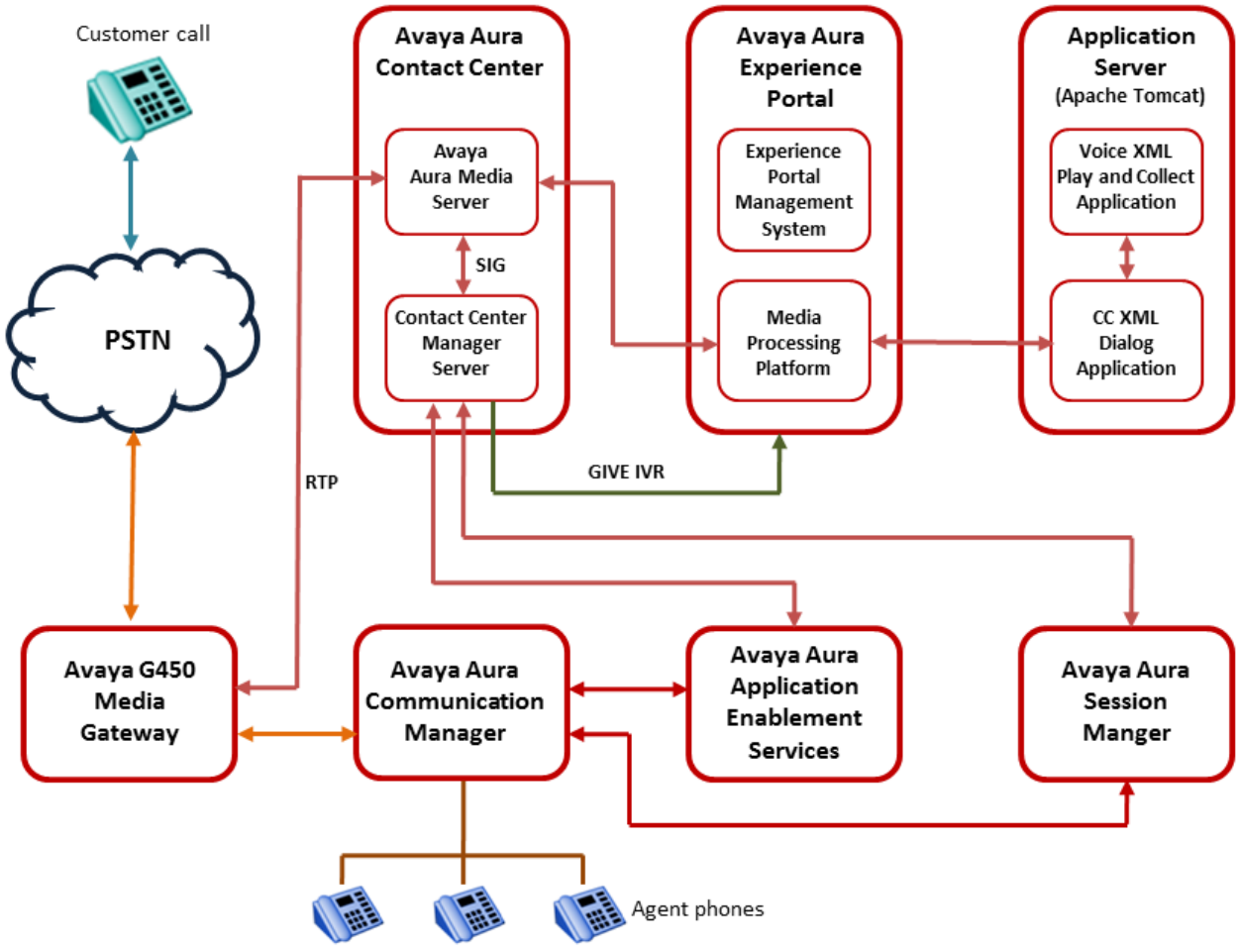


Figure 16: Example of back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

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.

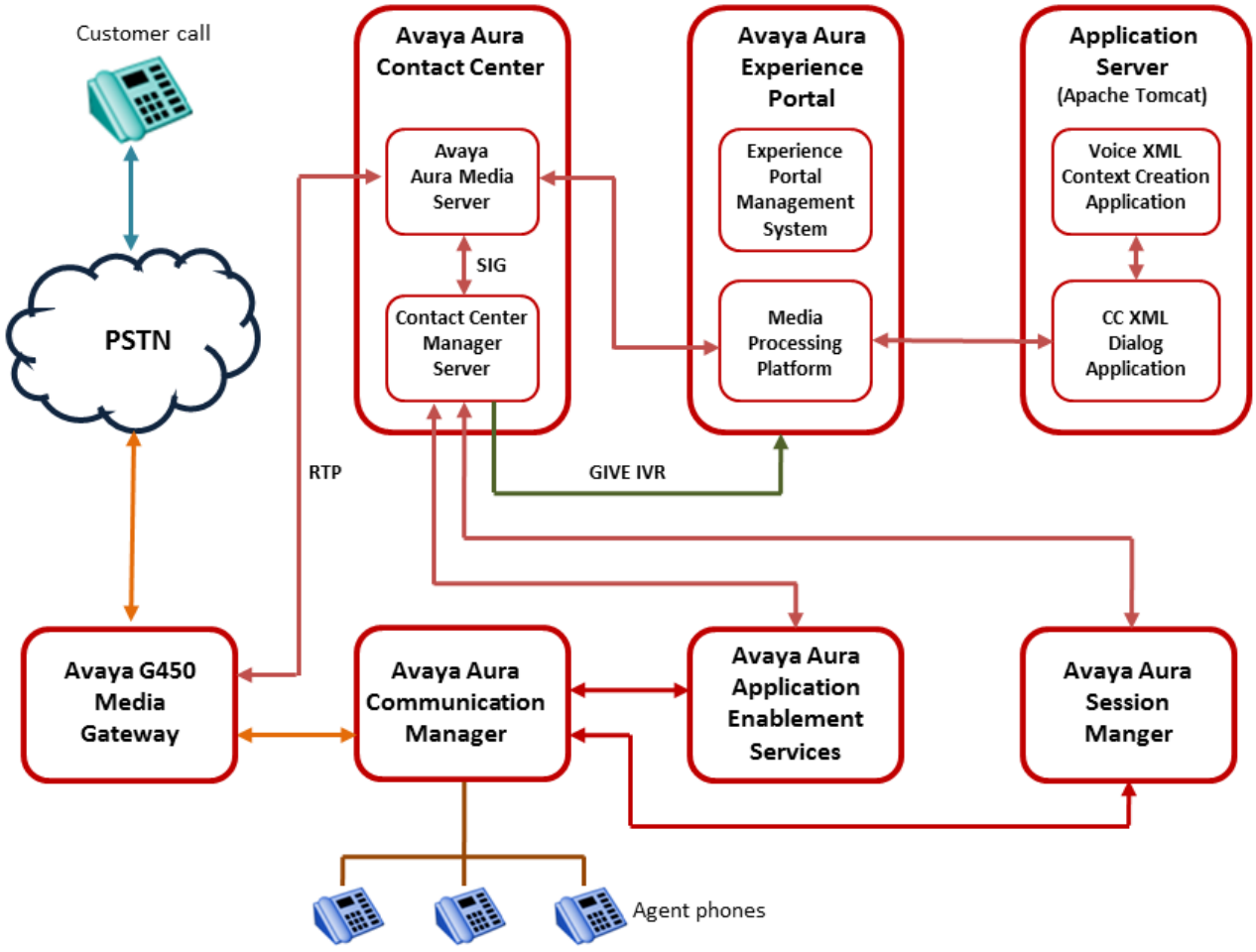


Figure 17: Example of back-end Avaya Aura® Experience Portal using the Context Creation sample application

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 14: Technical support

If you require remote technical support, your distributor or Avaya technical support staff requests to connect remotely to your server. You can receive technical support for your Contact Center server installations through a number of ways.

Secure Access Link for remote support

Avaya requires you to install Avaya Secure Access Link (SAL) on the server to provide remote support. SAL is a remote-access architecture that provides simplified network management and increased security, reliability and flexibility. Secure Access Link (SAL) gives you complete control of when and how Avaya, or any other service partner, can access your equipment.

Microsoft Remote Desktop Connection

By default, Microsoft Remote Desktop Connection for Administration is installed on Windows Server 2012 R2. When you install Windows Server 2012 R2, Microsoft Remote Desktop Connection is installed but not enabled. You must enable the RDC manually.

Microsoft Remote Desktop Connection for Administration requires a TCP/IP connection between the local computer and the remote Contact Center server (that is, a direct modem connection is not available). You have two options to establish a TCP/IP network connection:

- Virtual Private Network (VPN) connection using Avaya VPN Router
- Microsoft Network and dial-up connection for Remote Access Support connection

Virtual Private Network

A Virtual Private Network (VPN) provides more security than directly connected modems. While many VPN technologies and configurations are available for remote support of enterprise voice equipment, Avaya supports a standard technology based on the VPN Router 1100 (or later) in the following host-to-gateway configuration.

When you configure your VPN for remote support, follow these guidelines:

- Create a dedicated subnet for voice application servers (for example, the contact center subnet), and treat this subnet as mission-critical. (It is a good network engineering practice, even in a non-VPN environment, to optimize network traffic by grouping servers that need to communicate with each other on a subnet.)
- Install, at a minimum, VPN Router 1100 (or later) Version 4.8 (or later) with the modem option. Configure the modem as a user-tunnel to listen on the PSTN.
- Connect the VPN Router to the contact center subnet.
- Configure the VPN Router, as well as network routers and firewalls, to give inbound remote support users unrestricted access to the Avaya application servers.
- Optionally, restrict remote support user access to other subnets in your LAN or WAN. As usual, ensure that the Avaya application servers have unrestricted access to the enterprise LAN or WAN.
- Ensure that the ELAN subnet connects to the contact center subnet using a routed solution that adheres to the ELAN Engineering requirements. See *Converging the Data Network with VoIP Fundamentals (NN43001-260)* and *Communication Server 1000M and Meridian 1 Large System Planning and Engineering (NN43021-220)*. Take the additional precaution to configure the network router to permit only intended traffic into the ELAN subnet.
- Activate Split Tunneling on the VPN Router. Concerns over access into the corporate network can be alleviated by restricting access (through the VPN Router and firewalls) of remote support staff from other subnets upon logon.

The configurations described in this chapter meet the needs of most users. However, because every network is different, the exact configurations can not be practical in all environments. Use these recommendations as a starting point and building block when you create your Remote Support VPN. The recommended remote support configurations provide the following benefits:

- Protection for your network from unauthorized external users.
- Any location is accessible, even through an analog line, but remains protected by the VPN.
- Flexible designs exist that can be extended to non-Avaya products and can accommodate customer-specific network requirements.
- VPN equipment is local to the equipment it serves, resulting in network and management simplicity, while providing central security authentication management.
- The solution is cost-effective.

When you deviate from the recommended configurations, you can sacrifice some of these benefits.

You must get a host-to-gateway configuration for the Remote Support VPN. Note the VPN Router connection to the contact center subnet.

Direct-connect modem

If the VPN is not available, you can receive remote support over a direct-connect modem, but many enterprises view this as a security risk.

Due to the operating system communication-layer issues, you cannot configure Contact Center Manager Administration and the Communication Control Toolkit to use Remote Access Services (RAS) (and thereby the direct-connect modem) for remote support. Therefore, if you configure Contact Center Manager Server in a co-resident solution with Contact Center Manager Administration (or Contact Center Manager Administration and Communication Control Toolkit), and VPN access is not available, you can use a direct-connect modem access through an external RAS device on the data-network.

To facilitate remote support through a direct-connect modem the following are required:

- A modem connected to each Contact Center server
- Remote Access Services (RAS) configured on each server

With the listed alternatives, the end-user is responsible for the setup on their premises and the risks to their equipment associated with this pass-through type of connection.

Part 2: Interoperability

Chapter 15: Product compatibility

This section specifies the interoperability and compatibility of Avaya Aura® Contact Center with the other supported components of a contact center solution.

A typical contact center solution includes Avaya Aura® Contact Center and a number of other components such as a telephone platform (PABX), an IVR-system, and optional resources to handle multimedia contacts.

Avaya Aura® Unified Communications platform

Avaya Aura® Contact Center uses industry-standard SIP and CSTA (TR/87 over SIP) interfaces to communicate with SIP-enabled systems such as the Unified Communications platform. 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® Unified Communications phones. The Avaya Aura® Unified Communications platform benefits from Contact Center skill-based routing, call treatments, reporting, and the graphical Orchestration Designer. Avaya Agent Desktop supports Avaya Aura® Unified Communications phones and continues to support voice, email, and Web chat contact types.

Contact Center supports the following Avaya Aura® Unified Communications components:

Avaya Aura® component	Release
Avaya Aura® System Platform	6.2 FP4, 7.0.x, 7.1
Avaya Aura® Solution for Midsize Enterprise	6.2 FP4
Avaya Aura® Communication Manager	6.2 FP4, 7.0.x, 7.1
Avaya Aura® Application Enablement Services	6.2 FP4, 7.0.x, 7.1
Avaya Aura® System Manager	6.2 FP4, 7.0.x, 7.1
Avaya Aura® Session Manager	6.2 FP4, 7.0.x, 7.1

Avaya Aura® component	Release
Avaya Aura® Presence Services	6.2.6, 7.0.0.1 or later

Important:

For more information about the supported Avaya Aura® Unified Communications Service Packs (SPs), Feature Packs (FPs), patches, and deployment types, refer to the Contact Center Release Notes.

Important:

PABX products and other products in your solution follow independent life cycle dates. Depending on their life cycle state, full support might not be available on older versions of these products. In a case where Contact Center patches require a dependent patch on the PABX, that patch might not be available on an old switch release that is in End of Manufacture Support life cycle state. Please refer to life cycle bulletins specific to the products and versions in your solution.

For more information about integrating Contact Center with the Avaya Aura® Unified Communications platform and the required patch levels for each component, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

Multiple AACC instances and a single UC platform

An Avaya Aura® Unified Communications (UC) platform supports up to three Avaya Aura® Contact Center (AACC) servers. 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.

Where multiple AACC instances share a single UC platform, the AACC instances use a single common SIP domain name.

The following table specifies the capabilities shared by up to three Avaya Aura® Contact Center instances.

Capability	Support	Notes and Limitations
Duplex Communication Manager (CM)	Not Supported	
Shared Application Enablement Services server	Supported	Within engineering limits
Shared Session Manager server	Supported	Within engineering limits
Shared Avaya Aura® Workforce Optimization (WFO)	Not Supported	Independent WFO suites required per AACC.
Shared Avaya Aura® Experience Portal (AAEP)	Supported	

Capability	Support	Notes and Limitations
Shared Proactive Outreach Manager (POM)	Not Supported	Requires one to one relationship.
POM instance per AACC	Not Supported	Supports a single POM per CM.
Avaya Control Manager	Supported	
Shared Microsoft instant messaging server – Routed IM	Not Supported	
Shared Microsoft instant messaging server – Peer-to-peer	Not Supported	
Shared Avaya Presence Services – Routed IM	Not Supported	
Shared Avaya Presence Services – Peer-to-peer	Not Supported	
Shared VMware Host	Supported	Within engineering limits
Network Skills Based Routing between the AACC nodes.	Not Supported	

Avaya Aura® Unified Communications phones

Avaya Aura® Contact Center supports the following H.323 phones:

- Avaya 4600 IP deskphones
- Avaya 96x0 Series IP deskphones
- Avaya 9608 Series IP deskphones
- Avaya 9620D03C IP deskphones
- Avaya 96x1 Series IP deskphones
- Avaya Agent Desktop embedded softphone:
  - Ensure you provision an IP_Agent license on the Communication Manager for each softphone used by a contact center agent.
- Avaya one-X® Communicator 5.2 and 6.x softphone. You must disable the Agent Desktop embedded softphone to use Avaya one-X® Communicator concurrently with Agent Desktop.
- Avaya Communicator for Microsoft Lync softphone. You must ensure agents are not configured with the Instant Message (IM) contact type, if they are using Avaya Communicator for Microsoft Lync concurrently with Avaya Agent Desktop.

Avaya Aura® Contact Center supports the following digital phones:

- Call Master IV (603F1) and Call Master V (607A1)
- 9404 Series deskphones
- 9408 DCP Series deskphones

Avaya Aura® Contact Center supports the following SIP phones:

- Avaya 96x0 Series IP deskphones
- Avaya 96x1 Series IP deskphones
- Avaya 9608 IP deskphone
- Avaya one-X® Communicator 6.x softphone. You must disable the Agent Desktop embedded softphone to use Avaya one-X® Communicator concurrently with Avaya Agent Desktop.
- Avaya Communicator for Microsoft Lync softphone. You must ensure agents are not configured with the Instant Message (IM) contact type, if they are using Avaya Communicator for Microsoft Lync concurrently with Avaya Agent Desktop.

Avaya Aura® Contact Center supports SIP phones for DTMF functionality. Avaya Aura® Contact Center supports SIP phones for High Availability functionality.

Avaya Agent Desktop supports three voice modes; Desk Phone, My Computer (softphone), Other Phone (Telecommuter mode).

- For each Agent Desktop agent, supervisor, or agent supervisor using My Computer (softphone) or Other Phone (Telecommuter mode), provision one IP_Agent license on the Communication Manager.
- For each Agent Desktop agent, supervisor, or agent supervisor using Desk Phone mode, the corresponding Communication Manager station consumes one IP_Phone license.
- Agent Desktop agents or agent supervisors that handle only multimedia contacts do not require Communication Manager licenses.

Avaya Communication Server 1000 platform

Avaya Aura® Contact Center supports the Avaya Communication Server 1000 telephone switching platform.

Avaya Aura® Contact Center supports the following Avaya Communication Server 1000 AML-based switches:

AML-based switch	Supported versions
Avaya Communication Server 1000 E	7.6
Avaya Communication Server 1000 E SA Co-res	7.6
Avaya Communication Server 1000 E SA	7.6
Avaya Communication Server 1000 E HA	7.6
Avaya Communication Server 1000 M Single Group	7.6
Avaya Communication Server 1000 M Multi Group	7.6
Avaya Communication Server PBX 11C - Chassis	7.6
Avaya Communication Server PBX 11C - Cabinet	7.6
Avaya Communication Server PBX 61C	7.6

AML-based switch	Supported versions
Avaya Communication Server PBX 51C	7.6
Avaya Communication Server PBX 81C	7.6

New Avaya Aura® Contact Center Release 7.0 AML-based orders and installations support only Avaya Communication Server 1000 Release 7.6. Migrating Avaya Aura® Contact Center from an Avaya Communication Server 1000 platform to Avaya Aura® Unified Communications platform is supported.

To support staged upgrades and migrations, existing solutions using Avaya Communication Server 1000 Release 5.0, 5.5, 6.0, 7.0 or 7.5 can upgrade to Avaya Aura® Contact Center Release 7.0, with the following conditions:

- Avaya Communication Server 1000 (CS 1000) Release 5.0, 5.5, 6.0, 7.0 and 7.5 are End of Manufacture Support for Software (EoMS).
- To receive continued CS 1000 support, you must upgrade to CS 1000 Release 7.6.
- AML-based Avaya Aura® Contact Center Hot-standby High Availability is supported only with CS 1000 Release 7.0, 7.5, and 7.6.

Avaya Communication Server 1000 and other products in your solution follow independent life cycle dates. Depending on their life cycle state, full support might not be available on older versions of these products. In a case where Avaya Aura® Contact Center patches require a dependent patch on the CS 1000, that patch might not be available on an old switch release that is in End of Manufacture Support life cycle state. Please refer to life cycle bulletins specific to the products and versions in your solution.

Engineer the Avaya Communication Server 1000 PABX so it can support Contact Center, in particular engineer PABX resources to support the required agent numbers and call volume. For more information, see Communication Server 1000M Large System Planning and Engineering (NN43021-220) and Communication Server 1000E Planning and Engineering (NN43041-220).

The Avaya Communication Server 1000 Home Location Code (HLOC) must not exceed 3999.

Avaya Communication Server 1000 packages and patches

The following Avaya Communication Server 1000 patch is required in AML-based solutions using an Avaya Communication Server 1000 Release 7.6.

CS 1000 Patch	Comment
MPLR32655	Required if package 411 is enabled. Package 411 disconnects calls when agents attempt to go Not Ready while on a call.

Avaya Communication Server 1000 phones

Contact Center Manager Server supports the following Avaya Communication Server 1000 phones:

- Avaya 39xx Digital Deskphone
  - Avaya 3904 Digital Deskphone
  - Avaya 3905 Digital Deskphone

- IP phones and Softphones
  - Avaya 1120E IP Deskphone
  - Avaya 1140E IP Deskphone
  - Avaya 1150E IP Deskphone
  - Avaya 1200 Series IP Deskphone
  - Avaya 2002 IP Deskphone
  - Avaya 2004 IP Deskphone
  - Avaya 2007 IP Deskphone
  - Avaya 2050 IP Softphone

The following conditions apply:

- Support of specific types of phones can change with each software release of the call server (Avaya Communication Server 1000). Consult the Avaya Communication Server 1000 documents for an up-to-date list of supported phone types for the software release in use.

Avaya Communication Server 1000 AML features

Avaya Aura® Contact Center supports AML-based Avaya Communication Server 1000 switches.

The following table outlines the features supported by the Avaya Communication Server 1000 AML-based switches. Application Module Link (AML) is an internal protocol used by Avaya Aura® Contact Center to communicate directly with Avaya Communication Server 1000.

Table 5: Avaya Communication Server 1000 AML-based features

Feature	Avaya Communication Server 1000 (AML)
Agent features	
Agent logon location	The agent can log on at any ACD phone.
Length of Agent ID	4 to 16 digits
Validation of agent login	Contact Center Manager validates agent login.
Agent non-ACD DN	Personal DN follows agent (FWD)
Call presentation features	Contact Center Manager phone After Call Break, Call Forcing, Alternate Call Answer, Host Delay Time for each agent. After Call Break was formally known as Union Break Time. The Contact Center agent view and reports continue to label this as *UnionBreakTimer*.
Walkaway trigger	Headset removal
Phone features	
Conference	6-way Conference
Transfer and conference	Separate transfer, conference, simple

Feature	Avaya Communication Server 1000 (AML)
Entry/reporting of activity (Line of Business) code	Supported
Blind transfer to CDN	Supported
Agent transfer/ conference from InCalls to second agent InCalls key	Not applicable
Completion of transfer while far end is ringing (including blind transfers)	If the far end address is out-of-provider (not monitored by CCT), the remote connection state transitions immediately from the Alerting state to Established.
Telephone switch resource features	
Telephone switch interface	AML connection
Number of digits for CDN	15
Number of characters for CDN URI	Not applicable
Number of digits for DNIS	7
Number of characters for DNIS URI	Not applicable
Number of digits for agent ID	5
Number of digits for activity (Line of Business) code	3 to 32
Trunk and route statistics and displays	Supported
Synchronization of deleted resources	Reported by telephone switch
Monitoring of link status	Telephone switch brings down link after 20 non response calls
Handling of resources upon link failure	Retained
Recovery after link failure	Issues call release messages
Order of call presentation	Telephone switch alternates Contact Center Manager CDN and NACD ACD calls
Treatments	
IVR	Supports integrated IVR with Avaya CallPilot®
Caller-entered data for external IVR	Not supported
Give IVR script command	Supported
IVR statistics, displays	Supported
RAN	Supported
Controlled option for treatments	Supported. Return to CDN without answer supervision.
Automatic ringback	Supported
Automatic treatment resumption	Supported
Networking features	
Ability to network multiple Contact Center Manager Servers	Supported
Networking statistics and displays	Supported
Other features	

Feature	Avaya Communication Server 1000 (AML)
Call information	Directly supports call information (for example, CLID, DNIS, trunk, NPA)
Hardware dongle	Not required
Call ID reuse	Depends on telephone switch configuration
Language support	Multilanguage support
Reporting of internal and external DN calls	Reported separately
Trigger for pegging of outgoing DN call	Call connection
ACD and NACD calls	Reported separately
Taking skillsets out of service manually	Not applicable
Emergency key	Supported

Avaya Aura® Experience Portal

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.

Avaya Aura® Contact Center supports integration with Avaya Aura® Experience Portal Release 7.0.1, and 7.1, and 7.2.

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 process and use the message. In a contact center solution, you can use SIP headers 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 Communication Server 1000 AML-based solution, Avaya Aura® Contact Center supports Landing Pads for integration with Avaya Aura® Experience Portal. AML-based solutions do not support SIP header Information or Contact Intrinsics as call attached data.

In an Avaya Communication Server 1000 SIP-enabled 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

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

The following table shows the call transfer mechanism supported by each platform type:

Transfer method	CS 1000 AML-based Contact Center	Avaya Aura SIP-enabled Contact Center
Landing Pads	Yes	Yes
UUI SIP header	No	Yes
P-Intrinsic SIP header	No	Yes

Transfer method	CS 1000 AML-based Contact Center	Avaya Aura SIP-enabled Contact Center
SIP INFO message using Context Creation	No	Yes

The following table shows the additional licensing requirements for each Avaya Aura® Contact Center and Avaya Aura® Experience Portal integration type:

Transfer method	CS 1000 AML-based Contact Center	Avaya Aura SIP-enabled Contact Center
Landing Pads	OI Open Queue and OI Universal Networking.	OI Open Queue and OI Universal Networking.
Front-end Avaya Aura® Experience Portal	N/A	No additional licenses required.
Back-end Avaya Aura® Experience Portal	N/A	No additional licenses required.
SIP INFO message using Context Creation	N/A	No additional licenses required.

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.
- 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.

Avaya Aura® 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.

Additional voice services

The following table lists Avaya products and versions that are compatible with Contact Center.

Table 6: Contact Center voice services product compatibility

Product name	Supported releases
Avaya Aura® Workforce Optimization (WFO)	12.1, 15.1
Avaya Workforce Optimization Select (AWFOS)	5.2
Avaya Aura® Experience Portal	7.0.1, 7.1, 7.2
Avaya Proactive Outreach Manager (POM)	Release 3.0.5, 3.1
Avaya CallPilot®	5.1 SU 01 or later

Avaya CallPilot® is not supported in a SIP-enabled Contact Center. For the SIP-enabled Contact Center the Avaya Aura® Media Server component provides media services.

The following table lists other products supported with Contact Center and Avaya Communication Server 1000.

Table 7: Product compatibility with Contact Center

Product name	Supported releases
Remote Office 9150	1.3.4
Remote Office 9110, 9110, IP adapter	1.3.4

For Remote Office, the switch release determines which product version is relevant.

Avaya Breeze™ (EDP) snap-in interoperability support

Avaya Aura® Contact Center supports interoperability with the following Avaya Breeze™ (EDP) based snap-ins:

- Avaya Call Park and Page Snap-in
- Avaya Co-Browsing Snap-in
- Avaya Context Store Snap-in
- Avaya Real-Time Speech Snap-in
- Avaya Smart Caller ID Inbound Snap-in
- Avaya Smart Caller ID Outbound Snap-in
- Avaya WebRTC Snap-in
- Avaya Aura® Presence Services

For more information about these Avaya Breeze™ snap-ins, see the Avaya Support website at http://support.avaya.com.

Avaya Call Park and Page Snap-in interoperability support

Avaya Call Park and Page Snap-in is a telephony feature on Avaya Breeze™. 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 the expert. The call can then be picked up by the paged party by dialing the extension on which the call is parked.

The following list describes the interoperability scenarios for Avaya Call Park and Page Snap-in, and how the scenarios appear from an AACC perspective:

- Call Park: This scenario is similar to a consult transfer, for example an agent performs a consult transfer to the Call Park pilot number. For speed dialing, you can program Call Park pilot numbers on an agent's phoneset. When an agent parks a call, their phoneset displays the Park Extension number at which the system parks the call. The number is not displayed on Agent Desktop.
- Call Retrieve: If the paged party is an AACC agent, this scenario is similar to the agent making a DN out call.
- Call Recall/Return: If the paged party does not retrieve the call, the call is returned back to the original agent that parked the call. This scenario appears as an incoming DN call from an AACC perspective.

AACC cannot report on the parked call, or its return if it is not answered by the paged party.

For additional information about the Avaya Call Park and Page Snap-in, see the Avaya Support website at http://support.avaya.com.

Avaya Real-Time Speech Snap-in interoperability support

Avaya Real-Time Speech Snap-in provides a method of searching for speech on an answered call and reporting matches in real-time. Avaya Aura® Contact Center integrates with the Avaya Real-Time Speech Snap-in to provide policy adherence monitoring and reporting for agents, or to enable automated screen-popping of suggestions to agents based upon customer utterances.

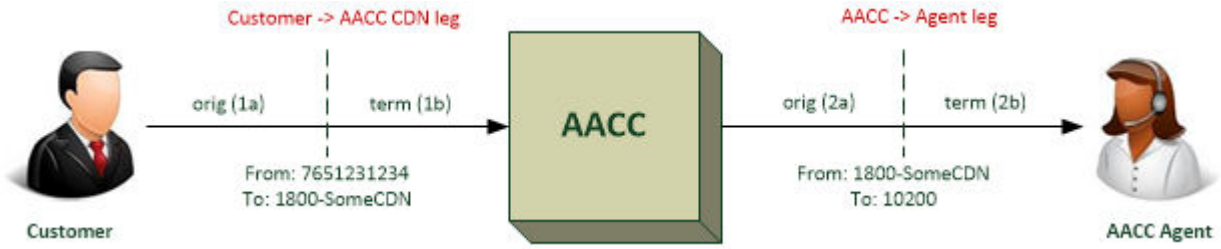
There are multiple options for when to engage the speech search functionality on AACC CDN calls:

1. Enable speech search functionality for calls to AACC CDNs on:
    a. the originating side, allowing calls from specific customer phone numbers (CLID) ranges to be targeted. For example, to speech search calls from specific geographic regions.
    b. the terminating side, allowing specific CDNs to be targeted.
2. Enable speech search functionality for calls from AACC to agent stations on:
    a. the originating side, allowing calls to agents from specific CDNs to be targeted. This is possible as the dialed CDN appears as the calling party for calls to agents.

b. the terminating side, allowing calls to specific agents to be targeted.

Use one or more of the above options in conjunction with Engagement Designer workflows to implement further intelligence on the selection of calls to be searched. For example, from CDN A, B or C to agents in the number range 1004xxx.

The following figure describes the four options listed above.



Identifying AACC CDN Call Parties

The table below provides the call information available about the Breeze™ events generated for the options above:

Call leg	Apparent calling party	Apparent called party
Customer -> AACC CDN	Customer	CDN
AACC -> Agent	AACC CDN	Agent

Avaya Smart Caller ID Inbound Snap-in interoperability support

Avaya Smart Caller ID Inbound Snap-in provides a method of providing a called party with additional information about a calling party. The information is provided from an existing customer database or LDAP system. The Avaya Smart Caller ID Inbound Snap-in integrates with an existing database or LDAP system and uses the calling party number to obtain the additional information. Avaya Aura® Contact Center integrates with the Avaya Smart Caller ID Inbound Snap-in to provide additional customer information agents answering calls.

For additional information about the Avaya Smart Caller ID Inbound Snap-in, see the Avaya Support website at http://support.avaya.com.

Avaya Smart Caller ID Outbound Snap-in interoperability support

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. Avaya Aura® Contact Center integrates with the Avaya Smart Caller ID Outbound Snap-in to present a different caller name and number to customers receiving outbound calls from an agent. For example, companies making calls to different countries or area codes can use this snap-in to present a caller ID name and number which is local (in the same country or area code) to the destination number being called.

For additional information about the Avaya Smart Caller ID Outbound Snap-in, see the Avaya Support website at http://support.avaya.com.

Avaya WebRTC Snap-in interoperability support

Avaya WebRTC Snap-in enables click-to-call from web applications, for example from a customer facing website, or an enterprise directory web page. Integration with this snap-in provides an additional method to bring skillset calls into AACC. Calls from a customer using a browser based application arrive into a customer's enterprise network through Avaya Aura® Session Border Controller. It is routed to Avaya Breeze™, where the Avaya WebRTC Snap-in converts it to a SIP call. This call is then delivered to AACC by Avaya Aura® Session Manager. Although the call originated as a WebRTC call, when it is routed to AACC it appears as if the call has arrived from a SIP network.

For additional information about the Avaya WebRTC Snap-in, see the Avaya Support website at http://support.avaya.com.

Part 3: Licensing

Chapter 16: Licensing requirements

This section describes the Avaya Aura® Contact Center license types, mechanisms, license files, and the licensing grace period. This section also describes how to obtain a license for your Avaya Aura® Contact Center solution.

Contact Center License Manager provides central control and administration of licensing for Avaya Aura® Contact Center. Contact Center License Manager supports the following licensing mechanisms:

- **WebLM license file**: Contact Center License Manager can use an Avaya WebLM license file to control Avaya Aura® Contact Center licensed features.
- **Avaya WebLM server**: Contact Center License Manager can obtain licenses from an Avaya WebLM server, and then use these licenses to control Avaya Aura® Contact Center licensed features.
- **PLIC license file**: Contact Center License Manager can use a PLIC license file to control Avaya Aura® Contact Center licensed features.

Use the Avaya WebLM license file or the Avaya WebLM server option with nodal SIP-enabled Avaya Aura® Contact Center solutions. Use the PLIC license file option with Avaya Communication Server 1000 AML-based (nodal and corporate) Avaya Aura® Contact Center solutions.

Contact Center License Manager supports the following license types:

- **Nodal Enterprise**: licensing type for a single contact center solution.
- **Corporate Enterprise**: licensing type for a network of Avaya Aura® Contact Center installations.
- **Nodal NCC**: licensing type when you install a Network Control Center.
- **Corporate NCC**: licensing type when you install a Network Control Center in a Corporate environment.

Before installing Avaya Aura® Contact Center software, you must choose a license type and a licensing mechanism. The licensing options available to you depend on your Contact Center solution type (AML-based or SIP-enabled), and on the ordering process you use.

License types

Contact Center License Manager supports the following license types:

Nodal Enterprise licensing

The Nodal Enterprise license type controls the licensing for a single Avaya Aura® Contact Center node. Contact Center License Manager uses Nodal Enterprise licensing to control a single installation of Contact Center Manager Server (CCMS), Contact Center Manager Administration (CCMA), Contact Center Multimedia (CCMM), and Communication Control Toolkit (CCT).

The Nodal Enterprise license type is supported by the WebLM and PLIC licensing mechanisms.

In SIP-enabled Avaya Aura® Contact Center solutions that use nodal WebLM licenses, Contact Center License Manager pushes licenses to the Avaya Aura® Media Server servers configured as Media Servers in Contact Center Manager Administration.

Nodal Enterprise licensing does not support a Standby License Manager.

Corporate Enterprise licensing

You can use Corporate Enterprise licensing to distribute licenses to multiple servers so they can share licenses from a single pool.

The Corporate License type is supported only by the PLIC licensing mechanism.

For example, if you have two sites: Galway and Auckland. Both sites share 100 Voice Agents. The Contact Center License Manager is on the Galway Voice and Multimedia Contact Server. When the day starts, all of the voice agents in Galway request licenses from the license server. One hundred licenses are issued in Galway. As Galway closes, the Auckland day starts. As the Galway agents log off, the licenses are made available for the agents in Auckland.

In this example, you require only 100 Voice Agent licenses to share across the two sites.

Each license that the Contact Center License Manager grants to Contact Center Manager Server, Contact Center Manager Administration, Contact Center Multimedia, or Communication Control Toolkit is refreshed by the respective application. This ensures that licenses always return to the Contact Center License Manager pool if the applications fail. The refresh mechanism requires an available network connection to the Contact Center License Manager.

Managing two License Manager servers

In a Corporate Licensing environment, you can configure two Contact Center License Managers: a primary Contact Center License Manager and a secondary Contact Center License Manager. Only one Contact Center License Manager can be active at one time. The primary Contact Center License Manager actively maintains the licenses. The secondary Contact Center License Manager runs as a standby Contact Center License Manager to provide redundancy in a corporate environment. You can configure the secondary Contact Center License Manager as the Standby Contact Center License Manager for the Contact Center License Manager components so that it is not actively used for licenses unless the active Contact Center License Manager fails.

Configure your preferred active Contact Center License Manager as the primary license manager.

Configure the secondary License Manager on any Voice and Multimedia Contact Server or Voice Contact Server. You cannot install the primary and secondary License Manager software on the same server.

The following conditions apply:

- You cannot configure a Standby License Manager in a Nodal licensing environment.
- Do not use the Standby License Manager for load balancing issues.

A Corporate Enterprise license is supported only in Avaya Communication Server 1000 based solutions. Avaya Aura® Unified Communications platform based solutions do not support Corporate Enterprise licensing.

Nodal NCC licensing

Use the Nodal NCC license type to distribute licenses from a single Network Control Center server to multiple Avaya Aura® Contact Center components in a single node.

The Avaya Aura® Contact Center components in a single node solution are licensed by a Nodal NCC license used by a Contact Center License Manager installed on a Network Control Center server.

Corporate NCC licensing

Use the Corporate NCC license type to distribute licenses from a single pool on a Network Control Center server to multiple Avaya Aura® Contact Center nodes. The Avaya Aura® Contact Center nodes share licenses from a single pool controlled by a Corporate NCC license file on a Contact Center License Manager installed on a Network Control Center server.

Corporate license management options reduce the cost of ownership by centralizing the control of software licensing for all elements on a node and all nodes in the network.

A Corporate Enterprise license is supported only in Avaya Communication Server 1000 based solutions. Avaya Aura® Unified Communications platform based solutions do not support Corporate Enterprise licensing.

Licensing mechanisms

Contact Center License Manager supports the following licensing mechanisms:

- **WebLM license file**: You can install a suitably configured WebLM license file on the Contact Center License Manager server. Contact Center License Manager then uses this WebLM license file to control Avaya Aura® Contact Center licensed features. WebLM license files do not support Corporate licensing.
- **Avaya WebLM server on a virtual machine**: Contact Center License Manager supports only Avaya WebLM server Virtualized Environment (VE) vAppliance Release 7.0 as a remote Avaya WebLM server. You can download this vAppliance from Avaya PLDS. Install and commission a suitably licensed VE Avaya WebLM server in your solution. Contact Center License Manager obtains licenses from this Avaya WebLM server, and uses these licenses to control Avaya Aura® Contact Center licensed features. Avaya WebLM server does not support Corporate Licensing.
- **PLIC license file**: You can install a suitably configured PLIC license file on the Contact Center License Manager server. Contact Center License Manager then uses this PLIC license file to control Avaya Aura® Contact Center licensed features.

You can view the licensed features for both licensing mechanisms using the License Manager Configuration Utility.

At startup, Contact Center License Manager identifies the license mechanism and extracts the licenses required by the other Avaya Aura® Contact Center applications and features.

For more information about the licensing mechanisms, see the following:

- WebLM licensing mechanism on page 203
- PLIC licensing mechanism on page 205

WebLM licensing mechanism

Each Avaya Aura® Contact Center License Manager includes a local instance of WebLM. When the License Manager service starts, it checks for a PLIC license file. If License Manager does not find a PLIC license file, it extracts WebLM license keys either from the local WebLM instance or an Avaya WebLM server. License Manager then converts the WebLM license keys into local PLIC license keys and distributes the keys to the Contact Center applications as required.

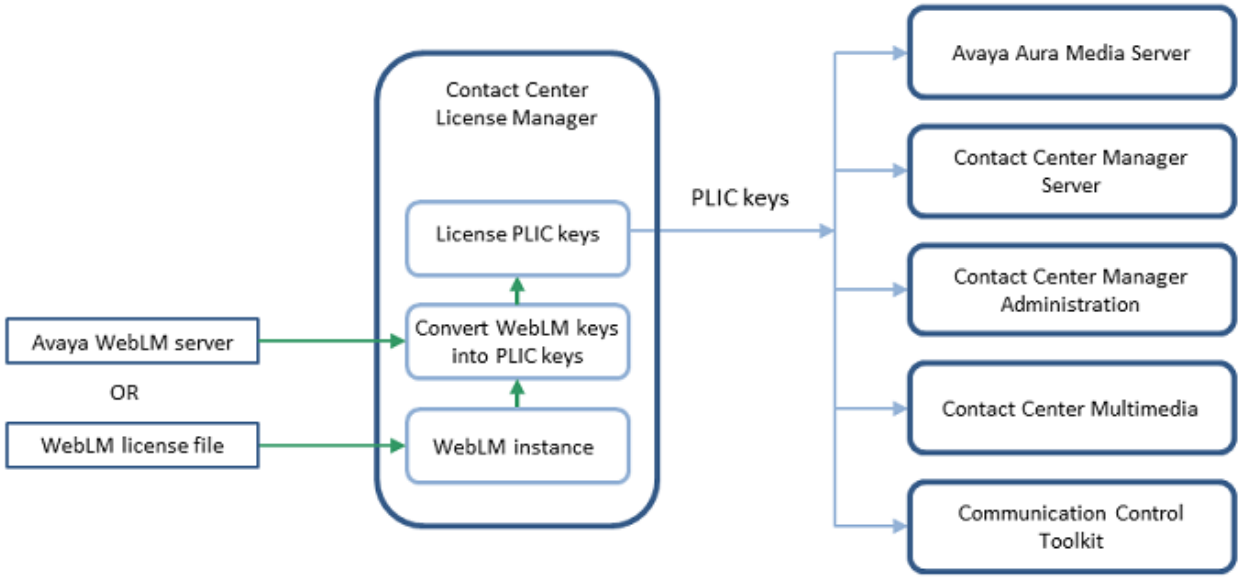
For deployments using an Avaya WebLM server, Contact Center License Manager supports only the Virtualized Environment deployment of Avaya WebLM server.

Contact Center License Manager supplies license keys to Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, and Contact Center Multimedia as required.

If you are using WebLM licensing, when you configure an Avaya Aura® Media Server as a Media Server in Contact Center Manager Administration, Contact Center License Manager pushes the license keys to that Avaya Aura® Media Server. You must restart Contact Center License Manager so it can push the licenses to Avaya Aura® Media Server.

Contact Center supports WebLM in nodal contact centers. WebLM does not support Contact Center corporate licensing.

The following diagram shows how Contact Center License Manager works with either a WebLM license file or an Avaya WebLM license server.



Contact Center License Manager supplies PLIC license keys to the Contact Center applications.

Local WebLM license file:

You use the WebLM Host ID to obtain a SIP-enabled nodal license file from the Avaya Product Licensing and Delivery System (PLDS).

If the WebLM Host ID used in the license file is incorrect, License Manager cannot start. WebLM uses an .xml file to store keys for licensed features.

Licenses on an Avaya WebLM virtual server:

If you use an Avaya WebLM Virtualized Environment (VE) vAppliance, you must use the primary host ID of the Avaya WebLM server to obtain your Contact Center license.

You use the Avaya WebLM primary host ID to activate your Contact Center license on PLDS. You must install and commission Avaya WebLM server, and determine the correct license primary host ID from the WebLM user interface, before activating your Contact Center license.

When Contact Center License Manager requests licenses from an Avaya WebLM server, it reserves all the Contact Center licenses available on that server. Contact Center therefore supports only the PLDS standard license file (SLF) type. Contact Center does not support the WebLM Enterprise model.

Contact Center deployments that use the Mission Critical High Availability or Remote Geographic Node feature, and use VE Avaya WebLM server licensing, must have two VE Avaya WebLM servers.

PLIC licensing mechanism

Avaya Aura® Contact Center supports PLIC license files for nodal and corporate licenses in Avaya Communication Server 1000 based contact center solutions.

Nodal licensing indicates that the licenses are distributed only to that node. You cannot share nodal licenses. A license key in the product name identifies the Nodal Enterprise license.

In Corporate Enterprise licensing mode you can use a secondary License Manager for redundancy. Both the primary and secondary License Managers can use the same license file. A Corporate Enterprise license is supported only in Avaya Communication Server 1000 based solutions. Avaya Aura® Unified Communications platform based solutions do not support Corporate Enterprise licensing. A license key in the product name identifies the Corporate Enterprise license.

Key Recovery System (KRS) uses a plservrc (PLIC) file to store keys for licensed features.

How to obtain an Avaya Aura® Contact Center license

Depending on your contact center type, and on the order tool path you used, you can use one of the following unique numbers to obtain an Avaya Aura® Contact Center (AACC) license:

- Contact Center License Manager server MAC address
- Avaya WebLM host ID
- Avaya Communication Server 1000 serial ID

You can use the unique number provided by one of these options, along with your order number and details, to generate a license for your Avaya Aura® Contact Center software. The unique number (MAC address, CS 1000 serial ID, or WebLM host ID) is encoded into the license file and license keys. When Contact Center License Manager loads the license, if the unique number in the license does not match the solution (MAC address, CS 1000 serial ID, or WebLM host ID), then License Manager shuts down and Avaya Aura® Contact Center cannot process contacts. If the unique number in the license matches the solution, then License Manager provides license keys, and Avaya Aura® Contact Center processes customer contacts.

The following table shows the license file generation methods for each type of Avaya Aura® Contact Center solution.

Table 8: License file generation summary

Unique Number (license key)	Enterprise Nodal SIP	Enterprise Nodal AML	Enterprise Nodal MM-only	Corporate Enterprise
LM server MAC address	Yes	Yes	Yes	Yes
WebLM host ID	Yes	No	Yes	No

Unique Number (license key)	Enterprise Nodal SIP	Enterprise Nodal AML	Enterprise Nodal MM-only	Corporate Enterprise
CS 1000 Serial ID	No	Yes	No	No
Note: The license mechanism is dependent on the order tool path used.				

Important:

A corporate license file can be generated only from the LM server subnet Network Interface Card (NIC) MAC address. WebLM does not support Corporate licensing.

For more details about obtaining a license file, see the following:

- How to obtain a license for a nodal SIP-enabled solution on page 206
- How to obtain a license for a nodal AML-based solution on page 207
- How to obtain a Corporate license on page 208

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:

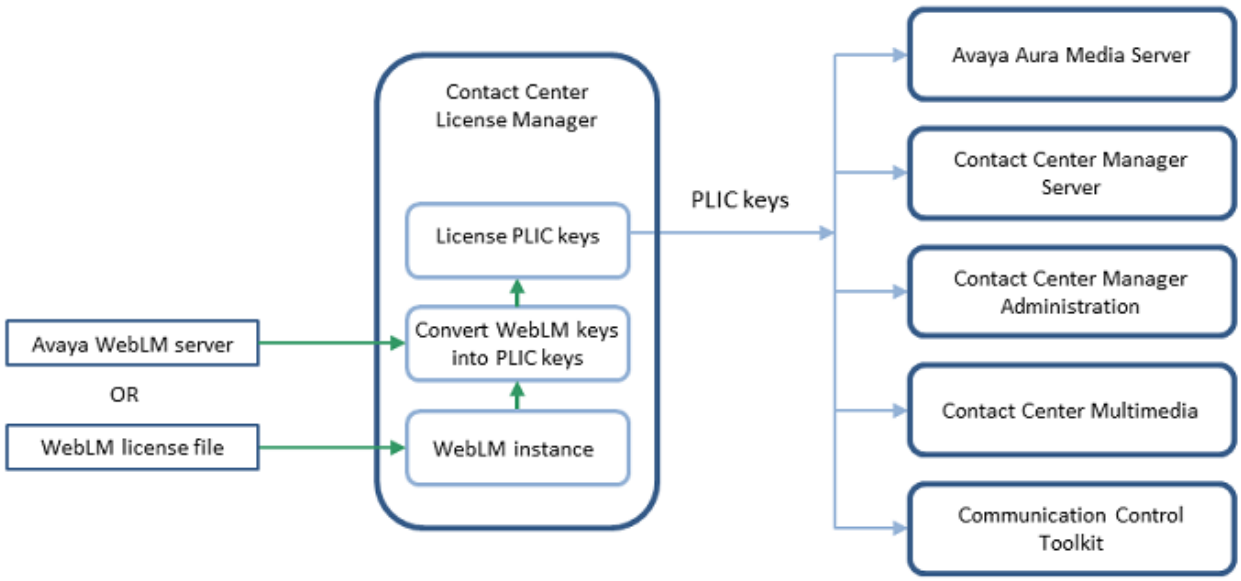


Figure 18: Licensing options for SIP-enabled Contact Center

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.

How to obtain a license for a nodal AML-based solution

Avaya Aura® Contact Center uses a PLIC license file in an Avaya Communication Server 1000 AML-based contact center.

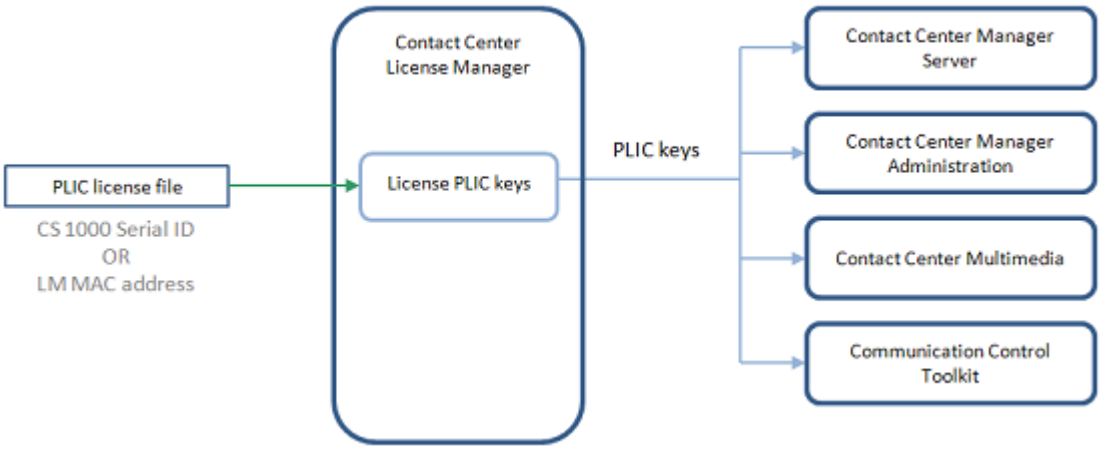


Figure 19: Diagram showing the licensing mechanism options for AML-based Avaya Aura® Contact Center solutions

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

1. Obtain the contact center server subnet NIC MAC address (CLAN NIC MAC address) of the Contact Center License Manager server.
2. Use the CLAN NIC MAC address to obtain a nodal PLIC license file from the Avaya Keycode Retrieval System (KRS).
3. Load the PLIC 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 unique number in the license does not match the LM server MAC address, then License Manager shuts down and Avaya Aura® Contact Center cannot process contacts. If the unique number in the license matches the License Manager server MAC address, then License Manager provides license keys, and Avaya Aura® Contact Center processes customer contacts.

OR

1. Obtain the Avaya Communication Server 1000 serial ID. The Avaya Communication Server 1000 Serial ID is also known as the Site ID.
2. Use the CS 1000 serial ID to obtain a nodal PLIC license file from the Avaya Keycode Retrieval System (KRS).
3. Load the PLIC 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 unique number in the license does not match the CS 1000 serial ID, then License Manager shuts down and Avaya Aura® Contact Center cannot process contacts. If the unique number in the license matches the CS 1000 serial ID, then License Manager provides license keys, and Avaya Aura® Contact Center processes customer contacts.

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.

How to obtain a Corporate license

Avaya Aura® Contact Center solutions that use Corporate licensing must use a PLIC license file. Avaya Aura® Contact Center does not support WebLM for Corporate licensing.

Avaya Aura® Contact Center supports Corporate licensing only for Avaya Communication Server 1000 AML-based contact centers. Corporate licensing does not support SIP-enabled Avaya Aura® Contact Center solutions.

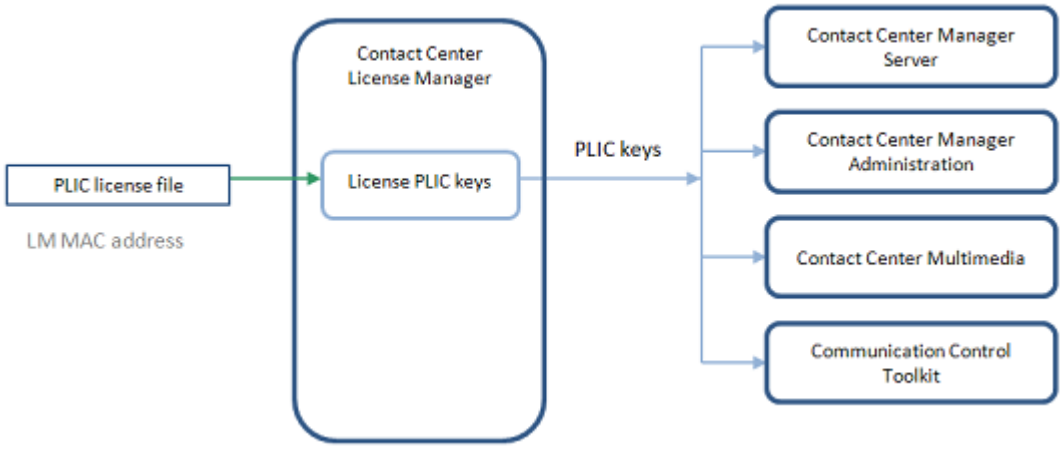


Figure 20: Diagram showing the licensing mechanism used when Avaya Aura® Contact Center uses Corporate licensing

Use the following process to obtain an Avaya Aura® Contact Center Corporate license:

1. Obtain the contact center server subnet NIC MAC address (CLAN NIC MAC address) of the Contact Center License Manager server.
2. Use the CLAN NIC MAC address to obtain a corporate PLIC license file from the Avaya Keycode Retrieval System (KRS).
3. Load the PLIC 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 unique number in the license does not match the LM server MAC address, then License Manager shuts down and Avaya Aura® Contact Center cannot process contacts. If the unique number in the license matches the License Manager server MAC address, then License Manager provides license keys, and Avaya Aura® Contact Center processes customer contacts.

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.

License Manager installation location in a solution

Before installing Avaya Aura® Contact Center software, you must choose a license type, licensing mechanism, and the location for your Contact Center License Manager.

The Contact Center License Manager component is installed on the following Contact Center server types:

- Voice and Multimedia Contact Server
- Voice Contact Server

- Network Control Center Server

The following table shows where to install Contact Center License Manager for a given license type.

Table 9: Contact Center License Manager installation location

License type	Enterprise Nodal	Enterprise Nodal Networked (Nodal NCC)	Corporate Enterprise	Corporate Enterprise Networked (Corporate NCC)
Contact Center License Manager location:	Voice and Multimedia Contact Server — OR — Voice Contact Server	Voice and Multimedia Contact Server — OR — Voice Contact Server	Voice and Multimedia Contact Server — OR — Voice Contact Server	Voice and Multimedia Contact Server — OR — Voice Contact Server

Avaya Aura® Media Server licensing considerations

Avaya Aura® Media Server requires licenses for the conference features.

If you are using WebLM licensing, when you configure an Avaya Aura® Media Server as a Media Server in Contact Center Manager Administration, Contact Center License Manager pushes the license keys to that Avaya Aura® Media Server. You must restart Contact Center License Manager to push the licenses to Avaya Aura® Media Server.

Licensed packages and features

Contact Center License Manager controls and distributes the licenses for the following optional Avaya Aura® Contact Center packages and features.

Agent Greeting

In SIP-enabled contact centers, Agent Greeting allows agents to pre-record their personal greetings. The feature plays the greeting automatically when an agent answers a call.

You must license Agent Greeting to use the Announcement Recorder application.

Avaya Aura® Media Server Zoning

Avaya Aura® Media Server (Avaya Aura® MS) Zoning allows contact center administrators to target a specific Avaya Aura® MS instance or prioritized list of instances when anchoring incoming contact center calls. The administrator chooses the preferred Avaya Aura® MS instance on which to anchor the contact center call using a scripting command in Avaya Aura® Orchestration Designer (OD).

Contact Recording

Multi DN Recording is available for each DN license to enable IP contact recording with a Call Recorder application. When you use Multi DN recording, an AST license is no longer required on the Avaya Communication Server 1000 system. The existing two-key limitation (using the AST licensing model for Call Recording) is removed and the number of keys for each terminal is unlimited. This license must include the total number of DNs including Multiple Appearance DN's that require Call Recording.

Record on Demand is available for each system license to globally trigger Call recording functions by using the Record on Demand, Save Conversation, Malicious Call Trace, and Emergency call keys.

Multiplicity

Multiplicity is the ability of an agent to handle multiple concurrent multimedia contacts. At any one time an agent can be active on a voice and multimedia contact. However, when one contact is active; the others automatically are on hold. The maximum number of concurrent multimedia or non-voice contacts that an agent can be assigned is five.

Networking

Agents and skillsets are configured on a Network Control Center (NCC) and propagated to network servers. If a server has a local skillset with the same name as a network skillset, the network skillset replaces the local skillset.

Offsite Agent

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

Table 10: Offsite Agent license requirements

Solution Component	Per No. Agents	License Required	Additional information
Communication Manager	1 agent	1 IP_Agent (soft phone) or IP_Supv license	Each agent requires a H.323 endpoint.
Contact Center	All	Offsite Agent license	
Contact Center	1 agent	1 agent license	Feature License needed

Open Interfaces Open Queue

The Web services are a series of Open Interfaces provided to third parties to enable application communication based on the SOA architecture. The Web services ensure customers can discover the functions offered by each Web service using the WSDL provided.

Open Interfaces Universal Networking

The Web services are a series of Open Interfaces provided to third parties to enable application communication with multiple switches. The WSDL for the Web services ensure customers can discover the functions offered to incorporate them into their own environment.

Open Queue

With Open Queue, you can queue voice and multimedia contacts in Contact Center and then route the contacts to agents by using the Avaya Agent Desktop. Configure Open Queue by using the Contact Center Manager Server Configuration utility. Open Queue is included by default with multimedia agents. Open Queue is available as an optional extra with the SOA Development Kit.

Outbound

Use the Multimedia server and the Outbound Campaign Management Tool in Contact Center Manager Administration to create progressive outbound campaigns on which calls are passed to agents and made from the Contact Center.

For more information about the Outbound feature, see *Avaya Aura® Contact Center Client Administration*.

Report Creation Wizard

Report Creation Wizard provides a method to customize historical reports within Contact Center.

Report Creation Wizard is a user-based license. License Manager controls the maximum concurrent Report Creation Wizard users.

Contact Center Manager Administration includes a one-user license for the Report Creation Wizard feature. You can order additional licenses in groups of 5 up to a maximum of 25 licenses (that is, 5, 10, 15, 20, or 25 licenses).

For more information about Report Creation Wizard, see the *Using Avaya Aura® Contact Center Reports and Displays*.

Standby Server High Availability

Contact Center supports the Active/Standby High Availability model. The active server processes contacts. The standby server takes over if the active server fails or is shutdown for maintenance.

TLS SRTP Signaling and Media Encryption

Avaya Aura® Contact Center (AACC) supports implementing Secure Real-Time Transport Protocol (SRTP) for voice contacts within the contact center.

Secure Real-Time Transport Protocol (SRTP) is an extension to the Real-time Transport Protocol (RTP) to support secure real-time communications. The primary use of SRTP is to encrypt and authenticate voice over IP (VOIP) on the network.

Universal Networking

Universal Networking is the networking between switch types:

- Network Skill-based Routing between all switch types supported by Contact Center
- attached data transport during agent-initiated transfers or conferences under the control of the Communication Control Toolkit

Web Based Statistics

An agent can use a peer-to-peer feature to exchange instant messages with other agents in the contact center while handling a customer contact. If the Web Reporting server is enabled, the peer-to-peer instant messages are tracked in the Contact Summary Report. If an agent creates a peer-to-peer IM while idle, the IM is not tracked.

Announcement and Dialog treatment licensing

In a SIP-enabled Contact Center, ensure that you have the required number of ANNC and DIALOG licenses. These licenses are based on following license keys:

PLDS / WebLM xml license

- VALUE_CCTR_ANNOUNCE_PORTS
- VALUE_CCTR_DIALOG_PORTS

The Avaya Aura® Contact Center Task Flow Executor (TFE) service controls the ANNC and DIALOG licensing. At startup, the TFE service reads the number of licenses from License Manager. If a new license file is applied with a change to the ANNC or DIALOG license count, then you must restart the TFE service.

The Orchestration Designer (OD) GIVE IVR script command is the only command that consumes ANNC or DIALOG licenses. When the GIVE IVR command completes, it returns the license to the free license pool. The GIVE IVR command consumes a DIALOG license if it is playing an announcement and collecting digits. The GIVE IVR command consumes an ANNC license only when playing an announcement.

The following OD script commands do not consume ANNC or DIALOG licenses:

- GIVE RINGBACK
- GIVE RAN <route>
- GIVE MUSIC <route>

Task Flow Executor (TFE) writes the following events to the Windows Event Log:

Category	AMS Dialog
Event	48582
Severity	Critical
Description	AMS Dialog license usage has reached critical condition

Category	AMS Dialog
Event	48583
Severity	Critical
Description	AMS Dialog license usage has reached major condition

Category	AMS Announcement
Event	48584
Severity	Critical
Description	AMS Announcement license usage has reached critical condition

Category	AMS Announcement
Event	48585

Severity	Critical
Description	AMS Announcement license usage has reached major condition

License thresholds are reported at 80% (major) and 90% (critical) usage condition. Both threshold percentages are configurable using the Windows Registry.

About the license file

The Contact Center License Manager offers flexible licensing options and supports licensing of features at the node (Nodal license) or network (Corporate license) level. You can use either a local license file or a remote Avaya WebLM server, to provide Avaya Aura® Contact Center licenses to License Manager.

The license file provides a single point of administration for licensing, and includes keycodes for Contact Center Manager Server, Contact Center Manager Administration, Contact Center Multimedia, and Communication Control Toolkit. This single file reduces the number of separate keycodes that you must maintain. If you require additional features, or if your requirements change, you can replace the existing licensing file.

Contact Center License Manager supports two license file mechanisms: PLIC or WebLM.

Interpretation of the license file

Contact Center licensing includes both agent and feature licensing.

Agent licenses

Agent licenses determine the number of agents that can log on to Contact Center. Agent licenses are available for both Nodal and Corporate Licensing.

Licensing is available for the following types of agents:

- voice agent
- outbound agent
- email agent (covering FAX messages, SMS text messages, voice mail messages, and scanned document messages)
- Web communications agent (or Web chat agents)
- Instant messaging agent
- offsite agent

Feature licenses

Contact Center License Manager controls access to contact center features that require a license. For a list of Avaya Aura® Contact Center licensed features, see Licensed packages on page 210.

Contact Center License Manager license identifiers

License identifiers connect a license file to a particular server or to a particular installation. License Manager converts WebLM identity keys into local PLIC license keys and distributes the keys the Avaya Aura® Contact Center applications as required. Avaya Aura® Contact Center applications continue to consume PLIC license keys.

The following table lists all Avaya Aura® Contact Center specific WebLM license identifiers and compares them to the PLIC license identifiers.

In a PLIC license file, the license identifier has the letter *N* appended when the license type is nodal, and the letter *C* appended when the license type is corporate enterprise. For example, the license identifier for the Maximum Inbound Voice Networked Agents (LM_LOC_VOA) appears as LM_LOC_VOAN in a nodal license file, and as LM_LOC_VOAC in a corporate enterprise license file.

Table 11: License identifiers used by Avaya Aura® Contact Center

PLIC license identifier	Description	WebLM license identifier
NODAL or CORPORATE	Installation	–
–	Solution Type	VALUE_CCTR_TYPE
–	Base system	VALUE_CCTR_BASE
LM_ENTERPRISE	Offer type	VALUE_CCTR_OFFER
LM_NET_VOA LM_NETWORKING = 1	Maximum Inbound Voice Networked Agents	VALUE_CCTR_IN_VOICE_AGENT_NET
LM_LOC_VOA	Maximum Inbound Voice Standard Agents	VALUE_CCTR_IN_VOICE_AGENT_STD
LM_VOD	Maximum Contact Center devices	VALUE_CCTR_CTIDT_CC
LM_ENTERPRISE LM_MULP LM_OB =1 LM_IM_PRESENCE LM_CONTACTREC LM_OI	Maximum Contact Center Manager Standard nodes	VALUE_CCTR_CCM_STD_NODE
LM_ENTERPRISE LM_MULP LM_OB =1 LM_IM_PRESENCE LM_CONTACTREC	Maximum Contact Center Manager Network nodes	VALUE_CCTR_CCM_NET_NODE

PLIC license identifier	Description	WebLM license identifier
LM_OI LM_HETERO LM_HET_ADM		
LM_MMP	Maximum Contact Center Multimedia nodes	VALUE_CCTR_CCMM_NODE
LM_CCT	Maximum Communication Control Toolkit nodes	VALUE_CCTR_CCT_NODE
If LM_NETWORKING = 1 set LM_NET_EMA, else set LM_LOC_EMA.	Maximum email agents	VALUE_CCTR_EMAIL_AGENT
If LM_NETWORKING = 1 set LM_NET_SMS, else set LM_LOC_SMS.	Maximum SMS agents	VALUE_CCTR_SMS_AGENT
If LM_NETWORKING = 1 set LM_NET_WCA, else set LM_LOC_WCA. If LM_NETWORKING =1 set LM_NET_VDA, else set LM_LOC_VDA.	Maximum Web chat agents	VALUE_CCTR_WEB_CHAT_AGENT
LM_OB =1 If LM_NETWORKING = 1 set LM_NET_OBA, else set LM_LOC_OBA. If LM_NETWORKING = 1 set LM_NET_PRA, else set LM_LOC_PRA	Maximum Preview/ Progressive Outbound agents	VALUE_CCTR_VOICE_PPOB
LM_MULP	Multiplicity	VALUE_CCTR_MULTIPLICITY
If LM_NETWORKING = 1 set LM_NET_IMA, else set LM_LOC_IMA. LM_IM_PRESENCE	Maximum Instant Message agents	VALUE_CCTR_IM
LM_STANDBY	Maximum CCM Standby Servers	VALUE_CCTR_CTIDT_RED_CCM
LM_CCT_STN	Maximum CCT Standby Servers	VALUE_CCTR_CTIDT_RED_CCT
LM_OI	Open Interface	VALUE_CCTR_OI
LM_OI LM_OIOpenQ LM_OIOpenN	SOA Development Kit	VALUE_CCTR_DEV_KIT

PLIC license identifier	Description	WebLM license identifier
LM_RCW_USER	Maximum Report Creation Wizard user licenses	VALUE_CCTR_REPORT_WIZ
LM_AGT If LM_NETWORKING = 1 set LM_NET_GRE, else set LM_LOC_GRE	Maximum Agent Greeting licenses	VALUE_CCTR_AGT_GREET
LM_OFF_SITE = 1	Maximum Offsite agent seats	VALUE_CCTR_OFFSITE_AGT
–	Maximum Geographical Standby Servers	VALUE_CCTR_CTIDT_RED_GEOG
–	Maximum Network Standby Servers	VALUE_CCTR_RED_NET
LM_CCS350 = 1 LM_HET_ADM	Maximum Network Control Center Servers	VALUE_CCTR_NCC_SVR
–	Maximum Network Control Center Standby Servers	VALUE_CCTR_NCC_RED_SVR
LM_WBSTAT	Web Statistics	FEAT_CCTR_WEBSTAT
LM_OQ	Open Queue	FEAT_CCTR_OQ
If LM_NETWORKING = 1 set LM_NET_OQA, else set LM_LOC_OQA	Open Queue Agent	VALUE_CCTR_OQ_AGENT
LM_OIOpenN	Open Interfaces Open Networking	FEAT_CCTR_OIOPEN
plicd	Maximum License Managers	VALUE_CCTR_PLICD
N/A	Maximum Announcement concurrent sessions. Consumed by the Contact Center Task Flow Executor (TFE) component.	VALUE_CCTR_ANNOUNCE_PORTS
N/A	Maximum Dialog concurrent sessions. Consumed by the Contact Center Task Flow Executor (TFE) component.	VALUE_CCTR_DIALOG_PORTS

PLIC license identifier	Description	WebLM license identifier
N/A	Maximum Avaya Aura® Media Server Instances.	Contact Center reads the number of licensed Avaya Aura® Media Server instances (VALUE_CCTR_AMS_INSTANCE) and automatically provides the SIP port licenses to the Avaya Aura® Media Server(s).
N/A	Contact Recording.	VALUE_CCTR_CONTACTREC
N/A	TLS SRTP Signaling and Media Encryption.	FEAT_CCTR_TLS_SRTP
N/A	Avaya Aura® Media Server Zoning.	FEAT_CCTR_AMS_ZONING

Licensing requirements for Agent Desktop features

Avaya Agent Desktop is a licensed client application of Avaya Aura® Contact Center. There are two basic types of license; a seat license and a site license.

A seat license controls the features an agent can perform. For example, 100 *Inbound Voice Agent* licenses permits 100 agents to log on and handle voice contacts. Or 50 Web Chat licenses permits 50 agents to log on and handle Web Chat sessions with customers.

A site license controls the features an AACC node or site can perform. A site license permits all the agents at that site to perform a specific function. For example, a High Availability license permits all agents to continue processing customer calls after a switchover in a resilient solution.

Some Agent Desktop features require an active Contact Center Multimedia (CCMM) server for the feature to work. Some Agent Desktop features require CCMM only for feature configuration.

The following table shows the licensing requirements for Avaya Agent Desktop features, and if CCMM is required.

Agent Desktop feature	AACC license	License key	Type	CCMM	Note
Log on to Agent Desktop as an Agent or a Supervisor/Agent	Maximum Inbound Voice Standard Agents or any multimedia contact license or both.	For example, LM_LOC_VOAN, or LM_LOC_EMAN or LM_LOC_WCAN or LM_LOC_IMAN	Seat	No	Agents can log as voice-only agents, multimedia-only agents, or blended agents. Blended agents can handle both voice and multimedia contacts. —

Agent Desktop feature	AACC license	License key	Type	CCMM	Note
					Voice-only agents do not require CCMM to log on.
Handle voice contacts using desktop phone (Desktop Phone mode)	—	—	—	No	Provision an IP_Phone license on Avaya Aura® Communication Manager for each Desktop Phone used by AACC.
Handle voice contacts using softphone (My Computer mode)	—	—	—	No	Provision an IP_Agent license on Avaya Aura® Communication Manager for each softphone used by AACC. See Note 1.
Handle voice contacts in Telecommuter mode. (Other Phone mode.) Supported in Avaya Aura® Communication Manager based solutions.	Maximum Offsite agent	LM_OFF_SITE	Site	No	Provision an IP_Agent license (soft phone) on Avaya Aura® Communication Manager for each offsite agent.
Log on to Microsoft instant messaging	—	—	—	Yes	Required for peer-to-peer Instant Messaging or for Instant Messaging (IM) contacts.
Log on to Avaya Presence Services	—	—	—	Yes	Required for peer-to-peer Instant Messaging or for Instant Messaging (IM) contacts.
Handle email contacts	Maximum email agents	LM_LOC_EMAN	Seat	Yes	
Handle Web communications (Web chat) contacts	Maximum Web Chat agents	LM_LOC_WCAN	Seat	Yes	

Agent Desktop feature	AACC license	License key	Type	CCMM	Note
Handle Instant Messaging (IM) contacts	Maximum Instant Message agents	LM_LOC_IMAN	Seat	Yes	
Handle fax contacts	Maximum email agents	LM_LOC_EMAN	Seat	Yes	One email license is used to handle an email, or a fax message.
Handle scanned document contacts	Maximum email agents	LM_LOC_EMAN	Seat	Yes	One email license is used to handle an email, or a scanned document message.
Handle Voice mail messages	Maximum email agents	LM_LOC_EMAN	Seat	Yes	One email license is used to handle an email, or a Voice mail message.
Handle Social Networking contacts	Maximum email agents	LM_LOC_EMAN	Seat	Yes	One email license is used to handle an email, or a Social Networking contact.
Handle Short Message Service (SMS) text message	Maximum email agents	LM_LOC_EMAN	Seat	Yes	One email license is used to handle an email, or a SMS text message.
Handle Outbound calls and callbacks	Maximum preview/ progressive outbound agents	LM_LOC_OBAN	Seat	Yes	
POM contacts	Maximum POM agents	LM_LOC_PRAN	Seat	Yes	
Support Agent Greeting	Maximum Agent Greeting licenses	LM_LOC_GREN	Seat	No	
Support third call appearance button (Third Line Appearance) for voice	N/A	N/A	—	No	No additional AACC license requirement.

Agent Desktop feature	AACC license	License key	Type	CCMM	Note
Support voice call join	N/A	N/A	—	No	No additional AACC license requirement.
Phonebook (LDAP)	N/A	N/A	—	Yes	Supported for agents that are licensed for any multimedia contact type.
After Call Work	N/A	N/A	—	Yes	
Activity Codes	N/A	N/A	—	Yes	
Not Ready Reason Codes NRRC (When not using Offsite Agent.)	N/A	N/A	—	Yes	
Multiplicity	Multiplicity	LM_MULPN	Site	Yes	
High Availability Agent Desktop functionality	High Availability	LM_STANDBYN and LM_CCT_STNN	Site	Yes	
Agent Statistics	Web Statistics	LM_WBSTATN	Site	Yes	
Display skillset statistics	Web Statistics	LM_WBSTATN	Site	Yes	
Voice contact history	Maximum Inbound Voice Standard Agents	—	Seat	Yes	Supported for agents that are licensed to handle voice contacts (LM_LOC_VOAN) .
Multimedia contact history	Any multimedia contact license	For example, LM_LOC_EMAN or LM_LOC_WCAN or LM_LOC_IMAN	Seat	Yes	
Customer Details information	Any multimedia contact license	For example, LM_LOC_EMAN or LM_LOC_WCAN or LM_LOC_IMAN	Seat	Yes	Information such as Title, Last Name, or First Name.
Screen Pops	Maximum Inbound Voice Standard Agents OR any multimedia contact license	For example, LM_LOC_VOAN or LM_LOC_EMAN or LM_LOC_WCAN or LM_LOC_IMAN	Seat	Yes	To receive a screen pop for a contact type, the agent must be licensed to handle that contact type.
Create a customer record	Any multimedia contact license	For example, LM_LOC_EMAN or	Seat	Yes	

Agent Desktop feature	AACC license	License key	Type	CCMM	Note
		LM_LOC_WCAN or LM_LOC_IMAN			
Add or edit customer information	Any multimedia contact license	For example, LM_LOC_EMAN or LM_LOC_WCAN or LM_LOC_IMAN	Seat	Yes	
Bar a customer phone number	Outbound license and any multimedia contact license	LM_LOC_OBAN and LM_LOC_EMAN or LM_LOC_WCAN or LM_LOC_IMAN	Seat	Yes	
View CCT intrinsic information	—	—	—	No	No additional AACC license requirement.
View or modify User to User Information	—	—	—	No	No additional AACC license requirement.
View customer contact intrinsics	—	—	—	No	No additional AACC license requirement.
Dashboard	—	—	—	No	CCMM server is not required, but without one the Agent Desktop dashboard offers reduced functionality.

- Note 1: Using the Agent Desktop softphone to handle a voice media stream using Voice over IP (VoIP) requires considered network bandwidth and topology planning. For more information, see Agent Desktop client network infrastructure requirements on page 406.
- Note 2: The above table shows Nodal license keys. Corporate and Networking licensing are also supported in Avaya Communication Server 1000 AML-based solutions.

The following Agent Desktop functions are supported only by logged-in supervisor/agents:

- Observe an inbound voice contact or non-skillset call (supervisor/agents only).
- Barge-in on an inbound voice contact or non-skillset call (supervisor/agents only).
- Observe a Web Communications contact (supervisor/agents only).
- Barge-in on a Web Communications contact (supervisor/agents only).
- Recording skillset tags using Agent Greeting.
- Display statistics for all skillsets. (Supervisors in a multimedia environment see all skillsets.)
- Close contacts from search results. Supervisors must enter a reason when closing a contact.

To perform the following functions, Agent Desktop agents must have an assigned and logged-in Agent Desktop supervisor:

- Use the Emergency key.
- Conference in a supervisor.
- Call a supervisor.

Licensing grace period

If a communication error occurs between a Contact Center application and the Contact Center License Manager, normal operation of the Contact Center application continues for a grace period.

The grace period is 30 days. If a communication problem occurs between Contact Center Manager Server and Contact Center License Manager, 30 days are available for the Contact Center Manager Server to continue normal operation. After the communication problem is resolved, the grace period adds back 20 minutes every 20 minutes until the grace period is back up to 30 days. For example, if the communication problem is resolved in two days, the grace period counts backs up to 30 days after two days of successful connection to the Contact Center License Manager.

If Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT) or Contact Center Multimedia (CCMM) cannot communicate with the License Manager, they continue to function for a period of time, called a grace period. If the grace period expires CCMS, CCT, and CCMM shut down and are locked. You cannot restart them without resetting the grace period using the License Grace Period Reset Utility.

If, at any stage, the grace period expires, Contact Center Manager Server shuts down and is locked. You cannot restart Contact Center Manager Server without resetting the grace period.

You can reset the grace period to 30 days at any time. When a communication error is detected, an event is fired to the Server Utility detailing that an error occurred, the time already elapsed in the grace period, and a lock code that you must return to Avaya to reset the grace period.

Contact Center Manager Administration (CCMA) updates the Grace Period Status every 6 hours. To verify the current Grace Period status, refresh the Contact Center Manager Server server on CCMA. Contact Center Manager Administration then displays the current Grace Period Status.

Emergency license files

If you cannot fix the connection between the Contact Center License Manager and Contact Center Manager Server within the 30-day grace period, contact your Avaya customer service representative to determine if you need to activate an emergency license file on your system.

The emergency license file expires after 30 days and is used only to ensure temporary operation of the Contact Center Manager Server. When an emergency license is provided to a customer, a daily Windows event is generated. The Windows event warns the customer of the number of days left for

the emergency license to expire. Customers can then ensure that operations on Contact Center Manager Server resume before the emergency license expires.

You must install the emergency license file through the Contact Center License Manager configuration tool. If you use corporate licensing, you might need to change the Contact Center Manager Server configuration if the Contact Center License Manager is installed on a different server than it was previously.

License manager statistics

Contact Center License Manager produces historical reporting data to support the analysis and management of concurrent license usage in the network. Historical data is available in 15-minute intervals daily, weekly, or monthly. License utilization is reported on a client basis, with the IP address of the client used to denote individual clients.

The Contact Center License Manager reports the following statistics:

- Timestamp—The time the data is written to the database.
- IP Address—The IP address of the Contact Center Manager Server, Contact Center Manager Administration, Contact Center Multimedia, and Communication Control Toolkit.
- License identifier—The name of the license.
- Maximum allocation during interval—The maximum number of licenses allocated to the server during the 15-minute interval.

If an interval has 10 licenses issued for a feature, then 10 is written to the database table. If another 5 licenses are issued in the next interval, then 15 is written to the database table. However, at the end of the interval, if only 14 licenses were issued, but 15 were issued at some stage during the interval, then a value of 15 is written to the database.

The data is written to the database on the server on which you installed the License Manager for each 15-minute interval. These statistics are consolidated daily, weekly, and monthly.

The License Manager reports any errors by writing error data to the database. The data is stored on a site-by-site basis where the site identifier is the IP address of the server.

A report template is available to generate reports using this statistical information. The data is available from the following database views:

- iLicenseStat—interval statistics
- dLicenseStat—daily statistics
- wLicenseStat—weekly statistics
- mLicenseStat—monthly statistics

Real-time statistics

You can use the Real Time Usage tab in the Contact Center License Manager utility to view a snapshot of the licenses issued by the License Manager.

Part 4: Performance specifications

Chapter 17: Maximum overall capacities

This section specifies the maximum overall capacities for Avaya Aura® Contact Center Release 7.0.

Maximum capacity overview

The following table specifies the maximum overall capacity values supported by Avaya Aura® Contact Center.

Table 12: Overview of maximum Avaya Aura® Contact Center capacity figures

Switch Type	Number of active agents	Calls per hour
Avaya Aura® - SIP	3000	45 000
Avaya Aura® Contact Center software appliance for VMware	400	8000
Avaya Communication Server 1000 - AML	5000	100 000
Avaya Aura® Solution for Midsize Enterprise 6.2 - SIP	600	10 000
Multimedia only (No voice platform)	3000	12 000

The following conditions apply to the table:

- The capacities supported on a server are limited by the server performance.
- 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.

For the complete list of capacity limits, see Maximum agent capacity and call rate values on page 229.

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 13: Contact Center capacity figures in detail

Parameter	SIP maximum	AML 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 • Avaya Aura® Solution for Midsize Enterprise based SIP: 600	5,000 The maximum of 5000 logged on agents is only applicable for the Avaya Communication Server 1000 Release 7.6.
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 • Avaya Aura® Solution for Midsize Enterprise based SIP: 600	3,000
Number of agents defined in the system	10,000	10,000
Number of phones:	N/A	10,000
Number of supervisors logged on	600	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	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	1,500
Number of active scripts	1,000 (997)	1,000 (997)

Parameter	SIP maximum	AML maximum
The product contains three predefined scripts. Therefore, you can create 997 scripts.		
Maximum script size—Master_Script (characters)	100,000	100,000
Maximum script size—other scripts (characters)	50,000	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)	1,005 (1,000)
Number of user defined call variables	500	500
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.	N/A
Number of skillsets The maximum includes both local skillsets and network skillsets.	3,000	3,000
Number of skillset priority levels	48	48
Number of skillsets for each call	20	20
Number of activity codes The product contains five predefined activity codes. Therefore, you can create 4995 activity codes.	5,000 (4,995)	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	100,000
Stand-alone Multimedia server Inbound Multimedia contacts per hour (for stand-alone server)	12,000	12,000
Co-resident Multimedia server Inbound Multimedia contacts per hour	2,400	2,400
Stand-alone Multimedia server new contacts backlog	100,000 The Extended Email Capacity backlog is 100 000 contacts.	100,000 The Extended Email Capacity backlog is 100 000 contacts.

Parameter	SIP maximum	AML maximum
Co-resident Multimedia server new contacts backlog	4,000	4,000
Number of waiting contacts	3,000	3,000
Call resources parameters		
Number of IVR queues (Communication Server 1000)	N/A	150
Number of IVR ports	1,000	1,000
Number of ACCESS ports (Communication Server 1000)	N/A	191
Number of routes	513	513
Number of CDNs	5,000	2,000
Number of RAN and music routes	512	512
Number of DNISs	10,000	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 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).	500	500
Number of assigned active agents per supervisor for observe and barge-in.	25	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)	N/A
Number of presence changes per hour	200,000	N/A
Assignment parameters		

Parameter	SIP maximum	AML maximum
Number of agents in an agent-to-supervisor assignment (No CCT)	1,000	1,000
Number of agents in an agent-to-supervisor assignment (CCT enabled)	100	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	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	1,500
Networking parameters		
Number of call processing nodes in the network (including local node)	30	30

Parameter	SIP maximum	AML maximum
The number of configured nodes is 30; however, only 20 nodes can be configured in the routing table.		
Number of network skillsets The maximum includes the predefined skillsets, local skillsets, and network skillsets.	1,500	1,500
Number of skillsets per agent	150	150
Number of sites in the routing table for a network skillset	20	20
Number of network skillsets to which a call is queued	10	10
Number of agent reservation requests per call	30	30
Number of remote applications (applications accessible over the network)	6,000	6,000
Network calls per hour for which CBC data is collected	10,000	10,000
Number of target nodes	20	20
Database parameters		
Number of client PCs and RTI applications connected to the database	100	100
Number of other applications connected to the database	100	100
Number of Fault Management messages in database	7,500	7,500
Maximum number of report clauses The database server supports a maximum of 255 clauses on a single SQL statement.	255	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	1,000,000

Parameter	SIP maximum	AML maximum
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 240.	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 240.
Maximum number of multimedia contacts per customer	1,000	1,000
Third-party interface parameters		
Number of MLS applications	N/A	16
Number of MLS DN registrations across all MLS applications	N/A	11,000
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	58,000
Number of HDX connections When configured, Database Integration Wizard (DIW) uses a single HDX connection.	10	10
Number of RTI client systems/ applications	100	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	1
Steady state CPU	70%	70%
Number of CCMS servers per Avaya Communication Server 1000	3 (Only to support phased migration between Contact Center releases)	3

Parameter	SIP maximum	AML maximum
Number of AML-based application servers per Avaya Communication Server 1000	N/A	16
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	0
Number of Phonebook entries on Avaya Agent Desktop	10,000	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	AML	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	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	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	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.	No	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 14: 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

Historical Reporting safeguards and maximums

Avaya Aura® Contact Center blocks historical reports that pull more than 50,000 records from the database. This maximum limit safeguards the memory and CPU usage on the Avaya Aura® Contact Center server. Avaya recommends that you run reports with selection criteria that reduce the amount of data on the report.

Contact Center Manager Server Call load

Call complexity and call rate determine the CPU or memory resources required to process the call load.

Call complexity

Call complexity is the number of each type of service used by a call.

Expected resource consumption

Over a period of time, you can use the average number of each type of service for each call to estimate the expected resource consumption. For example, if a typical call queues to an average of two skillsets, the expected resource cost for each call is two times the cost of queueing a call to one skillset (provided that the costs are a linear function of call rate).

Cost of call services

To estimate the resource consumption on Contact Center Manager Server for different call rates, you must define the cost of a basic call, as well as the costs associated with the most typical call operations.

The following conditions apply:

- The cost of a basic call is the resource consumption incurred due to basic call processing (assuming that the agent answers immediately).
- The default value for call rate is based on a holding time of three minutes.

The following table lists common call services and indicates the typical cost used for each call in the hybrid or typical call model for Avaya Communication Server 1000.

Table 15: Call service and cost per call

	Avaya Communication Server 1000 - AML
Parameter	Services for each call
Basic Call	1
Queue to Skillset	2
Queue to Agent	0
Give Controlled Broadcast (S/S)	1
Voice Services Collect Digits	0
Give IVR	1
Give RAN	2
Give Music	1
HDX Send Info	1
Voice Services Collect Digits	0
Give IVR	1
Give RAN	2
Give Music	1
HDX Send Info	1
HDX Request/Response	1
Intrinsics	5
If/Then's Executed	5
Proportion of Calls Transferred	5%
Proportion of Calls Conferenced	5%
Proportion of Calls Transferred to a DN	N/A
MLS Screen Pops	1.2
MLS Messages	0
Queue to Network Skillset	2

Call load table notes:

- The number of services for call is an average value taken over all inbound calls (or outbound calls, if that is the context).

Call rate

Call rate is the average rate of calls processed by the server. The call rate is measured in Calls Per Hour (CPH) and is a function of the average Call Arrival Rate and Mean Holding Time (MHT).

Mean Holding Time is the time the agent spends serving a call. MHT is the sum of:

- average talk time
- time required for post-call processing, when the agent is not available to handle other calls
- inter-call interval (including after call break time, if any)

Under heavy call loading, or during the busy time, when there is no agent idle time, Mean Holding Time is equal to Mean Time Between Calls (MTBC). (These definitions apply to both inbound and outbound calls.)

Call rate, number of active agents, and MHT are related. Given the same call rate, the more agents there are, the longer the MHT can be. For example, if the call rate is 60 CPH and only one agent is available, the MHT cannot be more than 1 minute. On the other hand, if there are 60 agents for the same call rate, then each agent can take up to an hour, on average, for a call.

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

Communication Control Toolkit capacity

The call capacity is 100 000 simple calls per hour (CPH) with data for a maximum of 5000 agents.

Agent counts are 5000 agents (5000 terminals, 10 000 addresses) if call data is not required or 1600 agents (1600 terminals, 3200 addresses) if call data is used. Self Service supports an additional 1000 IVR lines.

The performance of Communication Control Toolkit depends on a number of factors, including:

- number of resources (terminals, addresses, and users)

- number of clients
- number of calls per hour, call duration, and call complexity—transfers, conferencing, and attached caller-entered data all increase call complexity, and, therefore, the resources required to process a call
- amount of call-attached data (see the following section)
- hardware configuration (processor speed, memory, and disk space available)
- type of solution AACC Communication Control Toolkit and CCT-IVR
  - CCT-IVR is not supported co-resident with AACC

Call Attached Data considerations

Call attached data in Communication Control Toolkit uses one of three formats: binary, string, and key-value pairs. The string and key-value pair formats contain meta-data (the markup that describes their structure) when they are attached to TAPI as CallData. Because the size limit for TAPI call data is 4096 bytes, when these formats are used on systems that use the TAPI connector, the effective storage capacity of Call Data is reduced by the size of the meta-data.

The formatting meta-data overhead of string (Str) formatted data is 34 bytes, reducing the effective CallData storage capacity in TAPI to 4062 bytes (4061 characters plus the terminating null character).

The formatting meta-data overhead of the key-value pair (KVP) formatted data is 34 bytes for each key-value pair.

For example, for a 5-character key and a 5-character value, the actual data that is attached to TAPI is

34 (base formatting)

+ 16 (1 key-value pair)

+ 10 (the key and the value)

+ 1 (terminating null character)

= 61.

Adding a second similar key-value pair increases the number of bytes by 26 (16 for the key-value pair + 10 for the key and the value).

Attached data stored in the binary (bin) format is stored in TAPI CallData without formatting meta-data. The full 4096 bytes of TAPI CallData is used.

In SIP-enabled contact centers, Call Attached Data (CAD) is not available on the remote leg of a transfer or conference until the transfer or conference is complete.

CTI application performance impact

Meridian Link Services (MLS) can be used in a contact center environment. It is an intelligent signaling link offering computer-telephony integration (CTI) applications access to Avaya Communication Server 1000 call processing functions.

If you use MLS with Communication Control Toolkit, there is an impact on Contact Center Manager Server performance.

Access from an external client PC

When you use an external client PC to access Contact Center Manager Administration (CCMA) on a single server, Avaya recommends that you limit the number of on-demand and scheduled historical reports run on the co-resident server. Running historical reports can increase the CPU use on the server.

Access from a browser on the Contact Center Manager Server server

When you access Contact Center Manager Administration from a browser on the Contact Center Manager Server server, Avaya recommends that you limit the number of ad hoc and scheduled historical reports run on the single server. Running historical reports can increase the CPU use on the server.

In addition, Avaya recommends that you limit the number of real-time displays that you start. Viewing real-time displays also increases the CPU use on the server.

Landing Pads

The Avaya Aura® Contact Center Web Service Open Interfaces enable self-service systems and third-party applications to transfer a call into a 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 the contact center within 20 seconds.

Typically the time between a successful Landing Pad reservation and actual call arriving at the Landing Pad is between 2 and 4 seconds, depending on the call setup-time over your network.

If one call takes 4 seconds to setup, then the theoretical maximum for equally spaced calls is 900 calls per hour for each Landing Pad.

3600/4 = 900 calls per hour for each Landing Pad.

You must also consider the peak call rate and configure the number of Landing Pads in your Contact Center to handle the anticipated peak call rate. Avaya recommends that you configure one Landing Pad per simultaneous call: if you want to handle 70 simultaneous calls then configure at least 70 Landing Pads.

If the peak call rate increases above the capacity configured, calls are not lost, but your customers might experience delays in service.

Open Interfaces Web Service data limits

The Avaya Aura® Contact Center Open Interfaces Web Service enables self-service systems and third-party applications to transfer a call into a contact center by reserving a Landing Pad on the target contact center; it also allows custom data to be passed with the call. Avaya Aura® Contact Center script or flow applications also use the Open Interfaces Web Service to read, edit, and update call based User-to-User Information (UUI) data.

The Avaya Aura® Contact Center Open Interfaces Web Service supports 50 ASCII character maximum for User-to-User Information (UUI) access and editing.

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 18: Windows Server 2012 R2 common specifications

This section specifies the server requirements common to all Avaya Aura® Contact Center software installed on the Microsoft Windows Server 2012 R2 operating system.

The requirements in this section apply to the following Contact Center servers:

- Voice and Multimedia Contact Server with Avaya Aura® Media Server
- Voice and Multimedia Contact Server without Avaya Aura® Media Server
- Voice Contact Server Only
- Multimedia Contact Server Only
- Network Control Center Server Only

The requirements in this section apply to the Contact Center applications:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Network Control Center (NCC)
- Contact Center Manager Administration (CCMA)
- Contact Center Multimedia (CCMM)
- Contact Center Outbound
- Communication Control Toolkit (CCT)
- Orchestration Designer (OD)
- Avaya Aura® Media Server (coresident on Windows server)

You can install Contact Center applications and server types on servers that

- meet the minimum hardware specifications in this document
- meet the operating system and third-party software guidelines in this document
- meet the other guidelines in this document, for example the network and platform requirements

For information about the Avaya Aura® Media Server on Linux server requirements, see Avaya Aura Media Server on Linux configuration requirements on page 393.

Server naming requirements

Server names must adhere to RFC1123 (Requirements for Internet Hosts), which specifies that a host name must adhere to the following:

- Use only characters a to z, A to Z, and 0 to 9 can be used in a host name.
- You can use a hyphen (-), but not to start or end the host name.
- Host names must be 6 to 15 characters in length.
- Host names must not start with a number.
- Do not use the underscore character (_) and period character (.).
- Do not use spaces in the host name.

The Contact Center server must be able to resolve the host name or computer name of all other servers within the configuration. If you have a Domain Name Service (DNS) server, make sure an entry exists for each server. If you do not have a DNS server, manually update the HOSTS file on each server with the host name or computer name of all other servers to ensure that all clients can interpret the server names.

If network connectivity on your network requires the use of Fully Qualified Domain Names (FQDN), then the FQDN of each computer must be resolvable between all servers associated with Contact Center.

Common server disk partitioning requirements

The section describes the common Contact Center server hard disk drive partitioning requirements for Windows Server 2012 R2 servers. The type, number, and size of the disk drive partitions required depends on your solution type, agent count, and the size of your contact email attachments.

- Each Contact Center server must have the operating system on the C partition. Do not store Contact Center patches, trace logs, database backups, or email attachment folders on this partition.
- Avaya does not guarantee the support for future Windows Server 2012 R2 Server Service Packs, which might require more disk space. Avaya recommends that you create an operating system partition large enough to accommodate future Service Packs.
- Each Contact Center server must have an application partition, usually the D partition. Contact Center installs the component application software on this partition. Do not store database backups, trace log files, or other data on this partition.
- The Contact Center server DVD drive is typically assigned to the E partition letter.
- Each Contact Center server must have one or more database partitions. Do not store database backups, trace log files, or other data on the database partition.
- You can locate the operating system disk partition, the Contact Center application disk partition, and the Contact Center database partitions on the same physical hard disk drive, if

required, and if sufficient disk space is available. However, Avaya recommends that you locate the databases and the Contact Center applications on different hard disk drives for optimal system performance and reliability.

- The maximum size of the Contact Center Multimedia or Contact Center Manager Server database is limited to the size of the database disk partition. To increase the database partition size, use the Windows Server 2012 R2 Server Manager - Disk Management utility to extend the volume of the database partition. Increasing the database partition does not increase the overall Contact Center contact storage limits. Do not store database backups, trace log files, or other data on the database partition.

  Important:

  Increasing the CCMM database partition does not increase the overall contact storage limits in system.

- Partitioned sizes on all database drives must be in increments of 1 GB (equivalent to 1024 MB).

Table 16: Avaya Aura® Contact Center server disk partitioning requirements

Drive partition letter	Partition letter	Notes
Operating system partition	C:	NTFS partition on disk 0. This must be partitioned as the primary partition. The Windows Server 2012 Release 2 Server operating system is installed here.
Application partition	Typically D:	NTFS partition for Contact Center software.
DVD ROM drive	Typically E:	DVD ROM.
Database partition	Typically F:	NTFS partition for CacheTemp, Cache, ADMIN, PERFMON_STAT, CCMA, CCMS and CCT databases.
(Optional) Database partition	Typically G:	NTFS partition for CCMM database and multimedia attachments partition.
Database Journal partition	Typically H:	NTFS partition for database journal.

Operating system requirements

The following table provides the operating system compatibility for Avaya Aura® Contact Center.

Table 17: Avaya Aura® Contact Center operating system requirements

Operating system	International versions supported	Minimum service pack required
Windows Server 2012 Release 2, Standard Edition and Datacenter Edition	English French German Italian Dutch LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese Korean	

All nodes in an Avaya Aura® Contact Center networking deployment, including the Network Control Center server, must be installed on operating systems from the same language family. Contact Center Manager Administration does not support displaying names from two different languages families. For example, a single Contact Center Manager Administration does not support one node with a French operating system and another node with a Russian operating system.

Operating system installation and configuration

Contact Center Manager Server runs on the Windows components installed by default in Windows Server 2012 R2 with the following exceptions:

Important:

These exceptions apply to a stand-alone server only.

- The Simple Network Management Protocol (SNMP) service must be installed on your server. Installation enables you to use an SNMP management system for remote monitoring. This service is not installed by default, so you must select it when you install or configure the operating system.
- When Contact Center Manager Server is used in an Avaya Communication Server 1000 AML environment, you must disable all time synchronization features of the operating system to avoid potential call processing outages.

Do not install additional services on your server that are not installed by default or described in this document.

Microsoft security hotfixes

You must operate your server with the most current Microsoft patches.

- Review the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* (available from Technical Support website) for the list of applicable Microsoft security hotfixes to apply.
- Back up the entire server, and then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Avaya Security Advisories

Avaya Security Advisories are posted on the Avaya Security Support website at https://support.avaya.com/security. From the Avaya Support website, you can register to receive email notifications of Avaya Security Advisories.

The amount of time it takes to receive an Avaya Security Advisory varies depending on the vulnerability classification of the advisory. For more information about vulnerability classifications, responses, and maintenance policies, refer to the following documents:

- *Avaya's Product Security Vulnerability Response Policy*
- *Avaya's Security Vulnerability Classification*
- *Avaya's Maintenance Contract Requirements for Product Support*
- *Avaya Product Security Support Flow*

Operating system updates

Operating system updates includes service updates and service packs.

Service updates

Given the number of operating system security service updates and the complexity inherent in any network, create a systematic and accountable process for identifying and applying service updates. To help create such a process, you can follow a series of best practices guidelines, as documented in the National Institute of Standards and Technology (NIST) Special Bulletin 800-40, Procedures for Handling Security Patches.

This bulletin suggests that if an organization has no central group to coordinate the storage, evaluation, and chronicling of security service updates into a library, then system administrators or the contact center administrator must fulfill this role. In addition to these guidelines, whenever possible, follow Microsoft recommendations regarding newly discovered vulnerabilities and that you promptly install Microsoft security service updates.

Whenever possible, Avaya incorporates the most recent operating system security recommendations and service updates in an integrated solutions testing strategy during each test cycle. However, due to the urgent nature of security service updates when vulnerabilities are discovered follow Microsoft guidelines as they are issued, including any Microsoft installation procedures and security service update rollback processes.

Finally, you must perform a full system backup before you update the system to ensure that a rollback is possible, if required. If a Contact Center application does not function properly after you apply a Microsoft security service update, you must remove the service update and revert to the previous version of the application (from the backup you made before applying the service update).

For added security, always determine whether Avaya verified the Microsoft service update for compatibility with Contact Center Manager.

For more information about updating, see the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Compatibility List* on http://support.avaya.com.

Service packs

Avaya has a policy to implement co-residency testing of all new operating service packs for compatibility with the suite of Contact Center applications as soon as they are available. In practice, because a service pack can contain a significant amount of new content, Avaya requires that you wait until compatibility testing is complete before you apply the service pack. Note that operating system service packs are typically tested with the most recent Contact Center application SP and, therefore, an upgrade to a new service pack requires an upgrade to the most recent Avaya SP.

Before you upload a new service pack, you must perform a full system backup (for system rollback as in the updating scenario).

Important:

Service pack compatibility for all Contact Center applications is documented in the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* on the website at http://support.avaya.com.

Java Runtime Environment updates

Contact Center supports only specific versions of Java Runtime Environment (JRE). During installation, Contact Center disables JRE automatic updates on the contact center servers.

Important:

Updating to an unsupported version of JRE can cause the contact center to stop working and can require the reinstallation of the contact center server.

Dynamic Host Configuration Protocol support

Contact Center applications (CCMS, CCMA, CCT, CCMM, LM, and Avaya Aura® Media Server) do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Agent Desktop client computers support both DHCP and static IP addresses.

Network setup

Use the following sections to understand the requirements to configure your network.

Network configuration

All servers must connect to the Local Area Network (LAN) or Contact Center subnet. Third-party applications that interact with the servers also connect to this LAN.

The Contact Center Manager Server requires only a single NIC configuration to connect to the Contact Center subnet. In a single-NIC configuration, if the Contact Center connects to an Avaya Communication Server 1000 switch, the network must support layer 3 routing between the Contact Center subnet and the Avaya Communication Server 1000 switch ELAN. This allows AML messaging to pass between the Contact Center servers and the Avaya Communication Server 1000 switch.

Where an AML-based Contact Center connects to an Avaya Communication Server 1000 switch, it is also possible to configure a second NIC connected directly to the ELAN. Normally this accommodates legacy data networks awaiting design changes to support a single-NIC configuration. In such dual-NIC configurations, the network must prevent layer 3 routing between the Contact Center subnet and the Avaya Communication Server 1000 switch ELAN.

The single-NIC configuration is encouraged, because some Contact Center Manager Server releases and features (such as a SIP-enabled Contact Center) do not support a dual-NIC configuration.

The IP addresses used for the Primary and Secondary License Manager must be on the same Contact Center subnet and the Contact Center subnet must be first on the binding order on the Contact Center Manager Server and License Manager servers.

You require only one network interface card. However, if you have more than one network interface card, you must configure the binding order of the network interface cards so that the Contact Center subnet card is first, followed by the ELAN card, and finally the virtual adapters for remote access.

Domains and Windows Server security policies

Avaya recommends that you add the Avaya Aura® Contact Center servers to your domain.

If Contact Center Multimedia is a member of a domain, the agent's domain user name and password are used to authenticate access when the agent uses the attachment share locations. If you add the server to an existing customer network domain, you can add the server to the domain before or after you install Contact Center Multimedia. Typically the server is added to the domain before you install Contact Center Multimedia.

If Contact Center Multimedia is not part of a Windows domain, additional configuration is required. You can add Contact Center Multimedia as a member server and all agent network logon accounts to a domain. If Contact Center Multimedia is not a member of a domain, you must configure a local (windows) user name and password on the Multimedia server for each agent and the Network Administrator must provide the user name and password to the agent.

If Contact Center Multimedia is a member of a work group, then you must configure each agent with a local user name and password to allow authentication for access the shared drives. Each agent must be granted access rights to the shared folders on the drive.

Third-party software requirements

Due to the mission-critical, real-time processing that Contact Center applications perform, you must not install any other application class software on the server. You can install certain utility class software on the server, providing it conforms to the guidelines in this section.

Application class software generally requires a certain amount of system resources and must not be installed on a server running Contact Center applications. The installation of third-party applications can cause Contact Center applications to operate outside of the known engineering limits and can create potential unknown system problems (for example, CPU contentions, increased network traffic loading, and disk access degradations).

Certain third-party utility class software applications, such as hardware diagnostics or backup tools, generally require less system resources during the normal operation of Contact Center applications and are permitted. Exceptions are utilities such as screen savers, which can cause system problems and degrade performance.

Antivirus software is classified as a utility and is subject to the generic guidelines in the following section.

Generic guidelines for utility-class software applications

The following are generic guidelines for utility-class software:

- During run-time, the utility must not degrade the contact center application beyond an average percentage of CPU use (see each specific application section in this document for the recommended maximum CPU usage level). Furthermore, the utility must not lower the minimum amount of free hard disk space required by contact center application and the Windows Operating system.
- The utility must not cause improper software shutdowns or out-of-sequence shutdowns.
- The utility must not administer the contact center application.
- If the utility has a database, it must not affect the contact center application database.
- Disk compression utilities must not be used.
- Memory tweaking utilities used to reclaim memory that is unused by Microsoft must not be used.
- The installation or uninstallation of the third-party software must not impact or conflict with the contact center application (for example, it must not cause DLL conflicts). If such conflicts are discovered, a server rebuild might be necessary.
- The implementation personnel must perform tests to ensure these conditions and recommendations are met before you place the Contact Center application into production.

Support personnel can ask for the results of the testing during fault diagnosis. As part of fault diagnosis, the distributor or end user might be asked to remove third-party software.

- HyperTerminal must not be installed on the server as it interferes with the operation of Contact Center.

Additional guidelines for the use of antivirus software

Your security policies might require the installation of antivirus software on the application server.

Contact Center supports the following antivirus products:

- Symantec AntiVirus 12.x
- McAfee 8.8 Patch 3 or later

You can deploy antivirus products from other vendors subject to the following guidelines:

- Infected file quarantine policy on the server and client: antivirus software can be configured to clean up the detected virus automatically and files must be quarantined if infected files cannot be cleaned. Contact Avaya to verify whether the quarantine file is part of our product files or dependent system file. If a virus is detected, remove the server from the network immediately during virus eradication to prevent further virus propagation.
- Do not connect a contact center application platform directly to the Internet to download virus definitions or updated files. Furthermore, Avaya recommends that you do not use a contact center application client PC to connect to the Internet. Instead, download virus definitions and updated files to another location on the customer network and manually load them from this interim location onto the contact center application platform.
- Perform the previous steps to download Contact Center application service packs (SP). This method limits access to the Internet, and thus reduces the risk of downloading infected files.
- Scan all SP files, DVD-ROMs, and floppy disks before you upload or install to the server. This practice minimizes any exposure to infected files from outside sources.
- Capacity considerations: running virus scan software can place an additional load on a contact center application platform. The implementation personnel must run the performance monitor tool on the server to gauge CPU usage. If the antivirus software scan causes the platform average CPU usage to exceed the recommended percentage for longer than 20 minutes, the antivirus software must not be loaded onto the contact center application platform.
- Product Support do not provide support on the configuration of antivirus software, but offer guidance where possible. Direct questions or problems on antivirus software to the appropriate vendor.
- If performance or functionality issues are raised to Avaya support personnel as part of the fault diagnosis, you might be asked to remove third-party utility software or antivirus software.

Simple Network Management Protocol (SNMP) alerting on virus confirmation

Avaya Aura® Contact Center does not support this feature.

Remote support access tool

Avaya requires you to install an Avaya Secure Access Link (SAL) server to provide remote support. SAL is a remote-access architecture that provides simplified network management and increased security, reliability and flexibility. SAL gives you complete control of when and how Avaya, or any other service partner, can access your equipment.

You use the Remote Desktop Connection feature in Windows along with the SAL. Remote Desktop Connection is supported in console or admin mode only. Refer to the Microsoft website for details about how to verify that you are connected to the console/admin session (session 0).

Hardware requirements

The following sections describe the additional hardware requirements for all servers.

Redundant Array of Independent Disks (RAID)

Avaya Aura® Contact Center supports hardware RAID-1, RAID-5, and RAID-10. RAID technology provides disk data redundancy as well as error detection and correction. For maximum security and mission-critical solutions, Avaya mandates that all Contact Center servers contain a hardware RAID controller with battery backup. Hardware RAID-1, RAID-5, and RAID-10 are the only levels and types of RAID supported.

Avaya Aura® Contact Center does not support software RAID.

Storage Area Network (SAN)

A Storage Area Network (SAN) is a dedicated storage network that provides access to consolidated block level storage. SANs are used to make storage devices such as disk arrays, accessible to servers so that the devices appear as locally attached to the operating system.

When Avaya Aura® Contact Center is installed on a physical server it does not support a SAN. When Avaya Aura® Contact Center is installed on a virtual machine it supports a SAN.

Uninterruptible Power Supply

The use of an Uninterruptible Power Supply (UPS) with a server is permitted. A UPS provides the following benefits:

- Reduction in data loss—A UPS shuts down the server gracefully if an interruption in AC power occurs. A graceful shutdown prevents data corruption and reduces the risk of data loss.
- Reduction in power dips and spikes—The UPS regulates AC power supplied to the server.

Data backups running at the time of shutdown are unusable.

UPS requirements

The UPS must meet the following requirements:

- Provides at least 10 minutes of power to stop all services and shut down the server.
- Fits physically within the workplace.
- Affects environment minimally.
- Applies power to the server when line voltage reaches a stable state.
- Recharges before powering up the server if the server is down for a long time.
- Is compatible with the operating system running on the server.
- Meets all local regulatory requirements. For the European market, the UPS must generate a pure sine wave AC waveform.
- Has hot-swappable batteries. Replacement or capacity upgrades of the batteries must not interrupt service.
- Does not affect the Contact Center application software. UPS software must not replace software or drivers installed on the server with different versions. Install only the basic software functions necessary for UPS operation. Do not install advanced features as they can affect the Contact Center application software.
- If you install Smart UPS software on the server, it must conform to the guidelines in this document for third-party utilities. The UPS solution provider must perform the documentation, testing, and support of server shutdown and startup with UPS software.

Server performance and firmware settings

The Basic Input Output System (BIOS) of a server configures the hardware components and boots the operating system from a storage device. The server operating system (OS) then uses the BIOS to control the server hardware. You must configure the server BIOS settings to ensure optimum performance from the underlying server hardware. For most BIOS settings, you must choose between optimizing a server for power savings or for server performance. For real-time applications such as Avaya Aura® Contact Center, you must always choose the server BIOS settings that ensure the optimum performance from the underlying server hardware.

Server manufacturers provide their own motherboards, BIOS, hardware, and firmware. Determining the BIOS configuration for your server’s hardware can be challenging. There are several BIOS

settings that can significantly impact the system performance. When optimizing for system performance, you must select the BIOS settings that enhance the system performance over those that contribute to power savings. Other BIOS settings and recommendations are not as straight forward. Start by consulting the manufacturer's technical data for your server. Avaya recommends that you then test your solution in order to make the best BIOS configuration decisions.

Configure the server hardware, firmware, and Operating System settings to select system performance over power savings.

Server firmware

Firmware is a computer program that is stored on the server motherboard or on an add-on hardware controller. The firmware stored on the server motherboard is called the Basic Input Output System (BIOS). The BIOS is responsible for the behavior of the system when it is first switched on and for passing control of the server to the operating system. Firmware is also stored in hardware components such as Redundant Array of Independent Disks (RAID) controllers.

Routinely consult the manufacturer's technical data for your servers and, where appropriate, apply the most recent BIOS and firmware updates. The steps required to update firmware or a system BIOS vary depending on the hardware vendor and the component to be updated. Typically, the manufacturer supplies a firmware updating utility. Keeping your server BIOS and firmware at a supported level can improve reliability, serviceability, and help ensure optimum performance.

Unified Extensible Firmware Interface

The Unified Extensible Firmware Interface (UEFI) specification defines the interface between the operating system and the server firmware. Similar to the BIOS, UEFI is installed by the server manufacturer and it is the first program to run when the server is turned on. UEFI firmware provides some technical advantages over the traditional BIOS system.

Contact Center software, when deployed on physical servers, supports UEFI.

Contact Center software, when deployed on VMware virtual machines, does not support UEFI.

Contact Center does not support the UEFI Secure Boot feature.

Select the firmware boot option, BIOS or UEFI, on the server before installing the Windows Server 2012 R2 Operating System and the Contact Center software. Refer to your hardware vendor's documentation on how to change and implement the required firmware boot option. Changing the firmware boot option after the Operating System has been installed renders the server unbootable and this is not supported.

Power and performance management

For real-time applications such as Avaya Aura® Contact Center, you must always select the hardware, BIOS, firmware, and Operating System settings that enhance the system performance over those that contribute to power savings.

Intel Xeon CPUs offer two main power management options: C-states and Intel Turbo Boost.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to full power on.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power.

These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described below. Other server makes and models can have other terminology but equivalent BIOS settings.

The following are the recommended BIOS settings for the Dell PowerEdge servers:

- Set the Power Management Mode to Maximum Performance.
- Set the CPU Power and Performance Management Mode to Maximum Performance.
- Processor Settings: set Turbo Mode to enabled
- Processor Settings: set C States to disabled

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to Static High Mode.
- Disable Processor C-State Support
- Disable Processor C1E Support
- Disable QPI Power Management
- Enable Intel Turbo Boost

Configure the server hardware, firmware, and Operating System settings to select system performance over power savings.

Disk caching and RAID

Hard disk drives use cache memory to improve read and write access to the disk drives. In write-back mode caching, the disk or RAID controller writes data from the server to cache memory and acknowledges write completion to the server. The server is free to perform other tasks while the disk controller transfers the data from the write cache to the disk drives. This approach significantly increases write performance.

Avaya Aura® Contact Center supports hardware RAID-1, RAID-5, and RAID-10. RAID technology provides disk data redundancy as well as error detection and correction. For maximum security and mission-critical solutions, Avaya mandates that all Contact Center servers contain a hardware RAID

controller with battery backup. Hardware RAID-1, RAID-5, and RAID-10 are the only levels and types of RAID supported.

Read the hardware documentation for your server to determine how to configure disk caching. Typically, disk caching can be configured as a BIOS setting, a RAID setting, a RAID controller setting, or as an Operating System setting. Some RAID controllers expose the ability to manipulate the Caching Policy through the OS and therefore the OS level setting can override the BIOS level setting. Refer to your hardware documentation for more information about configuring disk caching. Avaya Aura® Contact Center does not support Operating System level disk caching, software disk caching, or software RAID. Avaya Aura® Contact Center requires battery backed hardware RAID caching to avoid data loss and possible database corruption on power outage.

Non-Uniform Memory Architecture (NUMA) and memory

Non-uniform memory access (NUMA) is a computer memory design used in multiprocessing, where the memory access time depends on the memory location relative to the processor. Using NUMA, a processor can access its own local memory faster than non-local memory (memory local to another processor or memory shared between processors). For Avaya Aura® Contact Center, the server must support and implement NUMA.

In the server BIOS settings, configure the memory operating mode for performance optimization and disable Node Interleaving. For example, for a Dell server configure “Memory Operating Mode” as “Optimizer Mode”, and configure “Node Interleaving” as “Disabled”. Refer to your hardware documentation for more information about NUMA and memory performance.

Performance management and VMware

For VMware host servers, to allow the VMware kernel to control CPU power saving while maximizing server performance when required, it is possible to set power management in the BIOS to “OS Control Mode”. The VMware hypervisor can then provide balanced performance and power management. This BIOS setting and VMware feature combination does not meet the real-time performance requirements of Avaya Aura® Contact Center. Avaya Aura® Contact Center does not support the BIOS “OS Control Mode” settings or its equivalents.

Virtualization technology

When virtualization technology is enabled, the BIOS enables processor virtualization features and provides virtualization support to the operating system through the DMAR table. In general, only virtualized environments such as VMware take advantage of these features.

For VMware host servers, enable all available Virtualization Technology options in the hardware BIOS. Enable Intel virtualization (VT-x) and if available enable Extended Page Tables (EPT).

The available virtualization settings vary by hardware provider and BIOS version. Read your hardware provider's documents covering virtualization support to determine which settings to configure.

Hyper-Threading

Hyper-Threading refers to Intel’s proprietary technology for increasing parallel computational power (processor multi-tasking) by allowing the operating system (OS) to see and address each physical processor core as if it were two virtual processors. It also enables the OS and applications to share work between those virtual processors whenever possible, thereby making full use of the available resources.

Enable Hyper-Threading on the Avaya Aura® Contact Center servers.

Unused hardware devices

On the server, disconnect or disable unused and unnecessary physical hardware devices such as: COM ports, LPT ports, USB controllers, Network interfaces, and Storage controllers. You must retain some USB devices for the mouse and keyboard. Disabling unnecessary hardware devices improves server performance and security. Consult the manufacturer’s technical data for your servers for information about disabling unused hardware devices in the BIOS.

Summary

For real-time applications such as Avaya Aura® Contact Center, choose server BIOS settings that optimize for performance in preference to power savings. Start by consulting the manufacturer’s technical data for your server. Avaya recommends that you then test your solution in order to make the best BIOS configuration decisions. Avaya recommends that you enable CPU Hyper-Threading. By enabling BIOS options such as CPU Prefetchers and CPU Hyper-Threading, the system performance can be improved effectively. When tuning system BIOS settings for performance, you must consider the various processor and memory options. Experiment with other options to find the optimum setting for your specific hardware and Contact Center solution.

Configure the server hardware, BIOS, firmware, and Operating System settings to select system performance over power savings.

Chapter 19: Physical server specifications

This section specifies Avaya Aura® Contact Center software deployments on physical servers. This section describes sample Avaya Aura® Contact Center solutions and the physical server specifications for each sample solution. The sample solutions are based on agent count and call flow rates.

Avaya Aura® Contact Center supports Platform Vendor Independence (PVI). This provides the flexibility to purchase a hardware specification that conforms to your corporate standard. A further benefit is that you need not seek approval for hardware that does not comply with your corporate specification.

The sample Avaya Aura® Contact Center solutions, with a minimum PVI server specification for each level, are as follows:

- Entry-level solution on page 263
- Mid-range solution on page 267
- High-end solution on page 272

For information about achieving the maximum performance from your physical server hardware, see Server performance and firmware settings on page 256.

Physical Server supported configurations

The following table summarizes the supported Avaya Aura® Contact Center deployments for each server type. The table shows which server specification each Avaya Aura® Contact Center server type requires when installed on a physical server.

Table 18: Supported server specifications for each physical server type

Server type	Voice PABX	Entry-level server	Mid-range server	High-end server
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	No	Yes	Yes
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	No	Yes	Yes
	CS 1000 AML	No	Yes	Yes
Voice Contact Server Only	Aura SIP	Yes	Yes	Yes
	CS 1000 AML	Yes	Yes	Yes
Multimedia Contact Server Only	Aura SIP	Yes	Yes	Yes
	CS 1000 AML	Yes	Yes	Yes
Multimedia Contact Server Only – Enterprise Web Chat	Aura SIP	No	Yes	Yes
Network Control Center Server	N/A	Yes	Yes	Yes
Avaya Aura® Media Server standalone on Linux	Aura SIP	No	Yes	Yes

SIP-enabled Avaya Aura® Contact Center requires one or more Avaya Aura® Media Server for media processing. Avaya Aura® Contact Center uses Avaya WebLM for license management.

AML-based Avaya Aura® Contact Center does not require or use Avaya Aura® Media Server or Avaya WebLM.

Entry-level solution

The following table lists the installation options, maximum number of agents, and maximum call rates of an entry-level Avaya Aura® Contact Center solution.

If your contact center requires more agents or a higher call rate than shown here, refer to the mid-range or high-end server specifications.

Server type	Voice platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/ Eph) Note 2
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
	CS 1000 AML	Not Supported	Not Supported	N/A	N/A
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
Voice Contact Server Only	Aura SIP	300 Note 3	100	6K	500 / 800
	CS 1000 AML	300	100	6K	500 / 800
Multimedia Contact Server Only	Aura SIP	1000	N/A	N/A	2.0K / 4.0K
	CS 1000 AML	1000	N/A	N/A	2.0K / 4.0K
Multimedia Contact Server Only with Enterprise Web Chat	Aura SIP	Not Supported	Not Supported	N/A	N/A
Network Control Center Server	All switch types	Supported	400	N/A	N/A

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

- For System Contact Rate calculations, IM contacts have a weighting equivalent to one system contact. One IM contact is equivalent to one system contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, Web chat contacts count as two system contacts. One Web chat is equivalent to two system contacts.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + (Web Chat * 2))
- Route to CDN and Transfer/Conference to CDN each count as two calls.

Note 2: Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Web chats per hour (WCph). Standard Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes.

Note 3: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on an entry-level server Avaya Aura® Contact Center supports 150 Agent Desktops and 150 Agent Browser applications.

Server type	Voice platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/ Eph) Note 2
Note: Avaya Aura® Contact Center High Availability is not supported on an entry-level server. **Note:** To achieve the stated capacities, configure your sever hardware for maximum performance. For more information, see Server performance and firmware settings on page 256. **Note:** You can use the instance of CCMA on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.					

Entry-level server specification

The following table lists the minimum specifications for an Avaya Aura® Contact Center server in an entry-level solution. These are the minimum specifications for Avaya Aura® Contact Center Release 7.0 for the entry-level server in order to support the rated capacities.

Specification	Configuration	Comment
CPU	Intel Xeon X5687 3.60 GHz	You must select a CPU that exceeds the benchmark rating for the Intel Xeon X5687 3.60 GHz CPU. Relative benchmark comparisons only apply for CPUs with the same number of cores. You can make CPU comparisons by viewing the benchmarked CPU passmark rankings here: http://www.cpubenchmark.net • AMD processors are not supported • CPUs based on more than 12 cores are not supported.
CPU - Minimum Clock Speed	2400 MHz	CPU clock speed must meet or exceed the minimum clock speed of 2400 MHz.
CPU - Required Technologies	Hyper-Threading	• 1 x additional logical core for each physical core. • Hyper-Threading must be enabled.
RAM	16 GB	For maximum performance, Avaya recommends that all DIMM slots are populated.
Windows Server 2012 R2 Operating System partition (C:)	80 GB NTFS	• System Reserved (350 MB) and C: (OS partition - 80 GB NTFS) • Minimum Operating System partition size.
Application partition (D:)	120 GB NTFS	Avaya Aura® Contact Center application partition
Voice database partition (F:)	200 GB NTFS	Required for the following server types: • Voice Contact Server • Network Control Center Server
Multimedia database partition (G:)	• 300 GB NTFS • 600 GB NTFS recommended	Required for the following server types: • Multimedia Contact Server Avaya recommends a 600 GB multimedia partition to support longer offline data retention.
Database journal partition (H:)	100 GB NTFS	Required for the following server types: • Voice Contact Server • Network Control Center Server • Multimedia Contact Server

Specification	Configuration	Comment
Partition size requirement (GB)	• 501 GB for voice only • 501 GB for NCC • 601 GB for multimedia only • 901 GB for multimedia only	• 501 GB NTFS for Voice Contact Server • 501 GB NTFS for Network Control Center (NCC) • 601 GB NTFS for Multimedia Contact Server with 300 GB NTFS multimedia database • 901 GB NTFS for Multimedia Contact Server with recommended 600 GB NTFS multimedia database .
Disk type and speed	SATA, SAS, Minimum 10000 RPM	• Avaya recommends using 15000 RPM disks. • Solid State Drives (SSDs) are not supported.
Minimum physical Disk Capacity (GB)	• 600 GB for Voice Contact Server • 600 GB for NCC • 900 GB for Multimedia Contact Server • 1.2 TB for Multimedia Contact Server	Minimum physical disk capacity to support the different server types. • 600 GB for Voice Contact Server • 600 GB for Network Control Center (NCC) • 900 GB for Multimedia Contact Server with 300 GB NTFS multimedia database • 1.2 TB for Multimedia Contact Server with recommended 600 GB NTFS multimedia database
RAID	RAID 1, RAID 5, or RAID 10	• Requires duplicate drives with identical specifications. • Battery backed hardware RAID controller with 512 MB cache minimum.
DVD Drive (E:)	One dual-layer DVD drive	• 16X or faster recommended. • DVD/Blu-Ray combo drives supported.
Network Interface	Dual 1Gbps or faster	Only Ethernet supported.

Note:

For information about achieving the maximum performance from your server hardware, see Server performance and firmware settings on page 256.

For servers operating at 50% or above the rated capacity figures for the server type, Avaya recommends that you use a physical database disk drive, separate from the Contact Center application and Operating System disk drives. Variations are allowed for the Windows and Application partitions providing there is sufficient capacity to prevent excessive disk fragmentation.

Mid-range solution

The following table lists the installation options, maximum number of agents, and maximum call rates of a mid-range Avaya Aura® Contact Center solution.

If your contact center requires more agents or a higher call rate than shown here, refer to the high-end server specifications.

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	300 Note 3	60	6K	0.8K / 1.2K
	CS 1000 AML	500	100	10K	0.8K / 1.2K
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	200 Note 3	40	4K	300 / 600
Voice Contact Server Only	Aura SIP	1500 Note 3	300	30K	4.0K / 8.0K
	CS 1000 AML	3000	400	60K	4.0K / 8.0K
Multimedia Contact Server Only	Aura SIP	2000	N/A	N/A	4.0K / 8.0K
	CS 1000 AML	2000	N/A	N/A	4.0K / 8.0K
Multimedia Contact Server Only with Enterprise Web Chat	Aura SIP	2000	N/A	N/A	12K / 8.0K
Network Control Center Server	All switch types	Supported	600	N/A	N/A

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

- For System Contact Rate calculations, IM contacts have a weighting equivalent to one system contact. One IM contact is equivalent to one system contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, standard Web chat contacts count as two system contacts. One standard Web chat is equivalent to two system contacts.
- For System Contact Rate calculations with standard Web Chat, the total maximum number of supported contacts per hour = (Voice + IM + Email + (standard Web Chat * 2)).
- For System Contact Rate calculations, Enterprise Web Chat contacts count as one system contact. One Enterprise Web Chat is equivalent to one system contact.
- For System Contact Rate calculations with Enterprise Web Chat, the total maximum number of supported contacts per hour = (Voice + IM + Email + Enterprise Web Chat).
- The maximum system contact rate is reduced if Work Force Optimization is part of the solution. For more details see the Workforce Optimization Distributor Technical Reference on https://support.avaya.com.

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
• *Route to CDN* and *Transfer/Conference to CDN* each count as two calls. **Note 2:** Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Web chats per hour (WCph). Standard Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes. Enterprise Web Chat supports up to 3000 concurrent sessions. **Note 3**: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on a mid-range Voice Contact Server, Avaya Aura® Contact Center supports 750 Agent Desktops and 750 Agent Browser applications. **Note:** Reduce capacity by 35 percent if you are recording all calls. Reduce by (the percentage of calls being recorded) X (35 percent) if you are using sampled recording. **Note:** Avaya Aura® Contact Center High Availability is supported on mid-range servers. **Note:** To achieve the stated capacities, configure your sever hardware for maximum performance. For more information, see Server performance and firmware settings on page 256. **Note:** You can use the instance of CCMA on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.					

Avaya Aura® Media Server standalone on mid-range physical server

The following table lists the maximum number of agents supported by Avaya Aura® Media Server on a mid-range physical server.

Operating System	No Avaya Call Recording (ACR)	Avaya Call Recording (ACR) enabled
Linux	500 maximum agents	325 maximum agents

Avaya Aura® Media Server is rated on supported sessions. The agent count is modelled on simple call offer and answer to agent plus 50% calls in queue. To estimate the supported agent counts for Avaya Aura® Media Server deployments, use 2.5 sessions per agent. To support more agent sessions, add additional Avaya Aura® Media Server servers to your solution, or refer to the high-end server specifications.

Avaya Aura® Media Server on a mid-range physical server supports High Availability.

Mid-range server specification

The following table lists the minimum specifications for an Avaya Aura® Contact Center server for a mid-range solution. These are the minimum specifications for Avaya Aura® Contact Center Release 7.0 for the mid-range server in order to support the rated capacities for the mid-range server type

Specification	Configuration	Comment
CPU	Dual 6–core Intel Xeon X5660 2.80 GHz	You must select a CPU that exceeds the benchmark rating for the Dual 6–core Intel Xeon X5660 2.80 GHz Relative benchmark comparisons only apply for CPUs with the same number of cores. You can make CPU comparisons by viewing the benchmarked CPU passmark rankings here: http://www.cpubenchmark.net • AMD processors are not supported • CPUs based on more than 12 cores are not supported.
CPU - Minimum Clock Speed	2400 MHz	CPU clock speed must meet or exceed the minimum clock speed of 2400 MHz.
CPU - Required Technologies	Hyper-Threading	• 1 x additional logical core for each physical core. • Hyper-Threading must be enabled.
RAM	32 GB	For maximum performance, Avaya recommends that all DIMM slots are populated.
Windows Server 2012 R2 Operating System partition (C:)	80 GB NTFS	• System Reserved (350 MB) and C: (OS partition - 80 GB NTFS) • Minimum Operating System partition size.
Red Hat Enterprise Linux 6.6 - 64–bit System partition	80 GB	When installing Avaya Aura® Media Server software on a Linux server, Avaya Aura® Media Server requires a single flat hard disk partition with a minimum of 80 GB.
Application partition (D:)	120 GB NTFS	Avaya Aura® Contact Center application partition
Voice database partition (F:)	200 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server • Voice Contact Server • Network Control Center Server
Multimedia database partition (G:)	• 300 GB NTFS • 600 GB NTFS recommended	Required for the following server types: • Voice and Multimedia Contact Server • Multimedia Contact Server Avaya recommends a 600 GB multimedia partition to support longer offline data retention.

Specification	Configuration	Comment
Database journal partition (H:)	100 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server • Voice Contact Server • Multimedia Contact Server • Network Control Center Server
Disk Type and Speed	SAS, Minimum 10000 RPM	• Avaya recommends using 15000 RPM disks. • For Avaya Aura® Media Server, the minimum disk speed is 15000 RPM. • Solid State Drives (SSDs) are not supported.
Partition size requirement (GB)	• 80 GB • 501 GB for voice only • 501 GB for NCC • 601 GB for multimedia only • 901 GB for multimedia only • 801 GB for voice and multimedia • 1101 GB for voice and multimedia	• 80 GB for Avaya Aura® Media Server on Linux • 501 GB NTFS for Voice Contact Server • 501 GB NTFS for Network Control Center (NCC) • 601 GB NTFS for Multimedia Contact Server with 300 GB NTFS multimedia database • 901 GB NTFS for Multimedia Contact Server with recommended 600 GB NTFS multimedia database • 801 GB NTFS for Voice and Multimedia Contact Server with 300 GB NTFS multimedia database • 1101 GB NTFS for Voice and Multimedia Contact Server with recommended 600 GB NTFS multimedia database
Minimum physical Disk Capacity (GB)	• 146 GB • 600 GB for Voice Contact Server • 600 GB for NCC • 900 GB for Multimedia Contact Server • 1.2 TB for Multimedia Contact Server • 900 GB for Voice and Multimedia Contact Server • 1.2 TB for Voice and Multimedia Contact Server	Minimum physical disk capacity to support the different server types. • 146 GB 15000 RPM for Avaya Aura® Media Server standalone on Linux • 600 GB for Voice Contact Server • 600 GB for Network Control Center (NCC) • 900 GB for Multimedia Contact Server with 300 GB NTFS multimedia database • 1.2 TB for Multimedia Contact Server with recommended 600 GB NTFS multimedia database • 900 GB for Voice and Multimedia Contact Server with 300 GB NTFS multimedia database • 1.2 TB for Voice and Multimedia Contact Server with recommended 600 GB NTFS multimedia database
RAID	RAID 1, RAID 5, or RAID 10	• Requires duplicate drives with identical specifications. • Battery backed hardware RAID controller with 512 MB cache minimum.
DVD Drive (E:)	One dual-layer DVD drive	• 16X or faster recommended.

Specification	Configuration	Comment
		• DVD/Blu-Ray combo drives supported.
Network Interface	Dual 1Gbps or faster	• Only Ethernet supported. • Avaya recommends Quad 1Gbps or faster. • Avaya Aura® Media Server configurations require support for Receive Side Scaling (RSS) with a minimum of 4 queues and minimum Receive Buffer size of 500

Note:

For information about achieving the maximum performance from your server hardware, see Server performance and firmware settings on page 256.

For servers operating at 50% or above the rated capacity figures for the server type, Avaya recommends that you use a physical database disk drive, separate from the Contact Center application and Operating System disk drives. Variations are allowed for the Windows and Application partitions providing there is sufficient capacity to prevent excessive disk fragmentation.

For Avaya Aura® Contact Center High Availability (HA) configurations, the active, standby, and optional Remote Geographic Node servers must have identical configurations, including disk partition names and sizes. For new installations, the active, standby, and Remote Geographic Node servers must have identical hardware specifications. When adding HA functionality to an existing non-HA solution, the standby Avaya Aura® Contact Center server hardware specification must be equal to or greater than the existing active server hardware specification. When adding a Remote Geographic Node (RGN) to an existing campus HA solution, the RGN server hardware specification must be equal to or greater than the existing active server hardware specification. If you are replacing a faulty standby or RGN server, the replacement server hardware specification must be equal to or greater than the existing active Avaya Aura® Contact Center server hardware specification.

High-end solution

The following table lists the installation options, maximum number of agents, and maximum call rates of a high-end Avaya Aura® Contact Center solution.

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	600 Note 3	100	12K	1.2K / 2.4K
	CS 1000 AML	1000	200	20K	1.2K / 2.4K
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	400 Note 3	80	8K	600 / 1200
Voice Contact Server Only	Aura SIP	3000 Note 3	600	45K	6.0K / 12K
	CS 1000 AML	5000	600	100K	6.0K / 12K
Multimedia Contact Server Only	Aura SIP	3000	N/A	N/A	6.0K / 12K
	CS 1000 AML	3000	N/A	N/A	6.0K / 12K
Multimedia Contact Server Only with Enterprise Web Chat	Aura SIP	3000	N/A	N/A	18K / 12K
Network Control Center Server	All switch types	Supported	600	N/A	N/A

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

- For System Contact Rate calculations, IM contacts have a weighting equivalent to one system contact. One IM contact is equivalent to one system contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, standard Web chat contacts count as two system contacts. One standard Web chat is equivalent to two system contacts.
- For System Contact Rate calculations with standard Web Chat, the total maximum number of supported contacts per hour = (Voice + IM + Email + (standard Web Chat * 2)).
- For System Contact Rate calculations, Enterprise Web Chat contacts count as one system contact. One Enterprise Web Chat is equivalent to one system contact.
- For System Contact Rate calculations with Enterprise Web Chat, the total maximum number of supported contacts per hour = (Voice + IM + Email + Enterprise Web Chat).
- The maximum system contact rate is reduced if Work Force Optimization is part of the solution. For more details see the Workforce Optimization Distributor Technical Reference on https://support.avaya.com.
- *Route to CDN* and *Transfer/Conference to CDN* each count as two calls.

Note 2: Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Standard Web chats per hour (WCph). Web chat capacity is based

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes. Enterprise Web Chat supports up to 3000 concurrent sessions. **Note 3**: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on a high-end Voice Contact Server, Avaya Aura® Contact Center supports 1500 Agent Desktops and 1500 Agent Browser applications. **Note:** Reduce capacity by 35 percent if you are recording all calls. Reduce by (the percentage of calls being recorded) X (35 percent) if you are using sampled recording. **Note:** Avaya Aura® Contact Center High Availability is supported on high-end servers. **Note:** To achieve the stated capacities, configure your sever hardware for maximum performance. For more information, see Server performance and firmware settings on page 256. **Note:** You can use the instance of CCMA on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.					

Avaya Aura® Media Server standalone on high-end physical server

The following table lists the maximum number of agents supported by Avaya Aura® Media Server on a high-end physical server.

Operating System	No Avaya Call Recording (ACR)	Avaya Call Recording (ACR) enabled
Linux	1000 maximum agents	650 maximum agents

Avaya Aura® Media Server is rated on supported sessions. The agent count is modelled on simple call offer and answer to agent plus 50% calls in queue. To estimate the supported agent counts for Avaya Aura® Media Server deployments, use 2.5 sessions per agent. To support more agent sessions, add additional Avaya Aura® Media Server servers to your solution.

Avaya Aura® Media Server on a high-end physical server supports High Availability.

High-end server specification

The following table lists the minimum specifications for an Avaya Aura® Contact Center High-end solution. These are the minimum specifications for Avaya Aura® Contact Center Release 7.0 for the high-end server in order to support the rated capacities for the high-end server type.

Specification	Configuration	Comment
CPU	Dual 8–core Intel Xeon E5-2670 2.60 GHz	You must select a CPU that exceeds the benchmark rating for the Dual 8–core Intel Xeon E5-2670 2.60 GHz Relative benchmark comparisons only apply for CPUs with the same number of cores. You can make CPU comparisons by viewing the benchmarked CPU passmark rankings here: http://www.cpubenchmark.net • AMD processors are not supported • CPUs based on more than 12 cores are not supported.
CPU - Minimum Clock Speed	2400 MHz	CPU clock speed must meet or exceed the minimum clock speed of 2400 MHz.
CPU - Required Technologies	Hyper-Threading	• 1 x additional logical core for each physical core. • Hyper-Threading must be enabled.
RAM	32 GB	For maximum performance, Avaya recommends that all DIMM slots are populated.
Windows Server 2012 R2 Operating System partition (C:)	80 GB NTFS	• System Reserved (350 MB) and C: (OS partition - 80 GB NTFS) • Minimum Operating System partition size.
Red Hat Enterprise Linux 6.6 - 64 bit System partition	80 GB	When installing Avaya Aura® Media Server software on a Linux server, Avaya Aura® Media Server requires a single flat hard disk partition with a minimum of 80 GB.
Application partition (D:)	120 GB NTFS	Avaya Aura® Contact Center application partition
Voice database partition (F:)	200 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server • Voice Contact Server • Network Control Center Server
Multimedia database partition (G:)	• 300 GB NTFS • 600 GB NTFS recommended	Required for the following server types: • Voice and Multimedia Contact Server • Multimedia Contact Server Avaya recommends a 600 GB multimedia partition to support longer offline data retention.

Specification	Configuration	Comment
Database journal partition (H:)	100 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server • Voice Contact Server • Multimedia Contact Server • Network Control Center Server
Disk Type and Speed	SAS, Minimum 10000 RPM	• Avaya recommends using 15000 RPM disks. • For Avaya Aura® Media Server, the minimum disk speed is 15000 RPM. • 15000 RPM disks required for High-End servers with workloads exceeding 50% of rated capacity. • Solid State Drives (SSDs) are not supported.
Partition size requirement (GB)	• 80 GB • 501 GB for voice only • 501 GB for NCC • 601 GB for multimedia only • 901 GB for multimedia only • 801 GB for voice and multimedia • 1101 GB for voice and multimedia	• 80 GB for Avaya Aura® Media Server on Linux • 501 GB NTFS for Voice Contact Server • 501 GB NTFS for Network Control Center (NCC) • 601 GB NTFS for Multimedia Contact Server with 300 GB NTFS multimedia database • 901 GB NTFS for Multimedia Contact Server with recommended 600 GB NTFS multimedia database • 801 GB NTFS for Voice and Multimedia Contact Server with 300 GB NTFS multimedia database • 1101 GB NTFS for Voice and Multimedia Contact Server with recommended 600 GB NTFS multimedia database
Minimum physical Disk Capacity (GB)	• 146 GB • 600 GB for Voice Contact Server • 600 GB for NCC • 900 GB for Multimedia Contact Server • 1.2 TB for Multimedia Contact Server • 900 GB for Voice and Multimedia Contact Server • 1.2 TB for Voice and Multimedia Contact Server	Minimum physical disk capacity to support the different server types. • 80 GB 15000 RPM for Avaya Aura® Media Server standalone on Linux • 600 GB for Voice Contact Server • 600 GB for Network Control Center (NCC) • 900 GB for Multimedia Contact Server with 300 GB NTFS multimedia database • 1.2 TB for Multimedia Contact Server with recommended 600 GB NTFS multimedia database • 900 GB for Voice and Multimedia Contact Server with 300 GB NTFS multimedia database • 1.2 TB for Voice and Multimedia Contact Server with recommended 600 GB NTFS multimedia database
RAID	RAID 1, RAID 5, or RAID 10	• Requires duplicate drives with identical specifications.

Specification	Configuration	Comment
		• Battery backed hardware RAID controller with 512 MB cache minimum.
DVD Drive (E:)	One dual-layer DVD drive	• 16X or faster recommended. • DVD/Blu-Ray combo drives supported.
Network Interface	Dual 1Gbps or faster	• Only Ethernet supported. • Avaya recommends Quad 1Gbps or faster. • Avaya Aura® Media Server configurations require support for Receive Side Scaling (RSS) with a minimum of 4 queues and minimum Receive Buffer size of 500.

Note:

For information about achieving the maximum performance from your server hardware, see Server performance and firmware settings on page 256.

For servers operating at 50% or above the rated capacity figures for the server type, Avaya recommends that you use a physical database disk drive, separate from the Contact Center application and Operating System disk drives. Variations are allowed for the Windows and Application partitions providing there is sufficient capacity to prevent excessive disk fragmentation.

For Avaya Aura® Contact Center High Availability (HA) configurations, the active, standby, and optional Remote Geographic Node servers must have identical configurations, including disk partition names and sizes. For new installations, the active, standby, and Remote Geographic Node servers must have identical hardware specifications. When adding HA functionality to an existing non-HA solution, the standby Avaya Aura® Contact Center server hardware specification must be equal to or greater than the existing active server hardware specification. When adding a Remote Geographic Node (RGN) to an existing campus HA solution, the RGN server hardware specification must be equal to or greater than the existing active server hardware specification. If you are replacing a faulty standby or RGN server, the replacement server hardware specification must be equal to or greater than the existing active Avaya Aura® Contact Center server hardware specification.

Chapter 20: VMware virtualization support

Avaya Aura® Contact Center supports server virtualization using VMware. In a virtualized environment, a single physical computer runs software that abstracts the physical computer's resources so that they can be shared between multiple virtual computers. In virtualization, the term host server refers to the actual physical hardware server on which the virtualization takes place. The virtualized servers on the host server are called virtual machines.

This section provides information about engineering and commissioning Avaya Aura® Contact Center using virtualization.

The benefits of using virtualization include the following:

- Decrease hardware, power, and cooling costs by running multiple operating systems on the same physical server.
- Lower management overhead costs by reducing the hardware footprint in the contact center.
- Guarantee high levels of performance for the most resource-intensive applications.
- Consolidate hardware resources with a production-proven and secure server virtualization platform.

Avaya Aura® Contact Center supports the following virtualization environments:

- ESXi 5.0 Update 2
- ESXi 5.1
- ESXi 5.5
- ESXi 6.0
- ESXi 6.5

Note:

VMFS 5.54 or later is required for all supported versions of ESXi.

Using virtualization in a contact center enterprise solution requires careful up-front planning, engineering, and implementation. While the technical and business advantages are clear, virtualization imposes extra considerations when designing the contact center solution architecture. Virtualization supports security and fault isolation. Environmental isolation allows multiple operating systems to run on the same machine. While virtualization offers these forms of isolation, virtualization environments do not provide performance isolation. The behavior of one virtual machine can adversely affect the performance of another virtual machine on the same host. Most modern virtualization environments provide mechanisms that you can use to detect and reduce

performance interference. You must carefully engineer your virtualized contact center solution to avoid performance interference.

If you plan to install non-Avaya Aura® Contact Center software applications on the other virtual machine of a host server with Contact Center installed, you must carefully analyze the impact of these applications on the contact center solution and provide extra performance isolation to safeguard Contact Center functionality.

Deploy Avaya Aura® Contact Center on an enterprise-grade virtual environment with the most recent hardware that supports hardware-assisted virtualization. Avaya recommends that you apply virtualization planning, engineering, and deployment with full organizational support for virtualization rather than organically growing a virtualization infrastructure.

Avaya Aura® Contact Center migrations

Avaya Aura® Contact Center supports migration from physical to virtual servers, and from virtual to physical servers. This is dependent on the server you are migrating to satisfying the server specifications. For more information about migration, see *Upgrading and patching Avaya Aura® Contact Center*.

Contact Center virtualization deployment options

Avaya Aura® Contact Center supports VMware vSphere. VMware vSphere allows multiple copies of the same operating system or several different operating systems to run as virtual machine on a large x86-based host hardware server. You must ensure that each virtual machine on which you plan to install Contact Center software satisfies the capacity requirements and specifications for your contact center.

The following table shows VMware support for each server type and platform available on the Avaya Aura® Contact Center DVD.

Table 19: Avaya Aura® Contact Center VMware support by server type

Voice Platform	Contact Center DVD server type	Virtual Machine OS	Supported
SIP-enabled Avaya Aura® Unified Communications platform	Voice and Multimedia Contact Server without Avaya Aura® Media Server	Windows	Yes
	Voice Contact Server Only	Windows	Yes
	Multimedia Contact Server Only	Windows	Yes
	Voice and Multimedia Contact Server with Avaya Aura® Media Server	Windows	No
	Avaya Aura® Media Server	Linux	Yes
AML-based Avaya Communication Server 1000 (CS 1000)	Voice and Multimedia Contact Server without Avaya Aura® Media Server	Windows	Yes
	Voice Contact Server Only	Windows	Yes
	Multimedia Contact Server Only	Windows	Yes

Voice Platform	Contact Center DVD server type	Virtual Machine OS	Supported
All voice platform types	Network Control Center Server Only	Windows	Yes

The Windows version of Avaya Aura® Media Server is not supported on VMware.

The following are some examples of Avaya Aura® Contact Center solutions using VMware.

Examples of small to medium size SIP-enabled Contact Center solutions

The following diagram shows a virtualized Avaya Aura® Contact Center example solution. This solution is based on the SIP-enabled Avaya Aura® Unified Communications platform. The diagram shows a Voice and Multimedia Contact Server on a Windows virtual machine. Avaya Aura® Media Server is installed on a physical Linux server.

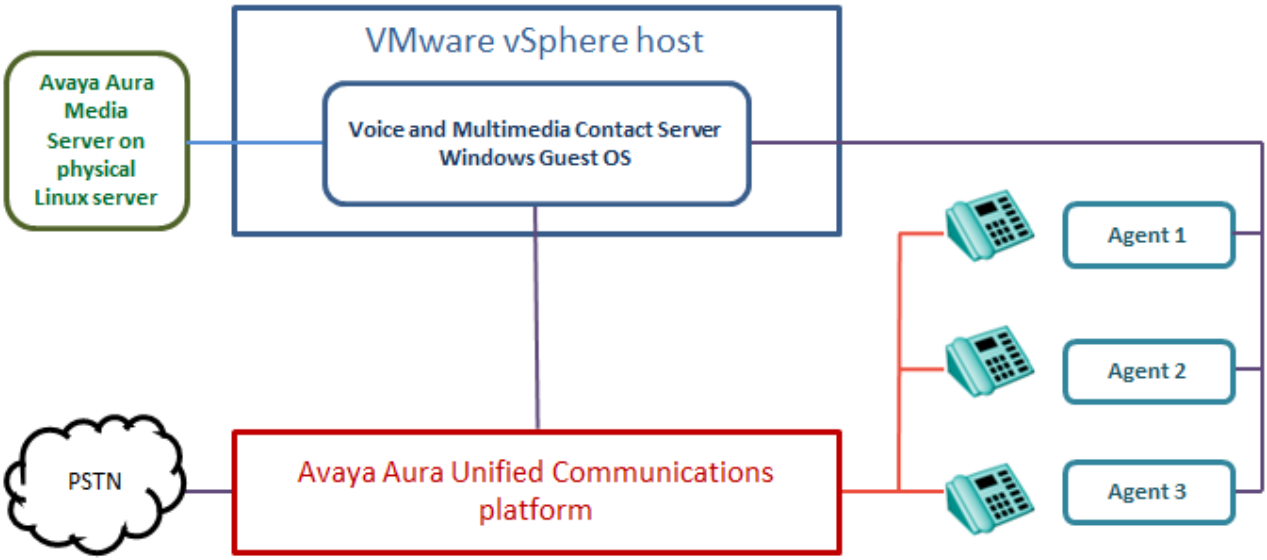


Figure 21: A typical SIP-enabled solution with virtualized Avaya Aura® Contact Center

The following diagram shows another virtualized SIP-enabled example solution. The diagram shows a Voice and Multimedia Contact Server on a Windows virtual machine. Avaya Aura® Media Server is installed on a Linux virtual machine. Avaya Aura® Media Server and the Voice and Multimedia Contact Server are installed on separate VMware host servers.

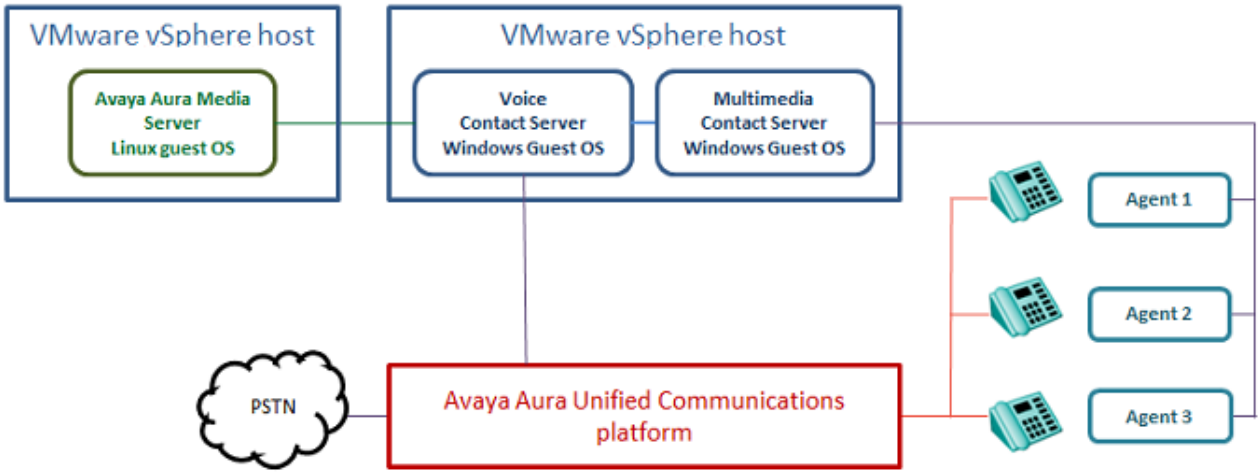


Figure 22: An example solution with Avaya Aura® Media Server and Avaya Aura® Contact Center on separate VMware host servers

For these small to medium size solution types, Avaya Aura® Contact Center supports Network Control Center as a VMware virtual machine on the same host as the Voice and Multimedia Contact Server.

Examples of large SIP-enabled Contact Center solutions

The following diagram shows a virtualized Avaya Aura® Contact Center example solution with a large agent count. This solution is based on the SIP-enabled Avaya Aura® Unified Communications platform. The diagram shows a Voice Contact Server on a Windows virtual machine, and Multimedia Contact Server on another Windows virtual machine. Avaya Aura® Media Server is installed a physical Linux server. Depending on the number of agents required, a large SIP-enabled solution might require more than one physical Avaya Aura® Media Server.

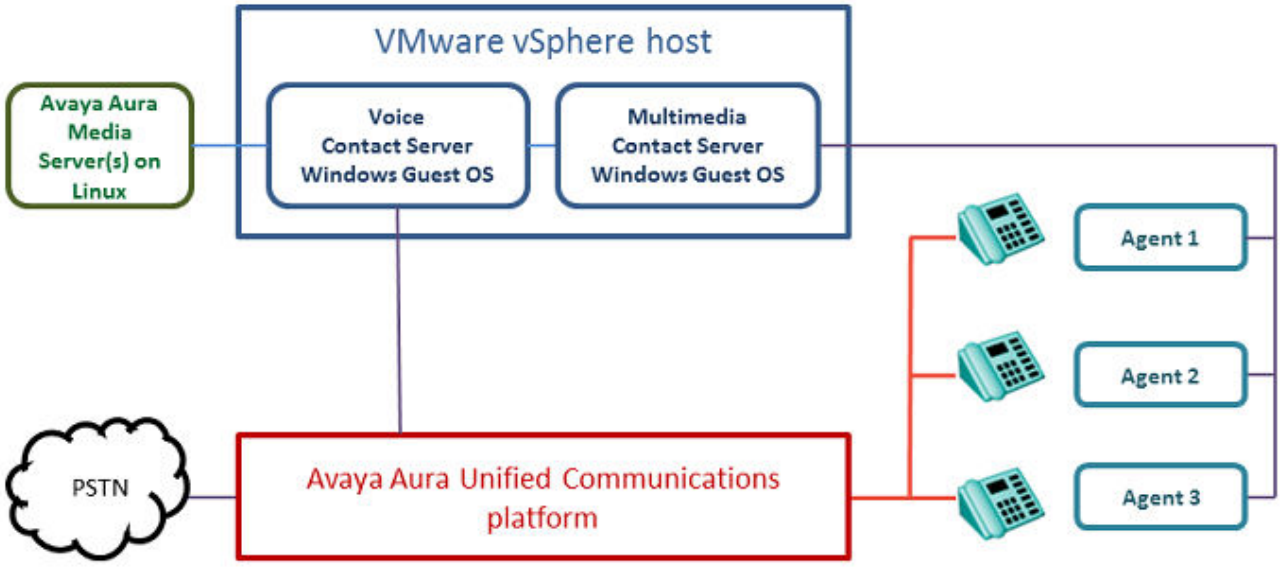


Figure 23: A typical SIP-enabled solution with virtualized Avaya Aura® Contact Center (large solution)

For these large solution types, Avaya Aura® Contact Center supports Network Control Center as a VMware virtual machine on the same host as the Voice Contact Server or the Multimedia Contact Server.

Example of a CS 1000 AML-based medium size Contact Center solution

The following diagram shows a typical virtualized Avaya Aura® Contact Center solution. This solution is based on the Avaya Communication Server 1000 platform. The diagram shows a Voice and Multimedia Contact Server on a Windows virtual machine.

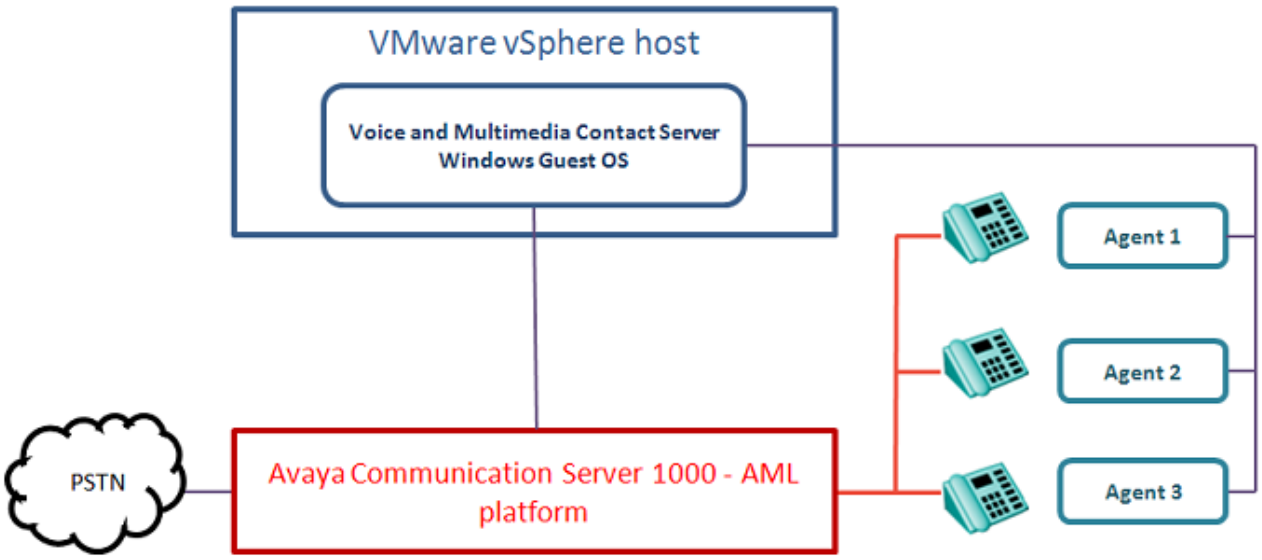


Figure 24: A typical CS 1000 AML-based solution with virtualized Contact Center (small to medium solution)

For this solution type, Avaya Aura® Contact Center supports Network Control Center as a VMware virtual machine on the same host as the Voice and Multimedia Contact Server.

Examples of CS 1000 AML-based large Contact Center solutions

The following diagram shows a typical virtualized Avaya Aura® Contact Center solution. This solution is based on the Avaya Communication Server 1000 platform. The diagram shows a Voice Contact Server on a Windows virtual machine, and Multimedia Contact Server on another Windows virtual machine.

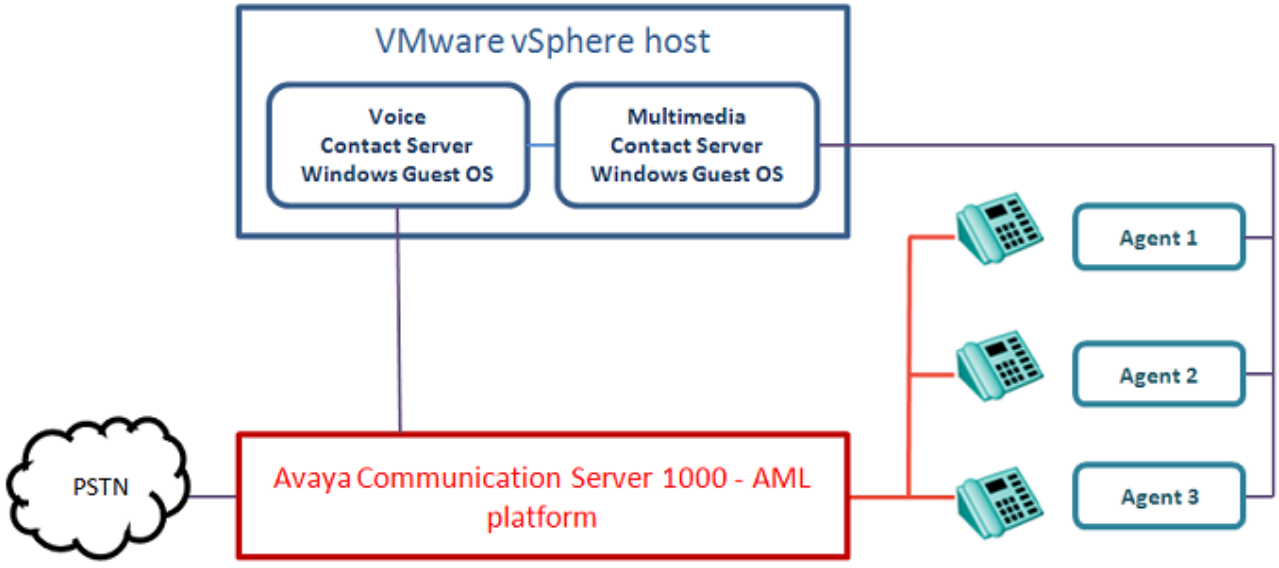


Figure 25: A typical CS 1000 AML-based solution with virtualized Contact Center (large solution)

Avaya Aura® Contact Center also supports Voice Contact Server and Multimedia Contact Server virtualized on separate VMware host servers.

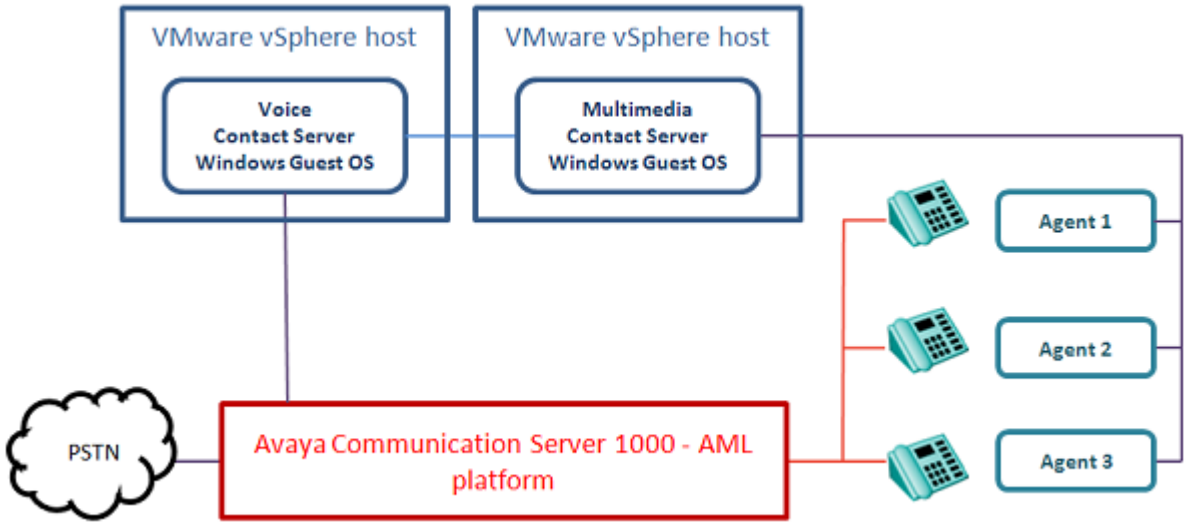


Figure 26: A typical CS 1000 based solution with contact center servers on separate VMware host servers

For this solution type, Avaya Aura® Contact Center supports Network Control Center as a VMware virtual machine on the same host as the Voice Contact Server and the Multimedia Contact Server.

VMware features

Avaya Aura® Contact Center is a collection of real-time applications running on the MS Windows Server 2012 R2 operating system. Avaya Aura® Contact Center provides real-time call control, multimedia handling, and statistical reporting.

Avaya Aura® Media Server is a real-time media processing application running on the Red Hat Enterprise Linux (RHEL) operating system. Avaya Aura® Media Server provides the real-time conferencing and media processing capabilities for Avaya Aura® Contact Center.

Some VMware features require CPU, Disk I/O, or networking resources to function. Running these VMware features can cause resource constraints and impact the real-time performance of the Avaya Aura® Contact Center and Avaya Aura® Media Server Virtual Machines (VMs). These features are therefore not supported while Avaya Aura® Contact Center or Avaya Aura® Media Server are active.

Some VMware features are not supported by Avaya Aura® Contact Center or Avaya Aura® Media Server. Some other VMware features are supported only while the Avaya Aura® Contact Center or Avaya Aura® Media Server Virtual Machines are stopped for maintenance.

The following table shows the Avaya Aura® Contact Center (AACC) and Avaya Aura® Media Server level of support for VMware features.

VMware Feature	Supported on active AACC VM	Supported during AACC VM maintenance window	Supported on active Avaya Aura® Media Server VM	Supported during Avaya Aura® Media Server VM maintenance window
Cloning	No	Yes	No	No
Distributed Power Management (DPM)	No	Yes	No	Yes
Distributed Resources Scheduler (DRS)	No	Yes	No	Yes
Distributed Switch	Yes	Yes	No	No
Fault Tolerance	No	No	No	No
High Availability (HA)	No	No	No	No
Snapshots	No	See Avaya Aura Contact Center VMware snapshot considerations on page 288	No	See Avaya Aura Media Server VMware Snapshot considerations on page 289
Storage DRS	No	Yes	No	Yes
Storage Thin Provisioning	No	N/A	No	N/A
Storage vMotion	No	Yes	No	Yes
Suspend & Resume	No	N/A	No	N/A
vMotion	No	Yes	No	No

VMware vSphere host considerations

When configuring virtual machines on your host system, the total resources needed by the virtual machines running on the host server must not exceed the total capacity of the host. It is good practice to under-commit CPU and memory resources on the host. If the host CPU capacity is overloaded, Contact Center does not function correctly.

Important:

Avaya Aura® Contact Center is not supported on an over-committed host where the total virtual resources from all virtual machines hosted exceeds the physical resources of the host.

Virtual Machine File System (VMFS)

VMware virtual machines and snapshots are stored in a Virtual Machine File System (VMFS) datastore. To support Avaya Aura® Contact Center on a virtual machine, the VMware datastore

containing Contact Center must be VMFS 5.54 or later. If you upgrade an existing VMware host server, ensure the associated datastore is upgraded to VMFS 5.54 or later.

Hardware-Assisted Virtualization

Most recent enterprise-level processors from Intel and AMD support virtualization. There are two generations of virtualization support: the first generation introduced CPU virtualization; the second generation included CPU virtualization and added memory management unit (MMU) virtualization. For the best performance, make sure your system uses processors with at least second-generation hardware-assist features.

Hardware-Assisted CPU Virtualization (Intel VT-x)

The first generation of hardware virtualization assistance includes VT-x from Intel. These technologies automatically trap sensitive interrupts, eliminating the overhead required to do so in software. This allows the use of a hardware virtualization (HV) virtual machine monitor (VMM).

Hardware-Assisted MMU Virtualization (Intel EPTI)

More recent enterprise-level processors also include a feature that addresses the overheads due to memory management unit (MMU) virtualization by providing hardware support to virtualize the MMU. VMware vSphere supports this feature in Intel processors, where it is called Extended Page Tables (EPT).

Storage Area Network (SAN)

A Storage Area Network (SAN) is a dedicated storage network that provides access to consolidated block level storage. SANs are used to make storage devices such as disk arrays, accessible to servers so that the devices appear as locally attached to the operating system.

When Avaya Aura® Contact Center is installed on virtual machines it supports a SAN. You must monitor the Contact Center demand on the SAN storage device. Adhere to your vendor-specific SAN configuration recommendations to ensure the SAN storage device meets the demands of Contact Center.

Disk drive provisioning

Provision sufficient hard disk drive space on the host server to support all the virtual machines, an ISO library, and provision additional space for snapshot image storage.

Guidance for storage requirements

Input/Outputs per Second (IOPS) is a measure of the maximum number of reads and writes to *non-contiguous* storage locations performed per second. IOPS measurements are associated with smaller files and more continuous changes, and comprise the workloads most typical in real-time enterprise applications such as Avaya Aura® Contact Center.

In a virtualized environment, any given storage array must be designed to have an IOPS capacity exceeding the sum of the IOPS required for all resident applications.

For a standalone (non-HA) Avaya Aura® Contact Center instance with 5000 voice-only agents and a call rate of 100K calls per hour, the IOPS is:

- Average: 137
- Maximum: 1496

For a standalone (non-HA) Avaya Aura® Contact Center instance with 600 multiplicity-enabled agents handling a call rate of 14K calls per hour and 12K contacts per hour, the IOPS is:

- Average: 105
- Maximum: 1488

These IOPS figures include Avaya Aura® Contact Center and the underlying operating system loads.

VMware Contact Center virtual machine Operating Systems

Provision each Avaya Aura® Contact Center virtual machine with at least the same specification as is listed for the physical server. The virtual machine must have at least the same amount of allocated memory and hard disk space as an equivalent physical server. The virtual hard disk must have the same size partitions as an equivalent physical server. Thick provision the virtual hard disks. The networking requirements of each virtual machine are the same as the networking requirements of an equivalent physical server.

Install the most recent version of the VMware Tools on each virtual machine operating system.

For improved performance, follow these recommendations:

- Disable screen savers and Window animations on the virtual machines. Screen savers and animations all consume extra physical CPU resources, potentially affecting consolidation ratios and the performance of other virtual machines.
- Schedule backups and virus scanning programs in virtual machines to run at off-peak hours and do not schedule them to run simultaneously in multiple virtual machines on the same VMware host.

For more useful information of this type, read *Performance Best Practices for VMware vSphere* for the version of VMware vSphere you are using. Using virtualization in a contact center enterprise solution requires careful up-front planning, engineering, and implementation. The VMware Best Practices guide is a good starting point.

Performance monitoring and management

You must continuously monitor and measure the performance of the Contact Center host server. You can use VMware vSphere vCenter to measure the critical host performance metrics in real-time.

VMware vCenter aggregates and archives performance data so that data can be visualized and reported on.

Configure VMware vCenter statistics collection to collect 5 minute and 30 minute Interval Duration data for the host at Statistics Level 3. Retain the 5 minute Interval Duration data for 3 days and retain the 30 minute Interval Duration for 1 week.

Generate performance reports using vCenter Report Performance and archive these reports to provide a baseline performance reference. Generate and store 1-day and 1-week reports. Store the associated vCenter Report Summary with the performance reports. You must analyze performance reports after changes to the host to assess the impact of the change on the host.

Monitor, acknowledge, and resolve VMware vCenter alarms. In particular, you must immediately investigate and resolve host CPU usage and host memory usage alarms.

In addition, the command-line tools “esxtop” and “resxtop” are available to provide a fine-grained look at real-time metrics. There are a number of critical CPU-related counters to watch out for:

- If the load average listed on the first line of the CPU Panel is equal to or greater than the number of physical processors in the system, this indicates that the system is overloaded.
- The usage percentage of physical CPUs on the PCPU line can indicate an overloaded condition. In general, 80 percent usage is a reasonable ceiling in production environments. Use 90 percent as an alert to the VMware administrator that the CPUs are approaching an overloaded condition, which must be addressed.
- %RDY - The percentage of time a schedulable entity was ready to run but is not scheduled to a core. If %RDY is greater than 10 percent, then this can indicate resource contention.
- %CSTP - The percentage of time a schedulable entity is stopped from running to allow other vCPUs in the virtual machine to catch up. If %CSTP is greater than 5 percent, this usually means the virtual machine workload is not using VCPUs in a balanced fashion. High %CSTP can be an indicator of a system running on an unconsolidated snapshot.

For more information about using esxtop or resextop, see the *VMware Resource Management Guide*.

Memory Reservations

Use VMware Reservations to specify the minimum amount of memory for a Contact Center virtual machine. VMware Reservations maintain sufficient host memory to fulfill all reservation guarantees. ESX does not power-on a virtual machine if doing so reduces the amount of available memory to less than the amount reserved. Using reservations might reduce the total number of virtual machines that can be hosted on a VMware host server. After all resource reservations have been met, ESX allocates the remaining resources based on the number of shares and the resource limits configured for your virtual machine.

High Availability and virtualization

The Avaya Aura® Contact Center High Availability feature supports virtualization.

Avaya Aura® Contact Center supports High Availability and virtualization where:

- The Active, Standby, and Remote Geographic Node servers are all virtualized on separate VMware host servers.
- The Active and Standby servers are virtualized on separate VMware host servers, and the Remote Geographic Node is installed on a physical server.
- The Active and Standby servers are installed on physical servers, and the Remote Geographic Node is installed on a virtual server.

All VMware host servers supporting Avaya Aura® Contact Center High Availability must use the same version of VMware. The virtualized Avaya Aura® Contact Center servers must have the same VMware virtual machine configuration settings.

Avaya Aura® Media Server supports High Availability when the Primary and Backup Avaya Aura® Media Servers are virtualized on separate VMware host servers.

Avaya Aura® Contact Center VMware Snapshot considerations

VMware snapshots save the current state of the virtual machine, so you can return to it at any time. Snapshots are useful when you need to revert a virtual machine repeatedly to the same state, but you don't want to create multiple virtual machines.

The following considerations apply when using snapshots with Avaya Aura® Contact Center on VMware:

- Snapshots must be taken during an Avaya Aura® Contact Center maintenance window. Do not take a snapshot of a Contact Center virtual machine while Contact Center is running. Snapshots have a negative impact on the performance of a virtual machine over time. You must Delete All snapshots at the end of the maintenance window and *Consolidate* snapshots if required, before putting the Contact Center virtual machine back into production. For more information about consolidating snapshots, refer to VMware documentation. Before taking a snapshot, shutdown all Contact Center services and stop the Caché database instance using the Caché Cube.
- Create a snapshot for the Contact Center virtual machines all at the same time. Likewise, when you restore a snapshot, restore all snapshots to ensure the data is consistent across the Contact Center suite.
- In solutions using the Avaya Aura® Contact Center — High Availability feature, take a snapshot of the Active and Standby virtual machines at the same time. The Active and Standby virtual machines must be hosted on different host servers.
- When restoring snapshots, carefully consider the possible impact from out-of-date antivirus definitions, missed Microsoft Windows OS and security updates, and lapsed domain accounts on the contact center. Isolate the restored virtual machine until these issues are resolved.

- By default, a Windows Server 2012 R2 machine account password is changed every 30 days. This is an important consideration when reverting to a snapshot of a virtual machine that has been in use for more than 30 days, as it might cause the machine to lose its connection to the Windows domain. If this issue occurs, rejoin the Windows Server 2012 R2 virtual machine to the domain.

VMware snapshots are not a replacement for Avaya Aura® Contact Center database backup (and restore) procedures and practices. You must continue to perform regular and frequent Contact Center backups. For more information, see *Maintaining Avaya Aura® Contact Center*.

Avaya Aura® Media Server VMware Snapshot considerations

VMware snapshots save the current state of the virtual machine, so you can return to it at any time. Snapshots are useful when you need to revert a virtual machine repeatedly to the same state, but you don't want to create multiple virtual machines.

The following considerations apply when using snapshots with Avaya Aura® Media Server on VMware:

- Snapshots must be taken during an Avaya Aura® Media Server maintenance window. Do not take a snapshot of an Avaya Aura® Media Server virtual machine while the contact center is running. Snapshots have a negative impact on the performance of a virtual machine over time. You must Delete All snapshots at the end of the maintenance window and *Consolidate* snapshots if required, before putting the Avaya Aura® Media Server virtual machine back into production. For more information about consolidating snapshots, refer to VMware documentation.
- When restoring snapshots, carefully consider the possible impact from out-of-date antivirus definitions, missed Linux operating system updates and security updates. Isolate the restored virtual machine until these issues are resolved.

VMware snapshots are not a replacement for Avaya Aura® Media Server database backup (and restore) procedures and practices. For more information, see *Maintaining Avaya Aura® Contact Center*.

VMware networking best practices

There are many different ways of configuring networking in a VMware environment. Review the VMware networking best practices documentation before deploying Avaya applications on an ESXi host. This section is not a substitute for the VMware documentation. For improved performance and best practice, Contact Center uses Network Adapter type VMXNET 3.

The following are some suggested networking best practices:

- Separate network services to achieve greater security and performance. Create a vSphere *Standard Switch* with dedicated NICs for each service. Separate VMware Management, iSCSI (SAN traffic), and VM networks to separate physical NICs. If separate switches are not possible, consider port groups with different VLAN IDs.
- All physical NICs that are connected to the same vSphere *Standard Switch* must be connected to the same physical network.
- Configure all VMkernal vNICs to the same MTU (IP Maximum Transmission Unit).
- Configure Contact Center to use Network Adapter type VMXNET 3.

For more information about VMware networking best practices, refer to the VMware documentation.

Time synchronization considerations

VMware time synchronization controls whether the virtual machine time is periodically resynchronized with the host server while it is running. Even if the VMware time synchronization check box is unselected, VMware Tools by default synchronize the virtual machine's time after a few specific events that are likely to leave the time incorrect, and this causes Avaya Aura® Contact Center to fail.

Follow the VMware instructions (KB 1189) to completely disable host time synchronization on the Contact Center Manager Server virtual machine.

Important:

You must disable Contact Center Manager Server virtual machine time synchronization to the VMware host server time.

Troubleshooting VMware

Virtualization platform performance issues can result with Contact Center performance problems. The virtualization platform includes the host and the running virtual machines on the host. Contact Center performance problems can include but are not limited to high CPU usage, link instability, defaulted or abandoned calls.

You must logically and systematically investigate any Contact Center performance issues to rule out virtualization performance problems. All deviations from the published specifications must be investigated and resolved before the Contact Center software investigation is initiated. For more information, refer to the VMware vSphere documentation.

To support troubleshooting VMware resourcing issues, collect information about the following VMware Key Performance Indicators (KPIs).

VMware vSphere Host KPIs:

- Physical CPU
  - PCPU - Physical CPU usage.
  - CPU load average - Average CPU load average of host.
- Physical Memory
  - SWAP/MB - Memory swap usage statistics.

VMware vSphere Virtual Machine (VM) KPIs:

- vCPU
  - CPU RDY - Time VM was ready to run, but was not provided CPU resource.
  - CPU WAIT - Percentage of time spent in the blocked or busy wait state.
  - AMIN - Reservation allocated.
  - ASHRS - CPU shares allocated.
  - CPU CSTP - Amount of time a Symmetric Multi-Processing (SMP) VM was ready to run, but was delayed due to co-vCPU scheduling contention.
- Disk I/O
  - GAVG - Average operating system read latency per read operation.
  - DAVG/rd - Average device read latency per read operation.
  - DAVG/wr - Average device write latency per write operation.
  - RESETS/s - Number of commands reset per second.
  - ABRTS/s - Number of disk commands abandoned per second.
- Network
  - %DRPTX - Percentage of packets dropped when transmitting.
  - %DRPRX - Percentage of packets dropped when receiving.
- Memory
  - MCTLSZ - Amount of physical memory reclaimed memory balloon statistics.

Chapter 21: VMware Virtual Machine specifications

This section describes sample Avaya Aura® Contact Center solutions and the VMware virtual machine specifications for each sample solution. The sample solutions are based on agent count and call flow rates.

The sample Avaya Aura® Contact Center solutions, with a minimum virtual machine specification for each level, are as follows:

- Entry-level solution
- Mid-range solution
- High-end solution

For more information about Avaya Aura® Contact Center and VMware, see VMware virtualization support on page 277.

For small to medium SIP-enabled contact center solutions, Avaya Aura® Contact Center provides a Software Appliance. For information about the Avaya Aura® Contact Center Software Appliance, see Contact Center Software Appliance VMware specifications on page 310.

Supported VMware virtual machine configurations

The following table summarizes the supported Avaya Aura® Contact Center deployments for each server type. The table shows which server specification each Avaya Aura® Contact Center server type requires when installed a VMware virtual machine.

Table 20: Supported VMware virtual machine (VM) specification for each server type

Server type	Voice PABX	Entry-level VM	Mid-range VM	High-end VM
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	No	No	No
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	No	Yes	Yes
	CS 1000 AML	No	Yes	Yes
Voice Contact Server Only	Aura SIP	Yes	Yes	Yes
	CS 1000 AML	Yes	Yes	Yes
Multimedia Contact Server Only	Aura SIP	Yes	Yes	Yes
	CS 1000 AML	Yes	Yes	Yes
Multimedia Contact Server Only – Enterprise Web Chat	Aura SIP	No	Yes	Yes
Voice and Multimedia Contact Server with Avaya Aura® Media Server	No Switch Configured	No	No	No
Network Control Center Server	N/A	Yes	Yes	Yes
Avaya Aura® Media Server standalone on Linux	Aura SIP	Virtualized Avaya Aura® Media Server is supported only on either a VMware 4 vCPU or 8 vCPU virtual machine.		

SIP-enabled Avaya Aura® Contact Center requires one or more Avaya Aura® Media Server for media processing. Avaya Aura® Contact Center uses Avaya WebLM for license management.

AML-based Avaya Aura® Contact Center does not require or use Avaya Aura® Media Server or Avaya WebLM.

Note:

ESXi 5.0 Update 2 and later supports the creation of virtual machines with up to 32 vCPUs.

ESXi 5.1 and greater supports the creation of virtual machines with more than 32 vCPUs.

ESXi 5.5 and greater supports the creation of virtual machines with more than 32 vCPUs.

ESXi 6.0 and greater supports the creation of virtual machines with more than 32 vCPUs.

ESXi 6.5 and greater supports the creation of virtual machines with more than 32 vCPUs.

The Avaya Aura® Contact Center high-end solution and high-end virtual machine, with 38 vCPUs, is therefore supported only on the versions of ESXi listed above.

Note:

In a SIP-enabled Avaya Aura® Contact Center solution with more than 1000 agents, the Avaya Aura® Media Server instances must be installed on physical servers. SIP-enabled Avaya Aura® Contact Center solutions with up to 1000 agents support Avaya Aura® Media Server virtualization. SIP-enabled Avaya Aura® Contact Center solutions with more than 1000 agents do not support Avaya Aura® Media Server virtualization.

Virtualized entry-level solution

The following table lists the installation options, maximum number of agents, and maximum call rates of a virtualized entry-level Avaya Aura® Contact Center solution.

If your contact center requires more agents or a higher call rate than shown here, refer to the mid-range or high-end server specifications.

Server type	Voice platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/ Eph) Note 2
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
	CS 1000 AML	Not Supported	Not Supported	N/A	N/A
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
Voice Contact Server Only	Aura SIP	300 Note 3	100	6K	500 / 800
	CS 1000 AML	300	100	6K	500 / 800
Multimedia Contact Server Only	Aura SIP	1000	N/A	N/A	2.0K / 4.0K
	CS 1000 AML	1000	N/A	N/A	2.0K / 4.0K
Multimedia Contact Server Only with Enterprise Web Chat	Aura SIP	Not Supported	Not Supported	N/A	N/A
Network Control Center Server	All switch types	Supported	400	N/A	N/A

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

- For System Contact Rate calculations, IM contacts have a weighting equivalent to one system contact. One IM contact is equivalent to one system contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, Web chat contacts count as two system contacts. One Web chat is equivalent to two system contacts.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + (Web Chat * 2))
- Route to CDN and Transfer/Conference to CDN each count as two calls.

Note 2: Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Web chats per hour (WCph). Standard Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes.

Note 3: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on an entry-level server Avaya Aura® Contact Center supports 150 Agent Desktops and 150 Agent Browser applications.

Server type	Voice platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/ Eph) Note 2
Note: Avaya Aura® Contact Center High Availability is not supported on an entry-level server. **Note:** To achieve the stated capacities, configure your sever hardware for maximum performance. For more information, see Server performance and firmware settings on page 256. **Note:** You can use the instance of CCMA on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.					

VMware entry-level virtual machine specification

The following table specifies the minimum VMware resources for an Avaya Aura® Contact Center entry-level virtual machine. These are the minimum specifications for Avaya Aura® Contact Center Release 7.0 for the entry-level virtual machine in order to support the rated capacities.

Resource	Minimum value
Number of CPUs	14
Minimum CPU Clock speed (MHz)	2400
CPU reservation (MHz)	16730
RAM (GB)	16 GB
RAM Reservation (MB)	16384 MB
Minimum Virtual Storage (GB) - Thick Provision Lazy Zeroed	• 501 GB NTFS - Voice Contact Server • 501 GB NTFS - Network Control Center (NCC) • 601 GB NTFS - Multimedia Contact Server with 300 GB NTFS multimedia database • 901 GB NTFS - Multimedia Contact Server with recommended 600 GB NTFS multimedia database
Virtual Network Interface Cards (VMXNET3)	• 1x 1000 Mbps - for SIP OR • 2x 1000 Mbps - for CS1000

This entry-level virtual machine offers performance equivalent to the Avaya Aura® Contact Center entry-level physical server.

Virtualized mid-range solution

The following table lists the installation options, maximum number of agents, and maximum call rates of a virtualized mid-range Avaya Aura® Contact Center solution.

If your contact center requires more agents or a higher call rate than shown here, refer to the high-end server specifications.

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	300 Note 3	60	6K	0.8K / 1.2K
	CS 1000 AML	500	100	10K	0.8K / 1.2K
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
Voice Contact Server Only	Aura SIP	1500 Note 3	300	30K	4.0K / 8.0K
	CS 1000 AML	3000	400	60K	4.0K / 8.0K
Multimedia Contact Server Only	Aura SIP	2000	N/A	N/A	4.0K / 8.0K
	CS 1000 AML	2000	N/A	N/A	4.0K / 8.0K
Multimedia Contact Server Only with Enterprise Web Chat	Aura SIP	2000	N/A	N/A	12K / 8.0K
Network Control Center Server	All switch types	Supported	600	N/A	N/A

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

- For System Contact Rate calculations, IM contacts have a weighting equivalent to one system contact. One IM contact is equivalent to one system contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, Web chat contacts count as two system contacts. One Web chat is equivalent to two system contacts.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + (Web Chat * 2))
- For System Contact Rate calculations, Enterprise Web Chat contacts count as one system contact. One Enterprise Web Chat is equivalent to one system contact.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + Enterprise Web Chat)
- *Route to CDN* and *Transfer/Conference to CDN* each count as two calls.

Note 2: Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Web chats per hour (WCph). Standard Web chat capacity is based

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes. Enterprise Web Chat supports up to 3000 concurrent sessions. **Note 3**: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on a mid-range Voice Contact Server, Avaya Aura® Contact Center supports 750 Agent Desktops and 750 Agent Browser applications. **Note:** Reduce capacity by 35 percent if you are recording all calls. Reduce by (the percentage of calls being recorded) X (35 percent) if you are using sampled recording. **Note:** Avaya Aura® Contact Center High Availability is supported on mid-range servers. **Note:** To achieve the stated capacities, configure your sever hardware for maximum performance. For more information, see Server performance and firmware settings on page 256. **Note:** You can use the instance of CCMA on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.					

VMware mid-range virtual machine specification

The following table specifies the minimum VMware resources for an Avaya Aura® Contact Center mid-range virtual machine. These are the minimum specifications for Avaya Aura® Contact Center Release 7.0 for the mid-range virtual machine in order to support the rated capacities.

Resource	Minimum value
Number of CPUs	24
Minimum CPU Clock speed (MHz)	2400
CPU reservation (MHz)	28680
RAM (GB)	32 GB
RAM Reservation (MB)	32768 MB
Minimum Virtual Storage (GB) - Thick Provision Lazy Zeroed	• 501 GB NTFS - Voice Contact Server • 501 GB NTFS - Network Control Center (NCC) • 601 GB NTFS - Multimedia Contact Server with 300 GB NTFS multimedia database • 901 GB NTFS - Multimedia Contact Server with recommended 600 GB NTFS multimedia database • 801 GB NTFS - Voice and Multimedia Contact Server with 300 GB NTFS multimedia database • 1101 GB NTFS - Voice and Multimedia Contact Server with recommended 600 GB NTFS multimedia database
Virtual Network Interface Cards (VMXNET3)	• 1x 1000 Mbps - for SIP OR • 2x 1000 Mbps - for CS1000

This mid-range virtual machine offers performance equivalent to the Avaya Aura® Contact Center mid-range physical server.

Virtualized high-end solution

The following table lists the installation options, maximum number of agents, and maximum call rates of a virtualized high-end Avaya Aura® Contact Center solution.

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	600 Note 3	100	12K	1.2K / 2.4K
	CS 1000 AML	1000	200	20K	1.2K / 2.4K
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
Voice Contact Server Only	Aura SIP	3000 Note 3	600	45K	6.0K / 12K
	CS 1000 AML	5000	600	100K	6.0K / 12K
Multimedia Contact Server Only	Aura SIP	3000	N/A	N/A	6.0K / 12K
	CS 1000 AML	3000	N/A	N/A	6.0K / 12K
Multimedia Contact Server Only with Enterprise Web Chat	Aura SIP	3000	N/A	N/A	18K / 12K
Network Control Center Server	All switch types	Supported	600	N/A	N/A

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

- For System Contact Rate calculations, IM contacts have a weighting equivalent to one system contact. One IM contact is equivalent to one system contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, Web chat contacts count as two system contacts. One Web chat is equivalent to two system contacts.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + (Web Chat * 2))
- For System Contact Rate calculations, Enterprise Web Chat contacts count as one system contact. One Enterprise Web chat is equivalent to one system contact.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + Enterprise Web Chat)
- *Route to CDN* and *Transfer/Conference to CDN* each count as two calls.

Note 2: Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Standard Web chats per hour (WCph). Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes. Enterprise Web Chat supports up to 3000 concurrent sessions.

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
Note 3: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on a high-end Voice Contact Server, Avaya Aura® Contact Center supports 1500 Agent Desktops and 1500 Agent Browser applications. **Note:** Reduce capacity by 35 percent if you are recording all calls. Reduce by (the percentage of calls being recorded) X (35 percent) if you are using sampled recording. **Note:** Avaya Aura® Contact Center High Availability is supported on high-end servers. **Note:** To achieve the stated capacities, configure your sever hardware for maximum performance. For more information, see Server performance and firmware settings on page 256. **Note:** You can use the instance of CCMA on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.					

VMware high-end virtual machine specification

The following table specifies the minimum VMware resources for an Avaya Aura® Contact Center high-end virtual machine. These are the minimum specifications for Avaya Aura® Contact Center Release 7.0 for the high-end virtual machine in order to support the rated capacities.

Resource	Minimum value
Number of CPUs	38
Minimum CPU Clock speed (MHz)	2400
CPU reservation (MHz)	45410
RAM (GB)	32 GB
RAM Reservation (MB)	32768 MB
Minimum Virtual Storage (GB) - Thick Provision Lazy Zeroed	• 501 GB NTFS - Voice Contact Server • 501 GB NTFS - Network Control Center (NCC) • 601 GB NTFS - Multimedia Contact Server with 300 GB NTFS multimedia database • 901 GB NTFS - Multimedia Contact Server with recommended 600 GB NTFS multimedia database • 801 GB NTFS - Voice and Multimedia Contact Server with 300 GB NTFS multimedia database • 1101 GB NTFS - Voice and Multimedia Contact Server with recommended 600 GB NTFS multimedia database
Virtual Network Interface Cards (VMXNET3)	• 1x 1000 Mbps - for SIP OR • 2x 1000 Mbps - for CS1000

This high-end virtual machine offers performance equivalent to the Avaya Aura® Contact Center high-end physical server.

Note:

ESXi 5.0 Update 2 and later supports the creation of virtual machines with up to 32 vCPUs.

ESXi 5.1 and greater supports the creation of virtual machines with more than 32 vCPUs.

ESXi 5.5 and greater supports the creation of virtual machines with more than 32 vCPUs.

ESXi 6.0 and greater supports the creation of virtual machines with more than 32 vCPUs.

The Avaya Aura® Contact Center high-end solution and high-end virtual machine, with 38 vCPUs, is therefore supported only on ESXi 5.1, ESXi 5.5, ESXi 6.0, and greater.

Contact Center virtual machine hard disks and partitions

Create individual virtual hard disks for each of the required partitions for your Contact Center virtual machine. When creating a virtual hard disk for the Operating System partition, create a hard disk size 1GB greater that the required partition size to accommodate any additional Windows partitions that the Windows Server 2012 R2 install might create automatically.

For example, for an Operating System partition size requirement of 80GB, create an 81GB virtual hard drive. For each additional Contact Center partition, create a virtual hard drive greater than or equal to the partition size requirement. The virtual hard disk must be of sufficient size such that when the associated partition is created and formatted for it has a size matching the required NTFS partition size.

For improved multimedia offline data retention, Avaya recommends using a 600 GB partition for multimedia storage. The multimedia 600 GB partition requires SAN Storage.

Table 21: Contact Center Virtual Machine hard disk minimum partition sizes

Hard disk drive partition description	Drive letter	Minimum partition sizes for Voice Contact Server / NCC	Minimum partition sizes for Multimedia Contact Server with 300 GB multimedia partition	Recommended partition sizes for Multimedia Contact Server with 600 GB multimedia partition	Minimum partition sizes for Voice and Multimedia Contact Server 300 GB multimedia partition	Recommended partition sizes for Voice and Multimedia Contact Server with 600 GB multimedia partition
Operating System drive	C:	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition
Application drive	D:	120 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition
DVD drive	E:	—	—	—	—	—
Voice database drive	F:	200 GB NTFS partition	—	—	200 GB NTFS partition	200 GB NTFS partition
Multimedia database drive	G:	—	300 GB NTFS partition	600 GB NTFS partition	300 GB NTFS partition	600 GB NTFS partition
Database journal drive	H:	100 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition
	Total	501 GB of disk space	601 GB of disk space	901 GB of disk space	801 GB of disk space	1101 GB of disk space on a SAN

If using 900 GB Raid–1 disks, use the above Minimum Partition size option. Contact Center requires Hardware RAID-1 with duplicate hard disk drives with identical specifications. Therefore, the host server must implement Hardware RAID-1 or better.

Avaya Aura® Media Server virtual machine specification

The following table specifies the VMware resources for two Avaya Aura® Media Server virtual machines. This table shows the number of supported agents and agent sessions for a 4 vCPU and 8 vCPU Avaya Aura® Media Server virtual machine.

VMware setting	Value 4 vCPU	Value 8 vCPU
Maximum supported agents (No Call Recording)	200	400
Maximum supported agents (With Call Recording)	130	260
Maximum supported agent sessions	500	1000
Number of CPUs	4	8
Minimum CPU clock speed	2400 MHz	2400 MHz
Minimum CPU Reservation (MHz)	9560	19120
Minimum RAM (GB)	8	8
Minimum RAM Reservation (MB)	8192 MB	8192 MB
Minimum Virtual Storage (GB) - Thick Provision Lazy Zeroed	50 GB	50 GB
Minimum Virtual Network Interface Cards (1 Gbit/s)	1	1

- Avaya Aura® Media Server supports only a 4 vCPU or 8 vCPU virtual machine.
- In a SIP-enabled Avaya Aura® Contact Center solution with more than 1000 agents, the Avaya Aura® Media Server instances must be installed on physical servers. SIP-enabled Avaya Aura® Contact Center solutions with up to 1000 agents support Avaya Aura® Media Server virtualization. SIP-enabled Avaya Aura® Contact Center solutions with more than 1000 agents do not support Avaya Aura® Media Server virtualization.
- To create an Avaya Aura® Media Server virtual machine, you have the following options:
  - Deploy the Avaya Aura® Media Server OVA on a host server and re-configure it to one of the above VMware specifications (4 or 8 vCPU).
  - Manually create a virtual machine to one of the above VMware specifications; create a 4 vCPU or 8 vCPU virtual machine. Install a supported Linux operating system and then install the Avaya Aura® Media Server software.
- The VMware host server must not be overcommitted. The total number of vCPUs assigned across all virtual machines must be less than the host's physical core count. Leave at least one vCPU unassigned for the VMware hypervisor.
- You can deploy multiple instances of virtual Avaya Aura® Media Server on the same VMware host server, with the following limitations:
  - For virtualized Avaya Aura® Media Server High Availability deployments, the Primary and Backup instances of Avaya Aura® Media Server must be deployed on separate VMware host servers.
  - Maximum of 2000 Avaya Aura® Media Server sessions supported per physical network interface for VMware virtualized deployments.

- The virtualization host server must have a Quad port 1 Gbit/s NIC or faster with Receive Side Scaling support.
- Virtual CPU resource requirements refer to physical cores only and not logical cores associated with Hyper-Threading.
- Avaya recommends that you deploy as few instances of Avaya Aura® Media Server as possible to satisfy deployment scale requirements. For virtualized deployments of Avaya Aura® Media Server, deploy one 8 vCPU virtual machine instead of two 4 vCPU virtual machines where applicable**.**
- Avaya Aura® Media Server High Availability (HA):
  - Avaya Aura® Media Server HA is supported on 4 vCPU and 8 vCPU virtual machines.
  - The Primary and Backup instances of Avaya Aura® Media Server must be deployed on separate VMware host servers.
  - There is a 30% reduction in supported capacity for virtualized Avaya Aura® Media Server when deployed in HA mode. For example, an 8 vCPU Avaya Aura® Media Server virtual machine supports up to 1000 agent sessions. In HA mode, the Avaya Aura® Media Server HA pair supports 700 agent sessions. If Call Recording is enabled, the capacity reduces further.
- The minimum CPU Reservation (MHz) figure is based on the minimum supported clock speed. To fully reserve each CPU, reserve the number of CPUs multiplied by the virtualization host's core clock speed.
- The agent count is modelled on simple call offer and answer to agent plus 50% calls in queue.
- To estimate the supported agent counts for Avaya Aura® Media Server deployments, use 2.5 sessions per agent.
- To support more agent sessions, add additional Avaya Aura® Media Servers to your solution.
- For more information about Avaya Aura® Contact Center, Avaya Aura® Media Server, and VMware, see VMware virtualization support on page 277.

VMware host server minimum CPU specification

Configure each VMware virtual machine with the CPU resources to support Avaya Aura® Contact Center or Avaya Aura® Media Server. For each virtual machine and required agent count, configure a specified number of vCPU cores and CPU Reservations in MHz.

Avaya Aura® Contact Center VMware profiling uses a Dual 8-core Intel Xeon E5-2670 2.60GHz CPU as a reference CPU. This reference processor has 16 physical CPU cores. Each of these 16 cores has an individual benchmark value that is one sixteenth of the overall benchmark score of the reference processor. You use this individual core benchmark value to compare the cores from different processors and to select suitable VMware host hardware for Avaya Aura® Contact Center virtualization.

The individual core benchmark value for the processor in your VMware host server must be equal to or greater than 90% of the individual core benchmark value for the Avaya Aura® Contact Center reference processor.

Follow these steps to ensure your proposed VMware host CPUs meet the Contact Center minimum requirements.

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the reference CPU: Dual 8-core Intel Xeon E5-2670 2.60GHz.

  Reference individual core benchmark value = (Reference CPU benchmark from website / Number of cores in reference CPU)

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for your VMware host server CPU.

  Individual core benchmark value = (Your host server CPU benchmark from website / Number of cores in host server CPU)

- To support Contact Center virtualization, the individual core benchmark value of your VMware host must be equal to or greater than 90% of the reference individual core benchmark value.

To support Contact Center, your VMware host must have a sufficient number of CPU cores each with at least the minimum individual core benchmark value.

VMware host server resource management and monitoring

When Avaya Aura® Contact Center is virtualized and commissioned, continue to monitor and manage its real-time VMware resources.

- VMware host servers where Avaya Aura® Media Server is deployed as a virtual machine must not be overcommitted in terms of physical cores. The total number of vCPUs assigned across all virtual machines must be less than the host's physical core count. Leave at least one vCPU unassigned for the VMware hypervisor.
- VMware host servers where Avaya Aura® Contact Center Entry-Level, Mid-Range, or High-End virtual machines are deployed must not be overcommitted in terms of logical cores. The total number of vCPUs assigned across all virtual machines must be less than the host's logical core count.
- Ensure VMware Tools is installed on all virtual machines. This is required for VMXNET3 support and VMware performance monitoring and management.
- The virtualization host server must have a Quad port 1 Gbit/s NIC or faster with Receive Side Scaling support.
- The VMware host server must not be overcommitted for RAM.
- Depending on your solution requirements, your Contact Center virtual machine might need additional RAM.

- If the total average CPU usage spikes above 50% for sustained periods, add additional CPU resources to the Contact Center virtual machine.
- If Contact Center virtual machine monitoring indicates resource starvation, add additional resources as necessary.
- Depending on your solution's call complexity, you might need to add additional VMware resources as necessary.
- Depending on your solution's administration and reporting requirements, you might need to add additional VMware resources as necessary. Avaya recommends running large or complex reports during off-peaks hours.
- The minimum CPU Reservation (MHz) figure is based on the minimum supported clock speed. To fully reserve each CPU, reserve the number of CPUs multiplied by the virtualization host's core clock speed.
- The supported agent counts and associated contact processing is modelled using simple contact processing with moderate reporting and administration.

Overview of deploying Contact Center with VMware

About this task

This section outlines how to engineer and install a virtualized environment to support Avaya Aura® Contact Center.

1. Read *Performance Best Practices for VMware vSphere* for the version of VMware vSphere you are using.
2. Each Contact Center server required equates to one virtual machine. The specification of each virtual machine must be at least the same as the specification of an equivalent physical Contact Center server.
3. Read your hardware provider's documents covering virtualization support.
4. Combine the individual Contact Center virtual machine specifications to determine the minimum specification for the Contact Center VMware vSphere host server hardware. The VMware host server must be sized to have at least the same resources as the collective resources of the physical servers required to run the Contact Center applications.
5. Obtain server hardware that meets the Contact Center host hardware specification and supports VMware vSphere.
6. Install the most recent firmware available for your host server. Configure the server BIOS settings to ensure optimum performance from the underlying server hardware. For more information, see Server performance and firmware settings on page 256.
7. On the host server, disconnect or disable unused or unnecessary physical hardware devices such as: COM ports, LPT ports, USB controllers, Network interfaces, Storage controllers.
8. On the host server, enable all available Virtualization Technology options in the hardware BIOS. Enable Intel virtualization (VT-x) and if available enable Extended Page Tables (EPT).

The available virtualization settings vary by hardware provider and BIOS version. Read your hardware provider's documents covering virtualization support to determine which settings to configure.

9. Install VMware vSphere software on the host server.
10. Configure a networking infrastructure on the host server. Configure a *VM Network* and a *Standard Switch vSwitch*. For each Contact Center virtual machine, configure and use VMXNET 3 networking.
11. Using the vSphere client, configure each Contact Center virtual machine with the CPU, memory, and disk space required for your contact center configuration.
12. On each Contact Center virtual machine, completely disable time synchronization to the host time. During Contact Center commissioning, the Contact Center virtual machines are synchronized with the voice switching (PABX) platform.
13. Add the Avaya Aura® Contact Center DVD image to the vSphere ISO library.
14. Prepare each virtual machine for Avaya Aura® Contact Center:
    - If you are installing Contact Center software, configure disk partitions and install Windows Server 2012 Release 2 operating system.
    - If you are installing Avaya Aura® Media Server, configure disk partitions and install Red Hat Enterprise Linux operating system.
15. On each Avaya Aura® Contact Center virtual machine, perform the Contact Center server preparation procedures.
16. Install Avaya Aura® Contact Center software on the operating system.
17. Commission and deploy each Contact Center virtual machine as normal.
18. Capture the initial CPU and memory usage, as baseline performance metrics.
19. Continue to monitor the CPU and memory of each Avaya Aura® Contact Center virtual machine.
20. Continue to monitor all the resources of the vSphere host server, focusing on CPU, memory, and disk drive resources.
21. For more information about configuring VMware virtual machines for Avaya Aura® Contact Center, see VMware virtualization support on page 277.

Chapter 22: Contact Center Software Appliance VMware specifications

This section specifies the VMware resources required to support the Avaya Aura® Contact Center software appliance. SIP-enabled Avaya Aura® Contact Center offers a software appliance for small to medium sized virtualized solutions. The software appliance consists of the following three VMware virtual machines:

- Avaya Aura® Contact Center Voice and Multimedia Contact Server virtual machine
- Avaya Aura® Media Server OVA
- Avaya WebLM OVA

The following diagram shows a typical virtualized solution using Avaya Aura® Contact Center, Avaya Aura® Media Server, and Avaya WebLM installed on a single VMware host server and integrated with an Avaya Aura® Unified Communications platform to build a SIP-enabled contact center solution.

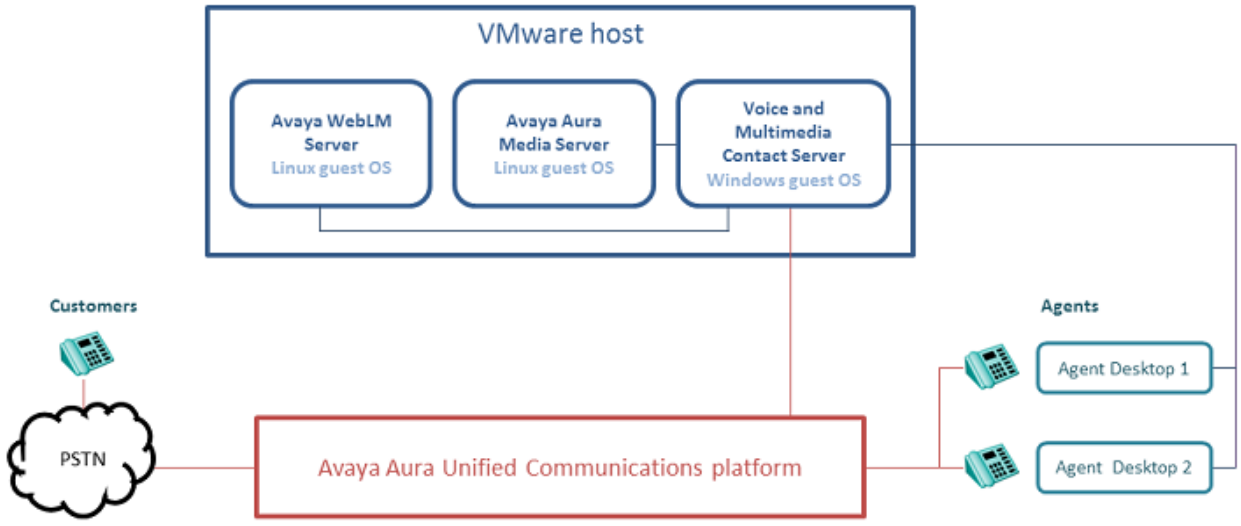


Figure 27: Typical SIP-enabled virtualized contact center solution

You can use a single Open Virtual Appliance (OVA) package to distribute a virtual appliance. For example, an Avaya Aura® Media Server OVA package includes all of the Open Virtualization Format (OVF) information required to create an Avaya Aura® Media Server virtual appliance on a VMware

host. A virtual appliance contains a preinstalled, preconfigured operating system and an application stack optimized to provide a specific set of services. The Avaya Aura® Media Server and Avaya WebLM OVAs are prepackaged and ready for deployment.

For the Avaya Aura® Contact Center virtual machine, you build a suitably specified virtual machine and then install product software from the Avaya Aura® Contact Center DVD or ISO image.

The following table specifies the maximum overall capacity of the Avaya Aura® Contact Center software appliance.

Maximum logged-in agents	Maximum CCMA supervisors	Maximum System Contact Rate (cph) Note 1	Maximum multimedia rate WCph/ Eph) Note 2
400	80	8K	600 /1200
Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types. **Note 2:** Multimedia contact rates are applicable only if multimedia is part of the solution. Email contacts per hour (Eph). Standard Web chats per hour (WCph). Standard Web chat maximum capacity is based on an average chat duration of 5 minutes. The maximum number of simultaneous Standard Web chat sessions is 50.			

You can use VMware vSphere or vCenter and these Avaya Aura® Contact Center components to create virtual machines in your virtualized environment.

The Avaya Aura® Contact Center software appliance is supported only on the following virtualization environments:

- ESXi 5.0 Update 2
- ESXi 5.1
- ESXi 5.5
- ESXi 6.0
- ESXi 6.5

Note:

VMFS 5.54 or later is required for all supported versions of ESXi.

Avaya Aura® Contact Center supports the Avaya WebLM virtual machine co-resident on the same VMware host server or deployed on a separate VMware host server.

Avaya Aura® Contact Center supports the Avaya Aura® Media Server virtual machine co-resident on the same VMware host server or deployed on a separate VMware host server.

AML-based Avaya Aura® Contact Center does not provide a software appliance. For information about Avaya Communication Server 1000 AML-based solutions and virtualization, see VMware Virtual Machine specifications on page 292 or Hyper-V virtualization support on page 322.

Voice and Multimedia Contact Server virtual machine

Use the Voice and Multimedia Contact Server virtual machine to provide context-sensitive and skill-based routing for customer voice and multimedia contacts.

The Voice and Multimedia Contact Server virtual machine contains the following contact center application software.

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)
- Firewall policy

To create the Voice and Multimedia Contact Server virtual machine, perform the following:

1. Create a VMware virtual machine that meets or exceeds the minimum specifications for your solution. For information about engineering the VMware resources for your solution, refer to *Avaya Aura® Contact Center Overview and Specification*.
2. Install the Windows Server 2012 Release 2 Standard or Datacenter edition English operating system on the virtual machine.
3. License and activate the Microsoft Windows 2012 R2 operating system.
4. Configure the server and format the hard disks and disk partitions to the required specifications.
5. Install VMware Tools on the server.
6. Download and read the most recent Avaya Aura® Contact Center Release Notes.
7. Obtain an Avaya Aura® Contact Center DVD or ISO image.
8. Download the most recent Avaya Aura® Contact Center Service Packs and updates.
9. Obtain an Avaya Aura® Contact Center license file.
10. Use the Avaya Aura® Contact Center DVD or ISO image to install the SIP-enabled Voice and Multimedia Contact Server without Avaya Aura® Media Server server type. The Voice and Multimedia Contact Server with Avaya Aura® Media Server install option does not support VMware.
11. Use the Avaya Aura® Contact Center Configuration Ignition Wizard to install the software.
12. Commission the Voice and Multimedia Contact Server for your solution.
13. Continue to monitor the VMware real-time resources.

Each SIP-enabled Voice and Multimedia Contact Server requires one or more Avaya Aura® Media Server. You must install and configure one or more Linux-based Avaya Aura® Media Servers in the contact center solution.

The Voice and Multimedia Contact Server supports the following Avaya Aura® Media Server options:

- Use the Avaya Aura® Contact Center DVD to install Avaya Aura® Media Server software on a physical Linux server.
- Use the Avaya Aura® Contact Center DVD to install Avaya Aura® Media Server software on a Linux virtual machine.
- Deploy the Avaya Aura® Media Server OVA package to create a virtualized Avaya Aura® Media Server virtual machine.

Each SIP-enabled Voice and Multimedia Contact Server virtual machine also requires an additional, separate, Avaya WebLM licensing server. In a Contact Center High Availability deployment you must provision a second Avaya WebLM server to provide licenses to the standby server or to the Remote Geographic Node server.

You can use any account with local administrative rights to install Avaya Aura® Contact Center. You can use any account with local administrative rights to upgrade and patch Avaya Aura® Contact Center; you do not need to always use the same account to perform these tasks.

Important:

You must disable the Admin Approval Mode security feature on the Contact Center server. This ensures that accounts with local administrative rights get full privileges for running applications on the Contact Center server.

Voice and Multimedia Contact Server virtual machine hard disks and partitions

Create individual virtual hard disks for each of the required partitions for your Contact Center virtual machine. When creating a virtual hard disk for the Operating System partition, create a hard disk size 1GB greater that the required partition size, to accommodate the creation of any additional Windows partitions that the Windows Server 2012 R2 install might create automatically.

For example, for an Operating System partition size requirement of 80GB, create an 81GB virtual hard drive. For each additional Contact Center required partition, create a virtual hard drive greater than or equal to the partition size requirement. The virtual hard disk must be of sufficient size such that when the associated partition is created and formatted it has a size matching the required partition size for the install.

For improved multimedia offline data retention, Avaya recommends using a 600 GB partition for multimedia storage. The multimedia 600 GB partition requires SAN Storage.

Table 22: Contact Center Virtual Machine hard disk minimum partition sizes

Hard disk drive partition description	Drive letter	Minimum partition sizes	Recommended partition sizes, 300 GB multimedia partition	Recommended partition sizes, 600 GB multimedia partition
Operating System drive	C:	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition
Application drive	D:	100 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition
DVD drive	E:	—	—	—
Voice database drive	F:	180 GB NTFS partition	200 GB NTFS partition	200 GB NTFS partition
Multimedia database drive	G:	200 GB NTFS partition	300 GB NTFS partition	600 GB NTFS partition
Database journal drive	H:	80 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition
	Total	641 GB of Thick Provisioned disk space in a VMware datastore.	801 GB of Thick Provisioned disk space in a VMware datastore.	1101 GB of Thick Provisioned disk space in a SAN datastore.

If using 900 GB Raid–1 disks, use the above Minimum Partition size option.

Contact Center requires Hardware RAID-1 with duplicate hard disk drives with identical specifications. Therefore, the VMware host server must implement Hardware RAID-1 or better.

Avaya Aura® Media Server OVA

The Avaya Aura® Media Server OVA contains information about the virtual machine specification, virtual machine operating system, and application software. This OVA contains the following components:

- Red Hat Enterprise Linux 6.6, 64–bit
- Avaya Aura® Media Server 7.7 software
- IP tables firewall file application
- VMware Tools. Do not update the VMware Tools software on this virtual machine unless instructed to do so by Avaya.

Avaya Aura® Media Server is a software based media processing platform. Avaya Aura® Media Server provides the conference services required by SIP-enabled Contact Center.

The Avaya Aura® Media Server OVA package has the following default hardware configuration:

vCPU	Minimum CPU speed	Virtual memory required	Number of NICs	Virtual disk storage required	
4	2400 MHz	4.5 GB (4608 MB)	1 VMXNET3 Network Adapter. The virtualization host server must have a Quad port 1 Gbit/s NIC or faster with Receive Side Scaling support.	Size	50 GB
				Deploy the Avaya Aura® Media Server OVA using Thick Provision Lazy Zeroed. Avaya Aura® Media Server does not support thin provisioning	

Contact Center does not support Avaya Aura® Media Server using these default deployment settings. After you deploy the Avaya Aura® Media Server, re-configure the virtual machine to have 4 or 8 CPUs and at least 8 GB RAM. Avaya Aura® Media Server is supported only on virtual machines with 4 or 8 CPUs.

In a virtualized Contact Center environment, you can use VMware to load the Avaya Aura® Media Server OVA package into a virtual machine in your contact center solution. The virtualized Contact Center server can then use the virtualized Avaya Aura® Media Server as a voice media processor.

Deploy the Avaya Aura® Media Server OVA using Disk Format - Thick Provision Lazy Zeroed. Avaya Aura® Media Server does not support thin provisioning.

WebLM OVA

Contact Center supports the WebLM license manager server. For increased efficiency and flexibility, the WebLM license manager supports the VMware Virtual Appliance and Open Virtualization Archive (OVA) deployment mechanisms. In a virtualized Contact Center environment, you can use VMware to load the WebLM OVA package onto a separate virtual machine in your contact center solution. The virtualized Contact Center server can then use the virtualized WebLM server as the license manager.

The WebLM OVA contains a hardened Linux operating system.

The WebLM OVA requires the following:

vCPU	Minimum CPU speed	Virtual memory reservation	Number of NICs	Virtual disk storage reservation
1	2300 MHz	2 GB	1 shared	35 GB

Note:

Do not change any of these WebLM OVA VMware virtual machine settings.

The WebLM OVA uses the following network mapping:

WebLM Server VM Interface	Application
Eth0	License management

The WebLM server for VMware is packaged as a vAppliance ready for deployment using either VMware vSphere Client or VMware vCenter.

Deploy the WebLM OVA using Disk Format - Thick Provision Lazy Zeroed. Avaya WebLM does not support thin provisioning in production environments.

Avaya Aura® Contact Center software appliance VMware resource profiling

This section defines the Avaya Aura® Contact Center software appliance VMware virtual machine resource requirements.

Use the following tables to determine the minimum VMware resources required to support a range of agent counts and system contact rates.

Table 23: Avaya Aura® Contact Center Voice and Multimedia Contact Server VMware virtual machine minimum resource requirements

Maximum supported agents	**200**	**400**
Maximum system Contact Rate (system contacts per hour)	**4000**	**8000**
Email Contact Rate (Emails per hour)	**600**	**1200**
WebChat Contact Rate (WebChat per hour)	**300**	**600**
Number of CPUs (Minimum CPU clock speed 2400 MHz)	4	6
Minimum CPU Reservation (MHz)	9560	14340
Minimum RAM (GB)	16 GB	16 GB
Minimum RAM Reservation (MB)	16384	16384
Minimum Disk Size (GB) - Thick Provision Lazy Zeroed	641 GB	641 GB
Virtual Network Interface Cards (1 GB) VMXNET3	1	1

- The System Contact Rate is the total maximum combined contact rate across all supported contact types.

Table 24: Avaya Aura® Media Server VMware virtual machine minimum resource requirements

Maximum number of supported agents	**200**	**400**
Maximum supported sessions	**500**	**1000**
Number of CPUs (Minimum CPU clock speed 2400 MHz)	4	8
CPU Reservation (MHz)	9560	19120
Minimum RAM (GB)	8	8
Minimum RAM Reservation (MB)	8192	8192
Minimum Disk Size (GB) - Thick Lazy Provisioning	50	50
Virtual Network Interface Cards (1 GB) VMXNET3	1	1

- Avaya Aura® Media Server is supported only on a virtual machine with 4 or 8 CPUs.
- Virtualized Avaya Aura® Media Server in High Availability mode, has a 30% reduction in supported capacity.
- The agent count is modelled on simple call offer and answer to agent plus 50% calls in queue.
- To estimate the supported agent counts for Avaya Aura® Media Server deployments, use 2.5 sessions per agent.

Table 25: Avaya WebLM VMware virtual machine resource minimum requirements

Maximum supported license requests	5000
Number of CPUs (Minimum CPU clock speed 2300 MHz)	1
CPU Reservation (MHz)	2290
Minimum RAM (GB)	2
Minimum RAM Reservation (MB)	2048
Minimum Disk Size (GB)	35
Virtual Network Interface Cards (1 GB) VMXNET3	1

VMware host server minimum CPU specification

Configure each VMware virtual machine with the CPU resources to support Avaya Aura® Contact Center or Avaya Aura® Media Server. For each virtual machine and required agent count, configure a specified number of vCPU cores and CPU Reservations in MHz.

Avaya Aura® Contact Center VMware profiling uses a Dual 8-core Intel Xeon E5-2670 2.60GHz CPU as a reference CPU. This reference processor has 16 physical CPU cores. Each of these 16 cores has an individual benchmark value that is one sixteenth of the overall benchmark score of the reference processor. You use this individual core benchmark value to compare the cores from different processors and to select suitable VMware host hardware for Avaya Aura® Contact Center virtualization.

The individual core benchmark value for the processor in your VMware host server must be equal to or greater than 90% of the individual core benchmark value for the Avaya Aura® Contact Center reference processor.

Follow these steps to ensure your proposed VMware host CPUs meet the Contact Center minimum requirements.

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the reference CPU: Dual 8-core Intel Xeon E5-2670 2.60GHz.

  Reference individual core benchmark value = (Reference CPU benchmark from website / Number of cores in reference CPU)

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for your VMware host server CPU.

  Individual core benchmark value = (Your host server CPU benchmark from website / Number of cores in host server CPU)

- To support Contact Center virtualization, the individual core benchmark value of your VMware host must be equal to or greater than 90% of the reference individual core benchmark value.

To support Contact Center, your VMware host must have a sufficient number of CPU cores each with at least the minimum individual core benchmark value.

VMware host server disks and storage

The VMware server hosting the Avaya Aura® Contact Center software appliance must have sufficient disk space or access to sufficient SAN storage.

The following table shows the VMware host server disk space required for the Avaya Aura® Contact Center software appliance virtual machines (VMs). For improved multimedia offline data retention, Avaya recommends using a 600 GB partition for multimedia storage. The multimedia 600 GB partition requires SAN Storage.

Table 26: VMware host server disk space for Avaya Aura® Contact Center software appliance

Virtual Machine	Minimum disk space	Recommended disk space with 300 GB multimedia partition	Recommended disk space with 600 GB multimedia partition
Avaya Aura® Contact Center VM	641 GB	801 GB	1101 GB NTFS
Avaya Aura® Media Server VM	50 GB	50 GB	50 GB
Avaya WebLM VM	35 GB	35 GB	35 GB
Total Avaya Aura® Contact Center software appliance storage	726 GB of disk space	886 GB of disk space	1186 GB of disk space on a SAN
VMware host server hard disk space	900 GB Datastore	1.2 TB Datastore	1.4 TB Datastore on SAN

Avaya Aura® Contact Center requires Hardware RAID-1 with duplicate hard disk drives with identical specifications. Therefore, the host server must implement Hardware RAID-1 or better.

VMware host server resource management and monitoring

When Avaya Aura® Contact Center is virtualized and commissioned, continue to monitor and manage its real-time VMware resources.

- VMware host servers where Avaya Aura® Media Server is deployed as a virtual machine must not be overcommitted in terms of physical cores. The total number of vCPUs assigned across all virtual machines must be less than the host's physical core count. Leave at least one vCPU unassigned for the VMware hypervisor.
- VMware host servers where Avaya Aura® Contact Center virtual machines for software appliance are deployed must not be overcommitted in terms of physical cores. The total number of vCPUs assigned across all virtual machines must be less than the host's physical core count.
- Ensure VMware Tools is installed on all virtual machines. This is required for VMXNET3 support and VMware performance monitoring and management.
- The virtualization host server must have a Quad port 1 Gbit/s NIC or faster with Receive Side Scaling support.
- The VMware host server must not be overcommitted for RAM.
- Depending on your solution requirements, your Contact Center virtual machine might need additional RAM.

- If the total average CPU usage spikes above 50% for sustained periods, add additional CPU resources to the Contact Center virtual machine.
- If Contact Center virtual machine monitoring indicates resource starvation, add additional resources as necessary.
- Depending on your solution's call complexity, you might need to add additional VMware resources as necessary.
- Depending on your solution's administration and reporting requirements, you might need to add additional VMware resources as necessary. Avaya recommends running large or complex reports during off-peaks hours.
- The minimum CPU Reservation (MHz) figure is based on the minimum supported clock speed. To fully reserve each CPU, reserve the number of CPUs multiplied by the virtualization host's core clock speed.
- The supported agent counts and associated contact processing is modelled using simple contact processing with moderate reporting and administration.

Chapter 23: Hyper-V virtualization support

This section describes sample Avaya Aura® Contact Center solutions and the Microsoft Hyper-V 2012 virtual machine specifications for each sample solution. The sample solutions are based on agent count and call flow rates.

The sample Avaya Aura® Contact Center solutions, with a minimum virtual machine specification for each level, are as follows:

- Entry-level solution
- Mid-range solution
- High-end solution

Avaya Aura® Contact Center supports virtualization using the following versions of Hyper-V.

- Microsoft Windows 2012 R2 Hyper-V
- Windows Server 2012 R2 Standard Core
- Windows Server 2012 R2 DataCenter Core

Avaya Aura® Contact Center does not support Hyper-V Clustered environments. The Avaya Aura® Contact Center Hyper-V host server must be standalone.

Avaya Aura® Contact Center is not supported on GUI-based installations of Windows Server 2012 R2 with the Hyper-V role added. Avaya Aura® Contact Center is supported only on Generation 2 virtual machines. The Generation 2 virtual machines must use EUFI boot firmware. Avaya Aura® Contact Center does not support Secure Boot. This feature is enabled by default on Generation 2 virtual machines; disable it before installing Avaya Aura® Contact Center.

Avaya Aura® Media Server is not supported on Microsoft Hyper-V. Avaya WebLM Server is not supported on Microsoft Hyper-V. Install Avaya Aura® Media Server on physical servers.

A dedicated Network Adapter is required for each Virtual Network Adapter. SIP-enabled Avaya Aura® Contact Center deployments require one virtual network adapter. AML-based Avaya Aura® Contact Center deployments support two virtual network adapters.

Supported Hyper-V virtual machine configurations

The following table summarizes the supported Avaya Aura® Contact Center deployments for each server type. The table shows which server specification each Avaya Aura® Contact Center server type requires when installed a Hyper-V virtual machine.

Table 27: Supported Hyper-V virtual machine (VM) specification for each server type

Server type	Voice PABX	Entry-level VM	Mid-range VM	High-end VM
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	No	No	No
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	No	Yes	Yes
	CS 1000 AML	No	Yes	Yes
Voice Contact Server Only	Aura SIP	Yes	Yes	Yes
	CS 1000 AML	Yes	Yes	Yes
Multimedia Contact Server Only	Aura SIP	Yes	Yes	Yes
	CS 1000 AML	Yes	Yes	Yes
Multimedia Contact Server Only — Enterprise Web Chat	Aura SIP	No	Yes	Yes
Voice and Multimedia Contact Server with Avaya Aura® Media Server	No Switch Configured	No	No	No
Network Control Center Server	N/A	Yes	Yes	Yes
Avaya Aura® Media Server standalone on Linux	Aura SIP	No	No	No

SIP-enabled Avaya Aura® Contact Center requires one or more Avaya Aura® Media Server for media processing. Avaya Aura® Contact Center uses Avaya WebLM for license management.

AML-based Avaya Aura® Contact Center does not require or use Avaya Aura® Media Server or Avaya WebLM.

Virtualized entry-level solution

The following table lists the installation options, maximum number of agents, and maximum call rates of a virtualized entry-level Avaya Aura® Contact Center solution.

If your contact center requires more agents or a higher call rate than shown here, refer to the mid-range or high-end server specifications.

Server type	Voice platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/ Eph) Note 2
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
	CS 1000 AML	Not Supported	Not Supported	N/A	N/A
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
Voice Contact Server Only	Aura SIP	300 Note 3	100	6K	500 / 800
	CS 1000 AML	300	100	6K	500 / 800
Multimedia Contact Server Only	Aura SIP	1000	N/A	N/A	2.0K / 4.0K
	CS 1000 AML	1000	N/A	N/A	2.0K / 4.0K
Multimedia Contact Server Only with Enterprise Web Chat	Aura SIP	Not Supported	Not Supported	N/A	N/A
Network Control Center Server	All switch types	Supported	400	N/A	N/A

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

- For System Contact Rate calculations, IM contacts have a weighting equivalent to one system contact. One IM contact is equivalent to one system contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, Web chat contacts count as two system contacts. One Web chat is equivalent to two system contacts.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + (Web Chat * 2))
- Route to CDN and Transfer/Conference to CDN each count as two calls.

Note 2: Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Web chats per hour (WCph). Standard Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes.

Note 3: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on an entry-level server Avaya Aura® Contact Center supports 150 Agent Desktops and 150 Agent Browser applications.

Server type	Voice platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/ Eph) Note 2
Note: Avaya Aura® Contact Center High Availability is not supported on an entry-level server. **Note:** To achieve the stated capacities, configure your sever hardware for maximum performance. For more information, see Server performance and firmware settings on page 256. **Note:** You can use the instance of CCMA on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.					

Hyper-V entry-level virtual machine specification

The following table specifies the minimum Hyper-V resources for an Avaya Aura® Contact Center entry-level virtual machine. These are the minimum specifications for Avaya Aura® Contact Center Release 7.0 for the entry-level virtual machine in order to support the rated capacities.

Resource	Minimum value
Number of CPUs	14
Minimum CPU Clock speed (MHz)	2400
Processor Reservation Percentage	50%
RAM (GB)	16 GB
RAM Assignment Profile	Static
Minimum Virtual Storage (GB) - Fixed Disks	• 501 GB NTFS - Voice Contact Server • 501 GB NTFS - Network Control Center (NCC) • 601 GB NTFS - Multimedia Contact Server with 300 GB NTFS multimedia database • 901 GB NTFS - Multimedia Contact Server with recommended 600 GB NTFS multimedia database
Virtual Network Interface Cards	• 1x 1000 Mbps - for SIP OR • 2x 1000 Mbps - for CS1000

This entry-level virtual machine offers performance equivalent to the Avaya Aura® Contact Center entry-level physical server.

Virtualized mid-range solution

The following table lists the installation options, maximum number of agents, and maximum call rates of a virtualized mid-range Avaya Aura® Contact Center solution.

If your contact center requires more agents or a higher call rate than shown here, refer to the high-end server specifications.

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	300 Note 3	60	6K	0.8K / 1.2K
	CS 1000 AML	500	100	10K	0.8K / 1.2K
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
Voice Contact Server Only	Aura SIP	1500 Note 3	300	30K	4.0K / 8.0K
	CS 1000 AML	3000	400	60K	4.0K / 8.0K
Multimedia Contact Server Only	Aura SIP	2000	N/A	N/A	4.0K / 8.0K
	CS 1000 AML	2000	N/A	N/A	4.0K / 8.0K
Multimedia Contact Server Only with Enterprise Web Chat	Aura SIP	2000	N/A	N/A	12K / 8.0K
Network Control Center Server	All switch types	Supported	600	N/A	N/A

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

- For System Contact Rate calculations, IM contacts have a weighting equivalent to one system contact. One IM contact is equivalent to one system contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, Web chat contacts count as two system contacts. One Web chat is equivalent to two system contacts.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + (Web Chat * 2))
- For System Contact Rate calculations, Enterprise Web Chat contacts count as one system contact. One Enterprise Web Chat is equivalent to one system contact.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + Enterprise Web Chat)
- *Route to CDN* and *Transfer/Conference to CDN* each count as two calls.

Note 2: Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Web chats per hour (WCph). Standard Web chat capacity is based

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes. Enterprise Web Chat supports up to 3000 concurrent sessions. **Note 3**: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on a mid-range Voice Contact Server, Avaya Aura® Contact Center supports 750 Agent Desktops and 750 Agent Browser applications. **Note:** Reduce capacity by 35 percent if you are recording all calls. Reduce by (the percentage of calls being recorded) X (35 percent) if you are using sampled recording. **Note:** Avaya Aura® Contact Center High Availability is supported on mid-range servers. **Note:** To achieve the stated capacities, configure your sever hardware for maximum performance. For more information, see Server performance and firmware settings on page 256. **Note:** You can use the instance of CCMA on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.					

Hyper-V mid-range virtual machine specification

The following table specifies the minimum Hyper-V resources for an Avaya Aura® Contact Center mid-range virtual machine. These are the minimum specifications for Avaya Aura® Contact Center Release 7.0 for the mid-range virtual machine in order to support the rated capacities.

Resource	Minimum value
Number of CPUs	24
Minimum CPU Clock speed (MHz)	2400
Processor Reservation Percentage	50%
RAM (GB)	32 GB
RAM Assignment Profile	Static
Minimum Virtual Storage (GB) - Fixed Disks	• 501 GB NTFS - Voice Contact Server • 501 GB NTFS - Network Control Center (NCC) • 601 GB NTFS - Multimedia Contact Server with 300 GB NTFS multimedia database • 901 GB NTFS - Multimedia Contact Server with recommended 600 GB NTFS multimedia database • 801 GB NTFS - Voice and Multimedia Contact Server with 300 GB NTFS multimedia database • 1101 GB NTFS - Voice and Multimedia Contact Server with recommended 600 GB NTFS multimedia database
Virtual Network Interface Cards	• 1x 1000 Mbps - for SIP OR • 2x 1000 Mbps - for CS1000

This mid-range virtual machine offers performance equivalent to the Avaya Aura® Contact Center mid-range physical server.

Virtualized high-end solution

The following table lists the installation options, maximum number of agents, and maximum call rates of a virtualized high-end Avaya Aura® Contact Center solution.

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
Voice and Multimedia Contact Server without Avaya Aura® Media Server	Aura SIP	600 Note 3	100	12K	1.2K / 2.4K
	CS 1000 AML	1000	200	20K	1.2K / 2.4K
Voice and Multimedia Contact Server with Avaya Aura® Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
Voice Contact Server Only	Aura SIP	3000 Note 3	600	45K	6.0K / 12K
	CS 1000 AML	5000	600	100K	6.0K / 12K
Multimedia Contact Server Only	Aura SIP	3000	N/A	N/A	6.0K / 12K
	CS 1000 AML	3000	N/A	N/A	6.0K / 12K
Multimedia Contact Server Only with Enterprise Web Chat	Aura SIP	3000	N/A	N/A	18K / 12K
Network Control Center Server	All switch types	Supported	600	N/A	N/A

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

- For System Contact Rate calculations, IM contacts have a weighting equivalent to one system contact. One IM contact is equivalent to one system contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, Web chat contacts count as two system contacts. One Web chat is equivalent to two system contacts.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + (Web Chat * 2))
- For System Contact Rate calculations, Enterprise Web Chat contacts count as one system contact. One Enterprise Web chat is equivalent to one system contact.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + Enterprise Web Chat)
- *Route to CDN* and *Transfer/Conference to CDN* each count as two calls.

Note 2: Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Standard Web chats per hour (WCph). Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes. Enterprise Web Chat supports up to 3000 concurrent sessions.

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate Note 1	Maximum multimedia rate (WCph/Eph) Note 2
Note 3: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on a high-end Voice Contact Server, Avaya Aura® Contact Center supports 1500 Agent Desktops and 1500 Agent Browser applications. **Note:** Reduce capacity by 35 percent if you are recording all calls. Reduce by (the percentage of calls being recorded) X (35 percent) if you are using sampled recording. **Note:** Avaya Aura® Contact Center High Availability is supported on high-end servers. **Note:** To achieve the stated capacities, configure your sever hardware for maximum performance. For more information, see Server performance and firmware settings on page 256. **Note:** You can use the instance of CCMA on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.					

Hyper-V high-end virtual machine specification

The following table specifies the minimum Hyper-V resources for an Avaya Aura® Contact Center high-end virtual machine. These are the minimum specifications for Avaya Aura® Contact Center Release 7.0 for the high-end virtual machine in order to support the rated capacities.

Resource	Minimum value
Number of CPUs	38
Minimum CPU Clock speed (MHz)	2400
Processor Reservation Percentage	50%
RAM (GB)	32 GB
RAM Assignment Profile	Static
Minimum Virtual Storage (GB) - Fixed Disks	• 501 GB NTFS - Voice Contact Server • 501 GB NTFS - Network Control Center (NCC) • 601 GB NTFS - Multimedia Contact Server with 300 GB NTFS multimedia database • 901 GB NTFS - Multimedia Contact Server with recommended 600 GB NTFS multimedia database • 801 GB NTFS - Voice and Multimedia Contact Server with 300 GB NTFS multimedia database • 1101 GB NTFS - Voice and Multimedia Contact Server with recommended 600 GB NTFS multimedia database
Virtual Network Interface Cards	• 1x 1000 Mbps - for SIP OR • 2x 1000 Mbps - for CS1000

This high-end virtual machine offers performance equivalent to the Avaya Aura® Contact Center high-end physical server.

Contact Center virtual machine hard disks and partitions

Create individual virtual hard disks for each of the required partitions for your Contact Center virtual machine. When creating a virtual hard disk for the Operating System partition, create a hard disk size 1GB greater that the required partition size to accommodate any additional Windows partitions that the Windows Server 2012 R2 install might create automatically.

For example, for an Operating System partition size requirement of 80GB, create an 81GB virtual hard drive. For each additional Contact Center partition, create a virtual hard drive greater than or equal to the partition size requirement. The virtual hard disk must be of sufficient size such that when the associated partition is created and formatted for it has a size matching the required NTFS partition size.

For improved multimedia offline data retention, Avaya recommends using a 600 GB partition for multimedia storage. The multimedia 600 GB partition requires SAN Storage.

Table 28: Contact Center Virtual Machine hard disk minimum partition sizes

Hard disk drive partition description	Drive letter	Minimum partition sizes for Voice Contact Server / NCC	Minimum partition sizes for Multimedia Contact Server with 300 GB multimedia partition	Recommended partition sizes for Multimedia Contact Server with 600 GB multimedia partition	Minimum partition sizes for Voice and Multimedia Contact Server 300 GB multimedia partition	Recommended partition sizes for Voice and Multimedia Contact Server with 600 GB multimedia partition
Operating System drive	C:	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition
Application drive	D:	120 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition
DVD drive	E:	—	—	—	—	—
Voice database drive	F:	200 GB NTFS partition	—	—	200 GB NTFS partition	200 GB NTFS partition
Multimedia database drive	G:	—	300 GB NTFS partition	600 GB NTFS partition	300 GB NTFS partition	600 GB NTFS partition
Database journal drive	H:	100 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition
	Total	501 GB of disk space	601 GB of disk space	901 GB of disk space	801 GB of disk space	1101 GB of disk space on a SAN

If using 900 GB Raid–1 disks, use the above Minimum Partition size option. Contact Center requires Hardware RAID-1 with duplicate hard disk drives with identical specifications. Therefore, the host server must implement Hardware RAID-1 or better.

Hyper-V server minimum CPU specification

Configure each Hyper-V virtual machine with the CPU resources to support Avaya Aura® Contact Center. For each virtual machine and required agent count, configure a specified number of vCPU cores and CPU Reservations in MHz.

Avaya Aura® Contact Center Hyper-V profiling uses a Dual 8-core Intel Xeon E5-2670 2.60GHz CPU as a reference CPU. This reference processor has 16 physical CPU cores. Each of these 16 cores has an individual benchmark value that is one sixteenth of the overall benchmark score of the reference processor. You use this individual core benchmark value to compare the cores from different processors and to select suitable Hyper-V host hardware for Avaya Aura® Contact Center virtualization.

The individual core benchmark value for the processor in your Hyper-V host server must be equal to or greater than 90% of the individual core benchmark value for the Avaya Aura® Contact Center reference processor.

Follow these steps to ensure your proposed Hyper-V host CPUs meet the Contact Center minimum requirements.

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the reference CPU: Dual 8-core Intel Xeon E5-2670 2.60GHz.

  Reference individual core benchmark value = (Reference CPU benchmark from website / Number of cores in reference CPU)

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for your Hyper-V host server CPU.

  Individual core benchmark value = (Your host server CPU benchmark from website / Number of cores in host server CPU)

- To support Contact Center virtualization, the individual core benchmark value of your Hyper-V host must be equal to or greater than 90% of the reference individual core benchmark value.

To support Contact Center, your Hyper-V host must have a sufficient number of CPU cores each with at least the minimum individual core benchmark value.

Hyper-V host server resource management and monitoring

When Avaya Aura® Contact Center is virtualized and commissioned, continue to monitor and manage its real-time Hyper-V resources.

- The Hyper-V host server must not be overcommitted. The total number of vCPUs assigned across all virtual machines must be less than the host's logical core count.
- Depending on your solution requirements, your Contact Center virtual machine might need additional RAM.

- The Hyper-V host server must not be over-committed in terms of RAM. Static RAM assignment required. Contact Center does not support Dynamic RAM.
- If the total average CPU usage spikes above 50% for sustained periods, add additional CPU resources to the Contact Center virtual machine.
- If Contact Center virtual machine monitoring indicates resource starvation, add additional resources as necessary.
- Depending on your solution's call complexity, you might need to add additional Hyper-V resources as necessary.
- Depending on your solution's administration and reporting requirements, you might need to add additional Hyper-V resources as necessary. Avaya recommends running large or complex reports during off-peaks hours.
- The supported agent counts and associated contact processing is modelled using simple contact processing with moderate reporting and administration.
- Contact Center supports Hyper-V Checkpoints but only during a maintenance window. Delete all checkpoints before returning to production.

Chapter 24: High Availability server requirements

Avaya Aura® Contact Center supports campus High Availability for fault tolerant and mission critical contact centers. You can configure your contact center to have no single point of failure. Contact Center supports the following levels of campus high availability:

- Mission Critical High Availability for SIP-enabled contact centers
- Hot-standby High Availability for AML-based contact centers

Contact Center also supports geographic high availability for data resiliency and disaster recovery.

This section provides information about standby server, Remote Geographic Node server, and network requirements. This section also describes how to optimize the Contact Center Mission Critical High Availability (HA) feature for your network.

Mission Critical High Availability

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

- Mission Critical HA with Avaya Aura® platform resiliency
- Mission Critical HA without Avaya Aura® platform resiliency
- Mission Critical HA with Midsize Enterprise

To achieve the highest level of Mission Critical High Availability, with Avaya Aura® 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. A Voice and Multimedia Contact Server supports fewer agents than a separate Voice Contact Server and Multimedia Contact Server.

- Two or more Avaya Aura® Media Server Linux-based servers, configured as High Availability pairs.

  Only Linux-based Avaya Aura® Media Servers support High Availability.
- If you are using Avaya WebLM server for licensing, two Virtualized Environment (VE) deployments of Avaya WebLM server.
- Two Avaya Aura® Session Manager instances.
- Two Avaya Aura® Application Enablement Services servers configured as a High Availability pair.
- Two Avaya Aura® Communication Manager servers configured as a High Availability pair.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

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. A Voice and Multimedia Contact Server supports fewer agents than a separate Voice Contact Server and Multimedia Contact Server.
- Two or more Avaya Aura® Media Server Linux-based servers, configured as High Availability pairs.

  Only Linux-based Avaya Aura® Media Servers support High Availability.
- If you are using Avaya WebLM server for licensing, two Virtualized Environment (VE) deployments of Avaya WebLM server.
- 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, because 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.

To achieve Mission Critical High Availability using Midsize Enterprise 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. A Voice and Multimedia Contact Server supports fewer agents than a separate Voice Contact Server and Multimedia Contact Server.

- Two or more Avaya Aura® Media Server Linux-based servers, configured as High Availability pairs.

  Only Linux-based Avaya Aura® Media Servers support High Availability.
- If you are using Avaya WebLM server for licensing, two Virtualized Environment (VE) deployments of Avaya WebLM server.
- Two Midsize Enterprise servers, configured for High Availability.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

In a Mission Critical HA solution, all of the above components must be in the same network subnet or campus network location. 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. 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.

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.

Hot-standby High Availability

To achieve Hot-standby High Availability with no single point of failure you must have an AML-based 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. A Voice and Multimedia Contact Server supports fewer agents than a separate Voice Contact Server and Multimedia Contact Server.
- Avaya Communication Server 1000 High Availability PBX.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

All of the above components must be in the same network subnet or campus network location.

Avaya Aura® Contact Center supports hot-standby High Availability (HA) resiliency for Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Multimedia (CCMM).

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. All Avaya Agent Desktop clients must be registered in this domain, or in domains with a two-way trust relationship with this Contact Center server domain.

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.

Avaya Aura® Unified Communications platform and Contact Center High Availability

Avaya Aura® Contact Center supports High Availability when using an Avaya Aura® Unified Communications platform. The level of High Availability supported depends on your entire solution, including the Unified Communications platform release, patch level, and installation type.

Contact Center High Availability is supported with the following platforms:

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

  OR

- Avaya Aura® Solution for Midsize Enterprise (ME) 6.2 FP4.

  Note:

  The Avaya Aura® Solution for Midsize Enterprise (ME) does not support geographic High Availability. Both ME servers must be in close proximity (within 100 meters) so that they can be connected with an Ethernet crossover cable.

For more information about the Unified Communications platform, including the required patch levels, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

The following table lists the level of Contact Center application High Availability supported for each Avaya Aura® Unified Communications platform release and installation type.

Table 29: Avaya Aura® Unified Communications platform HA support level summary

PABX	Release	HA Level	Agent experience after Contact Center switchover
Avaya Aura® CM/SM/AES	6.2, 7.0.x, 7.1	Mission Critical HA	Agent logon state is maintained.

PABX	Release	HA Level	Agent experience after Contact Center switchover
ME	6.2 FP4	Mission Critical HA	Agent logon state is maintained.
Avaya Aura® Unified Communications Virtualized Environment (VE)	6.2, 7.0.x, 7.1	Contact Center supports High Availability without AES resiliency	Agent logon state is maintained.
Important: If a Contact Center application or server fails, Mission Critical High Availability maintains voice calls in progress between customers and agents.			

Avaya Communication Server 1000 and Contact Center High Availability

Avaya Aura® Contact Center supports High Availability when using an Avaya Communication Server 1000 PABX. The level of High Availability supported depends on your entire solution, including the Avaya Communication Server 1000 release and installation type.

In AML-based Hot-standby High Availability solutions, if a Contact Center application or server fails, High Availability maintains calls in progress between customers and agents, but agents must manually log back on again after the switchover.

The following table lists the level of Contact Center application High Availability supported for each Avaya Communication Server 1000 release and installation type.

Table 30: Avaya Communication Server 1000 High Availability support level summary

CS 1000 Release	HA Level	Agent experience after switchover
7.6	Hot-standby HA	Agents log back on.
Important: If a Contact Center application or server fails, Hot-standby High Availability maintains voice calls in progress between customers and agents.		

High Availability levels supported

The level of Contact Center application High Availability supported depends on your entire solution, including the PABX platform.

The following table lists the level of Contact Center application High Availability supported for each PABX release and installation type.

Table 31: Contact Center application High Availability support level summary

PABX	Release	AML/SIP	HA Level	Agent Experience after switchover
Avaya Aura® CM/SM/AES	6.2 FP4, 7.0.x, 7.1	SIP	Mission Critical HA	Agent logon state is maintained.
ME[Note 1]	6.2 FP4	SIP	Mission Critical HA	Agent logon state is maintained.
CS 1000	7.6	AML	Hot-standby HA	Agents log back on.

[Note 1] In total, if the active ME server fails, it can take up to ten minutes for a switchover/failover on the ME to complete. If an active Contact Center application fails, the switchover to the standby server completes in seconds.

Important:

If a Contact Center application or server fails, High Availability maintains voice calls in progress between customers and agents.

Standby server requirements

The standby server specification must match the active server. The standby server must have the same hard disk partitions, the same amount of memory, and the same CPU type. The standby server must have the Contact Center software installed on the same partitions as the active server. The active and standby servers must have the same patch level and the same operating system updates.

If the active and standby Avaya Aura® Contact Center servers are virtualized, they must be on different VMware host servers. Both VMware host servers must use the same version of VMware. The virtualized active and standby servers must have the same VMware virtual machine configuration settings.

Important:

In a SIP-enabled contact center using an Avaya Aura® Unified Communications platform and High Availability resiliency, the active and standby CCMS servers must both have TLS certificates in place to communicate securely with the Avaya Aura® Unified Communications platform and to support High Availability switchover.

Remote Geographic Node server requirements

The High Availability feature supports Remote Geographic Nodes. Remote Geographic Nodes are similar to the standby servers but they only shadow data from the active server; Remote Geographic Nodes do not automatically take over if the active system fails. If the standby server and active

server are in the same building, then a Remote Geographic Node on remote site provides additional data protection by maintaining a remote copy of the configuration and statistical information.

The Remote Geographic Node server hardware specification must be equal to or greater than the active server hardware specification. The Remote Geographic Node server must have the same hard disk partitions, the same amount of memory, the same CPU type, and the same Operating System patches. The Remote Geographic Node server must have the Contact Center software installed on the same partitions as the active server, and it must be patched to the same level. The active and Remote Geographic Node servers must have the same operating system updates and the same operating system patch level.

If the active and Remote Geographic Node Contact Center servers are virtualized, they must be on different VMware host servers. Both VMware host servers must use the same version of VMware. The virtualized active and Remote Geographic Node servers must have the same VMware virtual machine configuration settings.

Campus network configuration

Contact Center uses a managed IP address for campus High Availability. A managed IP address is a virtual IP address hosted on the NIC of the currently active server. Both the active and standby servers also have a static IP address. You configure the static IP address of each server in the Windows operating system. You configure the Managed IP address in the Contact Center High Availability configuration interface.

To eliminate network points of failure in the Contact Center solution, you must use Link Aggregation Control Protocol (LACP), NIC Teaming, and Virtual Router Redundancy Protocol (VRRP).

Dynamic Host Configuration Protocol (DHCP):

Contact Center server applications do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Link Aggregation Control Protocol:

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

NIC teaming:

NIC teaming is the process of grouping together several physical NICs into one single logical NIC, which can be used for network fault tolerance and transmit load balancing. By teaming more than one physical NIC to a logical NIC, high availability is maximized. Even if one NIC fails, the network connection does not cease and continues to operate on other NICs.

Virtual Router Redundancy Protocol (VRRP):

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. Two or more physical routers,

such as Avaya ERS 5520, can be configured to stand for a virtual router. If one physical router fails, another physical router automatically replaces it.

Campus High Availability supports LAN environments where the round trip delay is less than 80ms, with less than 0.5% packet loss.

Geographic network configuration

If you have Contact Center HA at the campus, configure the Remote Geographic Node to communicate with the Managed IP address at the campus site.

To eliminate network points of failure in the contact center solution, you must use Link Aggregation Control Protocol (LACP), NIC Teaming and Virtual Router Redundancy Protocol (VRRP).

Dynamic Host Configuration Protocol (DHCP):

Contact Center server applications do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Link Aggregation Control Protocol:

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

NIC teaming:

NIC teaming is the process of grouping together several physical NICs into one single logical NIC, which can be used for network fault tolerance and transmit load balancing. By teaming more than one physical NIC to a logical NIC, high availability is maximized. Even if one NIC fails, the network connection does not cease and continues to operate on other NICs.

Virtual Router Redundancy Protocol (VRRP):

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. Two or more physical routers, such as Avaya ERS 5520, can be configured to stand for a virtual router. If one physical router fails, another physical router automatically replaces it.

Geographic High Availability supports WAN environments where the round trip delay is less than 80ms, with less than 0.5% packet loss.

Chapter 25: Voice and Multimedia Contact Server without Avaya Aura® Media Server configuration requirements

This section provides the configuration requirements for a Voice and Multimedia Contact Server without Avaya Aura® Media Server. Install this server to provide context-sensitive and skill-based routing for customer voice and multimedia contacts. This server provides routed contact support for voice calls, email messages, Web communications, voice mail messages, scanned documents, fax messages, and SMS text messages. SIP-enabled Voice and Multimedia Contact Server also supports Instant Message (IM) contact routing. This server provides extensive tools for agent management, real-time and historical reporting, and graphical tools to create contact flows and treatment rules. Use this server for license management, High Availability configuration, networking, Open Interfaces Web Service and third-party application interfaces integration.

This server includes the following Avaya Aura® Contact Center components:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Avaya Aura® Contact Center Orchestration Designer (OD)
- Contact Center Multimedia (CCMM)

Voice and Multimedia Contact Server without Avaya Aura® Media Server is supported only on the Microsoft Windows Server 2012 Release 2 operating system.

Voice and Multimedia Contact Server without Avaya Aura® Media Server supports High Availability.

If you access Contact Center Manager Administration from a browser on the server, Avaya recommends that you limit the number of on-demand and scheduled historical reports run on the server. Running historical reports can increase the CPU usage on the server. In addition, Avaya recommends that you limit the number of real-time displays that you start. Viewing real-time displays also increases the CPU usage on the server.

You can use the instance of Contact Center Manager Administration on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.

In a small to medium solution using one of these servers, agents download and install Agent Desktop software from this server.

In a voice-only solution, multimedia contacts are not supported. Therefore, in a voice-only solution without multimedia licenses, the CCMM Administration utility blocks access to the multimedia features and functions. In a voice-only solution that uses Agent Desktop, use the CCMM Administration utility to configure Agent Desktop features and functions.

To enable the multimedia features in the CCMM Administration utility, obtain and install a multimedia-enabled Avaya Aura® Contact Center license. Once you have obtained a multimedia license, install the new license file on the server, and reconfigure the Contact Center Manager Server server and license settings. You must also refresh all the servers in Contact Center Manager Administration. Once you have installed a multimedia-enabled license, the system enables all the multimedia features and functions.

Operating System requirements

Configure the Microsoft Windows Server 2012 Release 2 operating system to support Avaya Aura® Contact Center. For more information, see Windows Server 2012 R2 common specifications on page 245.

Server requirements

The Voice and Multimedia Contact Server without Avaya Aura® Media Server server specification depends on your solution type, agent count, and call flow rate. You can install the Voice and Multimedia Contact Server without Avaya Aura® Media Server software on a physical server or on a virtual machine.

Avaya Aura® Contact Center defines three server specification levels based on agent count and call flow rates: Entry-level, Mid-range, and High-end. The following table shows the server specification levels supported by Voice and Multimedia Contact Server without Avaya Aura® Media Server.

Table 32: Voice and Multimedia Contact Server without Avaya Aura® Media Server supported server specifications

Platform	Physical Server			VMware virtual machine			Hyper–V virtual machine		
Solution level	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes

Platform	Physical Server			VMware virtual machine			Hyper–V virtual machine		
CS 1000 AML	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes

For more information about Avaya Aura® Contact Center physical server specifications, see Physical server specifications on page 261.

For more information about Avaya Aura® Contact Center VMware virtual machine specifications, see VMware Virtual Machine specifications on page 292.

For more information about Avaya Aura® Contact Center Hyper–V virtual machine specifications, see Hyper-V virtualization support on page 322.

Communication Control Toolkit components

The Communication Control Toolkit simplifies integration. The transport components provide firewall friendliness, Network Address Translation (NAT), and Citrix support. The server components enable open telephone switch connectivity.

The Communication Control Toolkit consists of Avaya developed software and third-party components, as described in this section.

Important:

Q Signaling (QSIG) Path Replacement and Trunk Anti Tromboning is not supported in Communication Control Toolkit.

Client application

Client applications are third-party components and can include the following:

- software phones
- agent telephony toolbars with screen pop-ups
- intelligent call management applications

Important:

TAPI legacy clients are not supported.

Communication Control Toolkit server

The component that manages client sessions consists of the following subcomponents:

- Contact Management Framework—An infrastructure component that manages the states of contacts, agents, terminals, and addresses.
- TAPI Connector—An application that converts Communication Control Toolkit requests to TAPI API calls, and TAPI events to Communication Control Toolkit events. The TAPI Connector resides between the TAPI Service Provider and the Contact Management Framework. This service is installed only in AML-based solutions.

- TAPI Service Provider—A Microsoft TAPI client responsible for CTI operations of all lines controlled by the Communication Control Toolkit platform initialized by TAPI. This service is installed only in AML-based solutions.
- Communication Control Toolkit API—An API that controls voice resources. The API is published as Microsoft .NET types and distributed as a Windows assembly, which is referenced by application developers.

Communication Control Toolkit supported functionality

The tables in this section specify which functions are supported by Communication Control Toolkit. Avaya Agent Desktop is a client of Communication Control Toolkit.

Important:

If your phone supports Multiple Appearance Reduction Prime (MARP) of Multiple Appearance Directory Number (MADN) you must disable the configurations. These configurations are not supported in Communication Control Toolkit.

Important:

In SIP-enabled contact centers, 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).
- 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).

The following tables list the basic Communication Control Toolkit call control functions.

Table 33: Basic Communication Control Toolkit and Avaya Agent Desktop functions

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Make Call	Yes	Yes
Hold Current Call	Yes	Yes The CS 1000 Swap Hold switch feature is not supported.
Unhold Call	Yes (Retrieve Call)	Yes (Retrieve Call)
Drop Current Call (Release)	Yes	Yes
Blind Transfer Call	No	Yes
Initiate Supervised Transfer	Yes	Yes

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Complete Transfer	Yes	Yes
Initiate Conference Call	Yes	Yes (up to six parties)
Complete Conference Call	Yes	Yes
Call Forward	No	Yes
Cancel Call Forward	No	Yes
Join Conference	Yes	No
Deflect Calls	No	No
Get Status	Yes	Yes
Get Call Capabilities	Yes	Yes
Get Data	Yes	Yes
Delete Data	Yes	Yes
Append Data	Yes	Yes
Make Set Busy (Do Not Disturb)	No	Yes (on Agent Terminals only)
Get/Set UUI	Yes	No (UUI attached as call data)
Send DTMF (for example, credit card number to IVR)	Yes	Yes
Mute/Unmute	Yes (if logged on in My Computer mode)	No
Consult	Yes	Yes (but must designate as transfer or conference)
Park/Unpark	No	No
Message Waiting Indicator	No	No
HER (Host Enhanced Routing)	No	Yes
Answer	Yes	Yes

The fast transfer functionality does not support completing a fast transfer call to an external trunk number. This functionality is for predictive dialing environments in which the application sends a MakeCall request to an external customer number and, when the customer answers, the application sends the FastTransfer request to blind transfer the customer to a live agent.

The following table lists the Contact Center specific functions supported by Avaya Agent Desktop and Communication Control Toolkit.

Table 34: Contact Center-specific functions

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Agent Login	Yes	Yes
Agent Logout	Yes	Yes

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Set Ready	Yes	Yes
Set Not Ready	Yes	Yes
ACD Set Activity Code	Yes	Yes
ACD Set Not Ready/Reason Code	Yes	Yes
ACD Set After Call Work Item Code	Yes	Yes
Work Ready Key support	No	No
Agent Whisper	Yes	No
Observe call	Yes	No
Set Call treatment	No	Yes
Barge In	Yes	No
Call Supervisor	Yes	Yes
Emergency Key	Yes	Yes
Redirect to another skillset	No (must transfer to a CDN)	No
Return a call to the queue skillset that it came from	No	No
Redirect to another skillset	No	No
Return a call to the queue skillset that it came from	No	No

The following table indicates which events are delivered by Communication Control Toolkit.

Table 35: Communication Control Toolkit events

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Ringing Event	Yes	Yes
Dialtone Event	No	No
Busy Event	No	No
Offering Event	Yes	Yes
Ringback Event	Yes	Yes
Inbound Connected Event	Yes	Yes
Outbound Connected Event	Yes	Partial
Connected Event	Yes	Yes
Disconnected Event	Yes	Yes
Held Event	Yes	Yes
Unheld Event	Yes	Yes
OnHold Pending Conference Event	Yes	Yes

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Onhold Pending Transfer Event	Yes	Yes
Transferred Event	Yes	Yes
Conference Event	Yes	Yes
Initiated Transfer Event	Yes	Yes
Initiated Conference Event	Yes	Yes
Session Disconnect Event (includes shutdown)	Yes	Yes
Device Forward Event	No	No
Status Change Event	Yes	Yes
Notice Message Waiting Event	No	No
Notice No Message Waiting Event	No	No
Agent Logged out Event	Yes	Yes
Agent Logged in Event	Yes	Yes
Agent Ready Event	Yes	Yes
Agent Not Ready Event	Yes	Yes
Agent Busy Event	No	No
Agent Work Ready Event	No	No
Activity Code Entered	Yes	Yes
WalkAway Activated	No	No
WalkAway Return	No	No
Emergency Invoked	No	No
Call Supervisor Invoked	No	No

Client Terminal Relationships

AML-based Communication Control Toolkit supports a maximum of 5000 client-to-terminal relationships.

- A client monitoring a voice device (see voice terminal control capacity specification below)
- A client monitoring a multimedia terminal (see CCMM terminal control capacity specification below)

If a client monitors voice and multimedia terminals, each pair of voice + multimedia terminals are counted once; for example,

1 voice terminal + 1 multimedia terminal = 1

2 voice terminals + 1 multimedia terminal = 2

2 voice terminals + 2 multimedia terminals = 2

2 voice terminals + 3 multimedia terminals = 3

AML-based Communication Control Toolkit supports a maximum of 5000 CTI client-to-telephony device relationships where the CTI client-to-telephony device relationship is defined as a CTI client (CCT client or TAPI client) that monitors and controls a telephony device. A telephony device refers to one of the following:

- A CCT Voice Terminal (TN)
- A CCT RoutePointAddress (CDN)
- CCMM terminal control capacity

Communication Control Toolkit clients can monitor or control a multimedia terminal. A multimedia terminal is created dynamically when a Contact Center agent that is configured with one or more multimedia contact types logs on.

The following are some examples of configurations.

- 5000 CCT clients, each monitoring and controlling a single Terminal (5000 CTI clients x 1 telephony device = 5000)
- 1 CCT client monitoring and controlling 5000 Terminals (1 CTI client x 5000 telephony devices = 5000)
- 100 CCT clients, each monitoring and controlling 10 Terminals (100 CTI clients x 10 telephony devices = 1000)

Voice and multimedia

- 2750 CCT clients, each monitoring and controlling a single voice terminal + 600 CCT Clients each controlling a single multimedia terminal
- 2750 CCT clients, each monitoring and controlling a single voice terminal + 600 CCT Clients, each monitoring a single voice terminal and a single multimedia terminal

Email message memory requirements

In contact center solutions that support the email contact type, you must engineer your server to support email attachments.

The maximum attachment size formulas use the following variables and the approximate values, to calculate how much memory to reserve to process an email message.

Variable	Description	Value
Encoding adjustment	The factor by which the attachment size increases when the attachment is encoded and attached to an email message.	1.3 (this can vary slightly based on the encoding used)

Variable	Description	Value
Memory adjustment	The factor by which the encoded size increases when an email message is loaded into the internal representation of the email message in memory.	1.2 (this factor decreases slightly, the larger the email is, but it remains as a fixed value)
Buffer memory	The memory, which is fairly static, required by the parts of the application not involved in processing inbound email messages.	20 MB

When the following sections specify an attachment size, they mean the total size of all attachments of an email message. Also, the size of the body of an email lowers the supported attachment size by the size of the content of the message. In most cases, the content of an email is negligible compared to large attachments.

JVM size – Buffer memory / Memory adjustment / Encoding adjustment = Maximum attachment size

JVM sizes (MB)	Maximum attachment sizes (MB)
128	69.2
256 (default)	151.3
512	315.4
1024	643.6

Minimum JVM size formula

Attachment size * Encoding adjustment * Memory adjustment + Buffer memory = Minimum JVM size

Attachment sizes (MB)	Minimum JVM sizes (MB)
10	35.6
20	51.2
30	66.8
40	82.4
50	98
60	113.6
70	129.2
80	144.8
90	160.4
100	176
500	800

Calculating disk storage requirements

This section lists the database files used by Contact Center Multimedia and provides database capacity calculations.

Required database files

Contact Center Multimedia includes the following database files:

- CACHE.DAT in the `<Database Drive>:Avaya\Contact Center\Databases\CCMM \MULTIMEDIA\DATA` folder. This stores the two CACHE.DAT Contact Center Multimedia folders and files, one for code and one for data.
- `Avaya\Contact Center\Databases\Journals` folder is created during installation. This folder contains the Database Journal Files used for High Availability.

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

The CACHE.DAT file grows dynamically as the volume of data in the database grows. Initially it is just under 45 MB. One million contacts take approximately 20GB of space.

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 20GB space.

Email attachment storage

Email attachments are stored in the attachment folder. The 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
   * number of days before purging
```

Example

Following is the 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, and attachments are stored for 10 days before they are deleted.

```
Disk space for email attachments in MB
   = 9 000 * 0.3 * 0.5 * 10
   = 13500 MB
```

Network configuration

This section describes network configuration information for Communication Control Toolkit.

Network interface card binding order

Configure the binding order of the network interface cards so that the NIC connected to the contact center subnet is first, followed by others such as the virtual adapters for remote access.

Maximum acceptable use

Total usage of the Enterprise IP network must not exceed 30 percent in a shared network environment. Communication Control Toolkit use of the Enterprise IP network can be as high as 9 percent for a system with 500 agents. Ensure that the Enterprise IP network has enough spare capacity to accommodate Communication Control Toolkit traffic in addition to your traffic.

Contact modeling limitations in a network environment

Some limitations exist in the information you can model the Communication Control Toolkit when you deal with networked call scenarios.

Contact modeling

Conference calls that involve parties from more than one networked switch cannot be completely represented on each Communication Control Toolkit (CCT) system. Each CCT system can model only the parties that it has direct visibility with. For instance, consider a conference call involving parties A, B, and C, where A and B are on CCT 1 and party C is on CCT 2. If party B is the conference controller (initiated the conference with party C), then from the perspective of CCT 1 shows a three-party call with parties A, B, and C involved. However, the perspective of CCT 2 shows only a two-party call with B and C involved with B as the calling address and C as the called address.

Third-party software requirements

This section describes the third-party software requirements for the Voice and Multimedia Contact Server.

Warning:

You must install and actively manage a spam filter to remove spam messages from all contact center mailboxes. Unsolicited bulk spam messages to your Contact Center, if not filtered out, can impact performance or can cause damage to your contact center solution.

Important:

If your contact center uses an Avaya Aura® Communication Manager, Avaya Agent Desktop client computers do not support the following applications running concurrently with Avaya Agent Desktop:

- Avaya one-X® Communicator, if the administrator has enabled your Avaya Agent Desktop embedded softphone.
- IP Agent.
- IP Softphone.
- Any other non-Avaya softphone applications.
- Avaya one-X® Agent. In a Multimedia-only Contact Center deployment, where the Contact Center agents are configured for Multimedia contact types only, running Avaya Agent Desktop concurrently with Avaya one-X® Agent on a client computer is supported.

Third-party backup software

Two types of backups are available on Contact Center Manager Server:

- Full (offline) backup
- Database (online) backup

Use third-party backup software only for full (offline) backups. To create a full backup, you must use a third-party backup utility such as Microsoft backup utility. See the third-party documentation for information about the full backup procedure, and *Avaya Aura® Contact Center Server Administration* for information about procedures that you must perform before a full backup. If you use a third-party backup utility, it must comply with the general third-party software guidelines specified in Third-party software requirements on page 253.

You must shut down all Contact Center Manager Server services before you perform a full backup. Some third-party backup utilities can provide an online backup of all files, Contact Center Manager Server does not support an online backup from these third-party backup utilities.

Avaya recommends that you back up your database daily.

If you plan to back up your Contact Center Multimedia database across the network, be aware that disk capacity affects the speed of the backup and restore. To reduce the speed of a database back up or restore, follow disk capacity requirements on the remote locations.

Voice and Multimedia Contact Server antivirus software

This section describes the Voice and Multimedia Contact Server antivirus software requirements.

For antivirus software requirements, see Additional guidelines for the use of antivirus software on page 254.

Several maintenance tasks are automatically activated at 12:00 midnight. Therefore, you must schedule virus scans at a time other than midnight.

Exclude the following files and folders from scans (both real-time and scheduled):

- Exclude all files of type LOG, or exclude all files with a specific extension “*.log”. Avaya recommends this setting when your antivirus application supports it.
- `F:\Avaya\Contact Center\Database\` (including sub-directories)
- *<additional database drive>*`:\Avaya\Contact Center\Databases\` (including sub-directories)
- `C:\Avaya\Logs\` (including sub-directories)
- `D:\Avaya\Logs\` (including sub-directories)
- `D:\Avaya\Contact Center\` (including sub-directories)
- The Avaya log Archive folder. Generally, `D:\Avaya\Logs\Archive\`
- `D:\Avaya\Cache\CacheSys\mgr\Backup\`
- `cache.dat`. Exclude all files named `cache.dat` in any directory or sub-directory (use your antivirus wildcard convention)
- The folder where you store Service Packs and patches

Contact Center Multimedia interacts with an external email system and enables agents to send attachment files from their computers to the Contact Center Multimedia server. Both methods of retrieving data are potential sources of software infection.

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the email server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Contact Center Multimedia server do not have a virus. Contact Center Multimedia does not block specific attachment file types. Third-party antivirus software must be installed on the Portal Server according to guidelines in this document for such utilities.
- Exclude the Contact Center Multimedia partition from being scanned.
- Ensure the antivirus software is configured to permit outbound email messages. For example, configure the McAfee antivirus software *Access Protection* option not to block *Prevent mass mailing worms from sending mail*. Alternatively, add the Contact Center Multimedia “EmailManager.exe” process to the McAfee *Processes to exclude* list.
- If firewalls on individual computers are enabled on the Agent Desktop computer, the Report Listener might be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.
- You must not enable the Microsoft Updater to Auto-Run. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

Warning:

Running a Virus Scan on the Contact Center Multimedia attachment folder, which contains thousands of files, can use significant CPU time on a server and can cause drastic slowdown in agent's response times. Avaya recommends that you run scans, if necessary, during off-peak hours.

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in `<Install_drive>:\Avaya\Cache\CacheSys`. Databases and journal files are installed in `<Install_drive>:\Avaya\Contact Center\Databases`.

Chapter 26: Voice Contact Server configuration requirements

This section provides the configuration requirements for a Voice Contact Server. Install this server to provide context-sensitive and skill-based routing for customer voice and multimedia contacts. This server provides extensive tools for agent management, real-time and historical reporting, and graphical tools to create contact flows and treatment rules. Use this server for license management, High Availability configuration, networking, Open Interfaces Web Service and third-party application interfaces integration.

This server includes the following Avaya Aura® Contact Center components:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Avaya Aura® Contact Center Orchestration Designer (OD)

Voice Contact Server is supported only on the Microsoft Windows Server 2012 Release 2 operating system.

Voice Contact Server supports High Availability.

If you access Contact Center Manager Administration from a browser on the server, Avaya recommends that you limit the number of on-demand and scheduled historical reports run on the server. Running historical reports can increase the CPU usage on the server. In addition, Avaya recommends that you limit the number of real-time displays that you start. Viewing real-time displays also increases the CPU usage on the server.

You can use the instance of Contact Center Manager Administration on this server to manage the agents and supervisors associated with this server or with remote CCMS servers up to the maximum supervisor capacity for this server.

Operating System requirements

Configure the Microsoft Windows Server 2012 Release 2 operating system to support Avaya Aura® Contact Center. For more information, see Windows Server 2012 R2 common specifications on page 245.

Server requirements

The Voice Contact Server server specification depends on your agent count, and call flow rate. You can install Voice Contact Server software on a physical server or on a virtual machine.

Avaya Aura® Contact Center defines three server specification levels based on agent count and call flow rates: Entry-level, Mid-range, and High-end. The following table shows the server specification levels supported by Voice Contact Server.

Table 36: Voice Contact Server supported server specifications

Platform	Physical server			VMware virtual machine			Hyper–V virtual machine		
Solution level	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CS 1000 AML	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

For more information about Avaya Aura® Contact Center physical server specifications, see Physical server specifications on page 261.

For more information about Avaya Aura® Contact Center VMware virtual machine specifications, see VMware Virtual Machine specifications on page 292.

For more information about Avaya Aura® Contact Center Hyper–V virtual machine specifications, see Hyper-V virtualization support on page 322.

Communication Control Toolkit components

The Communication Control Toolkit simplifies integration. The transport components provide firewall friendliness, Network Address Translation (NAT), and Citrix support. The server components enable open telephone switch connectivity.

The Communication Control Toolkit consists of Avaya developed software and third-party components, as described in this section.

Important:

Q Signaling (QSIG) Path Replacement and Trunk Anti Tromboning is not supported in Communication Control Toolkit.

Client application

Client applications are third-party components and can include the following:

- software phones
- agent telephony toolbars with screen pop-ups
- intelligent call management applications

Important:

TAPI legacy clients are not supported.

Communication Control Toolkit server

The component that manages client sessions consists of the following subcomponents:

- Contact Management Framework—An infrastructure component that manages the states of contacts, agents, terminals, and addresses.
- TAPI Connector—An application that converts Communication Control Toolkit requests to TAPI API calls, and TAPI events to Communication Control Toolkit events. The TAPI Connector resides between the TAPI Service Provider and the Contact Management Framework. This service is installed only in AML-based solutions.
- TAPI Service Provider—A Microsoft TAPI client responsible for CTI operations of all lines controlled by the Communication Control Toolkit platform initialized by TAPI. This service is installed only in AML-based solutions.
- Communication Control Toolkit API—An API that controls voice resources. The API is published as Microsoft .NET types and distributed as a Windows assembly, which is referenced by application developers.

Communication Control Toolkit supported functionality

The tables in this section specify which functions are supported by Communication Control Toolkit. Avaya Agent Desktop is a client of Communication Control Toolkit.

Important:

If your phone supports Multiple Appearance Reduction Prime (MARP) of Multiple Appearance Directory Number (MADN) you must disable the configurations. These configurations are not supported in Communication Control Toolkit.

Important:

In SIP-enabled contact centers, 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).
- 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).

The following tables list the basic Communication Control Toolkit call control functions.

Table 37: Basic Communication Control Toolkit and Avaya Agent Desktop functions

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Make Call	Yes	Yes
Hold Current Call	Yes	Yes The CS 1000 Swap Hold switch feature is not supported.
Unhold Call	Yes (Retrieve Call)	Yes (Retrieve Call)
Drop Current Call (Release)	Yes	Yes
Blind Transfer Call	No	Yes
Initiate Supervised Transfer	Yes	Yes
Complete Transfer	Yes	Yes
Initiate Conference Call	Yes	Yes (up to six parties)
Complete Conference Call	Yes	Yes
Call Forward	No	Yes
Cancel Call Forward	No	Yes
Join Conference	Yes	No
Deflect Calls	No	No
Get Status	Yes	Yes
Get Call Capabilities	Yes	Yes
Get Data	Yes	Yes
Delete Data	Yes	Yes
Append Data	Yes	Yes
Make Set Busy (Do Not Disturb)	No	Yes (on Agent Terminals only)
Get/Set UUI	Yes	No (UUI attached as call data)

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Send DTMF (for example, credit card number to IVR)	Yes	Yes
Mute/Unmute	Yes (if logged on in My Computer mode)	No
Consult	Yes	Yes (but must designate as transfer or conference)
Park/Unpark	No	No
Message Waiting Indicator	No	No
HER (Host Enhanced Routing)	No	Yes
Answer	Yes	Yes

The fast transfer functionality does not support completing a fast transfer call to an external trunk number. This functionality is for predictive dialing environments in which the application sends a MakeCall request to an external customer number and, when the customer answers, the application sends the FastTransfer request to blind transfer the customer to a live agent.

The following table lists the Contact Center specific functions supported by Avaya Agent Desktop and Communication Control Toolkit.

Table 38: Contact Center-specific functions

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Agent Login	Yes	Yes
Agent Logout	Yes	Yes
Set Ready	Yes	Yes
Set Not Ready	Yes	Yes
ACD Set Activity Code	Yes	Yes
ACD Set Not Ready/Reason Code	Yes	Yes
ACD Set After Call Work Item Code	Yes	Yes
Work Ready Key support	No	No
Agent Whisper	Yes	No
Observe call	Yes	No
Set Call treatment	No	Yes
Barge In	Yes	No
Call Supervisor	Yes	Yes
Emergency Key	Yes	Yes
Redirect to another skillset	No (must transfer to a CDN)	No
Return a call to the queue skillset that it came from	No	No

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Redirect to another skillset	No	No
Return a call to the queue skillset that it came from	No	No

The following table indicates which events are delivered by Communication Control Toolkit.

Table 39: Communication Control Toolkit events

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Ringing Event	Yes	Yes
Dialtone Event	No	No
Busy Event	No	No
Offering Event	Yes	Yes
Ringback Event	Yes	Yes
Inbound Connected Event	Yes	Yes
Outbound Connected Event	Yes	Partial
Connected Event	Yes	Yes
Disconnected Event	Yes	Yes
Held Event	Yes	Yes
Unheld Event	Yes	Yes
OnHold Pending Conference Event	Yes	Yes
Onhold Pending Transfer Event	Yes	Yes
Transferred Event	Yes	Yes
Conference Event	Yes	Yes
Initiated Transfer Event	Yes	Yes
Initiated Conference Event	Yes	Yes
Session Disconnect Event (includes shutdown)	Yes	Yes
Device Forward Event	No	No
Status Change Event	Yes	Yes
Notice Message Waiting Event	No	No
Notice No Message Waiting Event	No	No
Agent Logged out Event	Yes	Yes
Agent Logged in Event	Yes	Yes
Agent Ready Event	Yes	Yes
Agent Not Ready Event	Yes	Yes

Event	SIP-enabled Avaya Aura®	AML-based CS 1000
Agent Busy Event	No	No
Agent Work Ready Event	No	No
Activity Code Entered	Yes	Yes
WalkAway Activated	No	No
WalkAway Return	No	No
Emergency Invoked	No	No
Call Supervisor Invoked	No	No

Client Terminal Relationships

AML-based Communication Control Toolkit supports a maximum of 5000 client-to-terminal relationships.

- A client monitoring a voice device (see voice terminal control capacity specification below)
- A client monitoring a multimedia terminal (see CCMM terminal control capacity specification below)

If a client monitors voice and multimedia terminals, each pair of voice + multimedia terminals are counted once; for example,

1 voice terminal + 1 multimedia terminal = 1

2 voice terminals + 1 multimedia terminal = 2

2 voice terminals + 2 multimedia terminals = 2

2 voice terminals + 3 multimedia terminals = 3

AML-based Communication Control Toolkit supports a maximum of 5000 CTI client-to-telephony device relationships where the CTI client-to-telephony device relationship is defined as a CTI client (CCT client or TAPI client) that monitors and controls a telephony device. A telephony device refers to one of the following:

- A CCT Voice Terminal (TN)
- A CCT RoutePointAddress (CDN)
- CCMM terminal control capacity

Communication Control Toolkit clients can monitor or control a multimedia terminal. A multimedia terminal is created dynamically when a Contact Center agent that is configured with one or more multimedia contact types logs on.

The following are some examples of configurations.

- 5000 CCT clients, each monitoring and controlling a single Terminal (5000 CTI clients x 1 telephony device = 5000)

- 1 CCT client monitoring and controlling 5000 Terminals (1 CTI client x 5000 telephony devices = 5000)
- 100 CCT clients, each monitoring and controlling 10 Terminals (100 CTI clients x 10 telephony devices = 1000)

Voice and multimedia

- 2750 CCT clients, each monitoring and controlling a single voice terminal + 600 CCT Clients each controlling a single multimedia terminal
- 2750 CCT clients, each monitoring and controlling a single voice terminal + 600 CCT Clients, each monitoring a single voice terminal and a single multimedia terminal

Network configuration

This section describes network configuration information for Communication Control Toolkit.

Network interface card binding order

Configure the binding order of the network interface cards so that the NIC connected to the contact center subnet is first, followed by others such as the virtual adapters for remote access.

Maximum acceptable use

Total usage of the Enterprise IP network must not exceed 30 percent in a shared network environment. Communication Control Toolkit use of the Enterprise IP network can be as high as 9 percent for a system with 500 agents. Ensure that the Enterprise IP network has enough spare capacity to accommodate Communication Control Toolkit traffic in addition to your traffic.

Contact modeling limitations in a network environment

Some limitations exist in the information you can model the Communication Control Toolkit when you deal with networked call scenarios.

Contact modeling

Conference calls that involve parties from more than one networked switch cannot be completely represented on each Communication Control Toolkit (CCT) system. Each CCT system can model only the parties that it has direct visibility with. For instance, consider a conference call involving

parties A, B, and C, where A and B are on CCT 1 and party C is on CCT 2. If party B is the conference controller (initiated the conference with party C), then from the perspective of CCT 1 shows a three-party call with parties A, B, and C involved. However, the perspective of CCT 2 shows only a two-party call with B and C involved with B as the calling address and C as the called address.

Third-party software requirements

This section describes the third-party software requirements for the Voice and Multimedia Contact Server.

Warning:

You must install and actively manage a spam filter to remove spam messages from all contact center mailboxes. Unsolicited bulk spam messages to your Contact Center, if not filtered out, can impact performance or can cause damage to your contact center solution.

Important:

If your contact center uses an Avaya Aura® Communication Manager, Avaya Agent Desktop client computers do not support the following applications running concurrently with Avaya Agent Desktop:

- Avaya one-X® Communicator, if the administrator has enabled your Avaya Agent Desktop embedded softphone.
- IP Agent.
- IP Softphone.
- Any other non-Avaya softphone applications.
- Avaya one-X® Agent. In a Multimedia-only Contact Center deployment, where the Contact Center agents are configured for Multimedia contact types only, running Avaya Agent Desktop concurrently with Avaya one-X® Agent on a client computer is supported.

Third-party backup software

Two types of backups are available on Contact Center Manager Server:

- Full (offline) backup
- Database (online) backup

Use third-party backup software only for full (offline) backups. To create a full backup, you must use a third-party backup utility such as Microsoft backup utility. See the third-party documentation for information about the full backup procedure, and *Avaya Aura® Contact Center Server Administration* for information about procedures that you must perform before a full backup. If you use a third-party

backup utility, it must comply with the general third-party software guidelines specified in Third-party software requirements on page 253.

You must shut down all Contact Center Manager Server services before you perform a full backup. Some third-party backup utilities can provide an online backup of all files, Contact Center Manager Server does not support an online backup from these third-party backup utilities.

Avaya recommends that you back up your database daily.

If you plan to back up your Contact Center Multimedia database across the network, be aware that disk capacity affects the speed of the backup and restore. To reduce the speed of a database back up or restore, follow disk capacity requirements on the remote locations.

Voice Contact Server antivirus software

This section describes the Voice Contact Server antivirus software requirements.

For antivirus software requirements, see Additional guidelines for the use of antivirus software on page 254.

Several maintenance tasks are automatically activated at 12:00 midnight. Therefore, you must schedule virus scans at a time other than midnight.

Avaya recommends that you exclude the following files and folders from scans (both real-time and scheduled):

- Exclude all files of type LOG, or exclude all files with a specific extension “*.log”. Avaya recommends this setting when your antivirus application supports it.
- `F:\Avaya\Contact Center\Database\` (including sub-directories)
- *<additional database drive>*`:\Avaya\Contact Center\Databases\` (including sub-directories)
- `C:\Avaya\Logs\` (including sub-directories)
- `D:\Avaya\Logs\` (including sub-directories)
- `D:\Avaya\Contact Center\Common Components\CMF\logs\`
- `D:\Avaya\Contact Center\Manager Server\iccm\data\` (including sub-directories)
- `D:\Avaya\Contact Center\Manager Server\iccm\logs\` (including sub-directories)
- `D:\Avaya\Contact Center\Manager Server\iccm\sgm\config\`
- The Avaya log Archive folder. Generally, `D:\Avaya\Logs\Archive\`
- `D:\Avaya\Cache\CacheSys\mgr\Backup\`
- `D:\Avaya\Contact Center\apache-tomcat\logs\`
- `D:\Avaya\Contact Center\Manager Administration\Apps\` (including sub-directories)

- `cache.dat`. Exclude all files named `cache.dat` in any directory or sub-directory (use your antivirus wildcard convention)
- The folder where you store Service Packs and patches

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in `<Install_drive>:\Avaya\Cache\CacheSys`. Databases and journal files are installed in `<Install_drive>:\Avaya\Contact Center\Databases`.

Chapter 27: Multimedia Contact Server configuration requirements

This section provides the configuration requirements for a Multimedia Contact Server. Install this server to increase the number of contact center agents in your enterprise solution. When installed, this server provides the multimedia contact processing capabilities, and the Voice and Multimedia Contact Server processes only voice contacts.

This server provides routed contact support for voice calls, email messages, instant messages (IMs), Web communications, voice mail messages, scanned documents, fax messages, and SMS text messages.

This server includes the following Avaya Aura® Contact Center components:

- Contact Center Multimedia (CCMM)

Multimedia Contact Server is supported only on the Microsoft Windows Server 2012 Release 2 operating system. Multimedia Contact Server supports High Availability.

In a solution using one of these servers, agents download and install Agent Desktop software from this server.

In a solution where agents use Agent Desktop to log on and handle customer calls, each Voice Contact Server requires one Multimedia Contact Server. In a SIP-enabled voice contact center solution, agents must use Agent Desktop to log on and handle customer calls. Therefore each SIP-enabled voice solution using a Voice Contact Server also requires one Multimedia Contact Server.

In an Avaya Communication Server 1000 AML-based voice-only solution, where agents use Agent Desktop to log on and handle customer calls, each Voice Contact Server requires one Multimedia Contact Server. In an Avaya Communication Server 1000 AML-based voice-only solution, where agents use their desk phones to log on and handle customer calls, and where the agents do not use Agent Desktop, a Multimedia Contact Server is not required.

In a voice-only solution, multimedia contacts are not supported. Therefore, in a voice-only solution without multimedia licenses, the CCMM Administration utility blocks access to the multimedia features and functions. In a voice-only solution that uses Agent Desktop, use the CCMM Administration utility to configure Agent Desktop features and functions.

To enable the multimedia features in the CCMM Administration utility, obtain and install a multimedia-enabled Avaya Aura® Contact Center license. Once you have obtained a multimedia license, install the new license file on the server, and reconfigure the Contact Center Manager Server server and license settings. You must also refresh all the servers in Contact Center Manager

Administration. Once you have installed a multimedia-enabled license, the system enables all the multimedia features and functions.

Operating System requirements

Configure the Microsoft Windows Server 2012 Release 2 operating system to support Avaya Aura® Contact Center. For more information, see Windows Server 2012 R2 common specifications on page 245.

Server requirements

The Multimedia Contact Server server specification depends on your solution type, agent count, and call flow rate. You can install Multimedia Contact Server software on a physical server or on a virtual machine.

Avaya Aura® Contact Center defines three server specification levels based on agent count and call flow rates: Entry-level, Mid-range, and High-end. The following table shows the server specification levels supported by Multimedia Contact Server.

Table 40: Multimedia Contact Server supported server specifications

Platform	Physical server			VMware virtual machine			Hyper—V virtual machine		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CS 1000 AML	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

For more information about Avaya Aura® Contact Center physical server specifications, see Physical server specifications on page 261.

For more information about Avaya Aura® Contact Center VMware virtual machine specifications, see VMware Virtual Machine specifications on page 292.

For more information about Avaya Aura® Contact Center Hyper–V virtual machine specifications, see Hyper-V virtualization support on page 322.

Email message memory requirements

In contact center solutions that support the email contact type, you must engineer your server to support email attachments.

The maximum attachment size formulas use the following variables and the approximate values, to calculate how much memory to reserve to process an email message.

Variable	Description	Value
Encoding adjustment	The factor by which the attachment size increases when the attachment is encoded and attached to an email message.	1.3 (this can vary slightly based on the encoding used)
Memory adjustment	The factor by which the encoded size increases when an email message is loaded into the internal representation of the email message in memory.	1.2 (this factor decreases slightly, the larger the email is, but it remains as a fixed value)
Buffer memory	The memory, which is fairly static, required by the parts of the application not involved in processing inbound email messages.	20 MB

When the following sections specify an attachment size, they mean the total size of all attachments of an email message. Also, the size of the body of an email lowers the supported attachment size by the size of the content of the message. In most cases, the content of an email is negligible compared to large attachments.

JVM size – Buffer memory / Memory adjustment / Encoding adjustment = Maximum attachment size

JVM sizes (MB)	Maximum attachment sizes (MB)
128	69.2
256 (default)	151.3
512	315.4
1024	643.6

Minimum JVM size formula

Attachment size * Encoding adjustment * Memory adjustment + Buffer memory = Minimum JVM size

Attachment sizes (MB)	Minimum JVM sizes (MB)
10	35.6
20	51.2
30	66.8
40	82.4
50	98

Attachment sizes (MB)	Minimum JVM sizes (MB)
60	113.6
70	129.2
80	144.8
90	160.4
100	176
500	800

Calculating disk storage requirements

This section lists the database files used by Contact Center Multimedia and provides database capacity calculations.

Required database files

Contact Center Multimedia includes the following database files:

- CACHE.DAT in the *<Database Drive>*:Avaya\Contact Center\Databases\CCMM \MULTIMEDIA\DATA folder. This stores the two CACHE.DAT Contact Center Multimedia folders and files, one for code and one for data.
- Avaya\Contact Center\Databases\Journals folder is created during installation. This folder contains the Database Journal Files used for High Availability.

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

The CACHE.DAT file grows dynamically as the volume of data in the database grows. Initially it is just under 45 MB. One million contacts take approximately 20GB of space.

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 20GB space.

Email attachment storage

Email attachments are stored in the attachment folder. The 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
   * number of days before purging
```

Example

Following is the 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, and attachments are stored for 10 days before they are deleted.

```
Disk space for email attachments in MB
   = 9 000 * 0.3 * 0.5 * 10
   = 13500 MB
```

Third-party software requirements

This section describes the third-party software requirements for the Voice and Multimedia Contact Server.

Warning:

You must install and actively manage a spam filter to remove spam messages from all contact center mailboxes. Unsolicited bulk spam messages to your Contact Center, if not filtered out, can impact performance or can cause damage to your contact center solution.

Important:

If your contact center uses an Avaya Aura® Communication Manager, Avaya Agent Desktop client computers do not support the following applications running concurrently with Avaya Agent Desktop:

- Avaya one-X® Communicator, if the administrator has enabled your Avaya Agent Desktop embedded softphone.
- IP Agent.
- IP Softphone.
- Any other non-Avaya softphone applications.
- Avaya one-X® Agent. In a Multimedia-only Contact Center deployment, where the Contact Center agents are configured for Multimedia contact types only, running Avaya Agent Desktop concurrently with Avaya one-X® Agent on a client computer is supported.

Third-party backup software

Two types of backups are available on Contact Center Manager Server:

- Full (offline) backup
- Database (online) backup

Use third-party backup software only for full (offline) backups. To create a full backup, you must use a third-party backup utility such as Microsoft backup utility. See the third-party documentation for information about the full backup procedure, and *Avaya Aura® Contact Center Server Administration* for information about procedures that you must perform before a full backup. If you use a third-party

backup utility, it must comply with the general third-party software guidelines specified in Third-party software requirements on page 253.

You must shut down all Contact Center Manager Server services before you perform a full backup. Some third-party backup utilities can provide an online backup of all files, Contact Center Manager Server does not support an online backup from these third-party backup utilities.

Avaya recommends that you back up your database daily.

If you plan to back up your Contact Center Multimedia database across the network, be aware that disk capacity affects the speed of the backup and restore. To reduce the speed of a database back up or restore, follow disk capacity requirements on the remote locations.

Multimedia Contact Server antivirus software

Contact Center Multimedia interacts with an external email system and enables agents to send attachment files from their computers to the Contact Center Multimedia server. Both methods of retrieving data are potential sources of software infection.

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the email server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Contact Center Multimedia server do not have a virus. Contact Center Multimedia does not block specific attachment file types. Third-party antivirus software must be installed on the Portal Server according to guidelines in this document for such utilities.
- Exclude the following folders from scans, both real-time and scheduled: `D:\Avaya\Contact Center\` (including sub-directories).
- Exclude the Contact Center Multimedia partition from being scanned.
- Ensure the antivirus software is configured to permit outbound email messages. For example, configure the McAfee antivirus software *Access Protection* option not to block *Prevent mass mailing worms from sending mail*. Alternatively, add the Contact Center Multimedia “EmailManager.exe” process to the McAfee *Processes to exclude* list.
- If firewalls on individual computers are enabled on the Agent Desktop computer, the Report Listener might be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.
- You must not enable the Microsoft Updater to Auto-Run. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

  Warning:

  Running a Virus Scan on the Contact Center Multimedia attachment folder, which contains thousands of files, can use significant CPU time on a server and can cause drastic

slowdown in agent's response times. Avaya recommends that you run scans, if necessary, during off-peak hours.

Avaya recommends that you exclude the following files and folders from scans (both real-time and scheduled):

- The folder where you store Service Packs and patches

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in `<Install_drive>:\Avaya\Cache\CacheSys`. Databases and journal files are installed in `<Install_drive>:\Avaya\Contact Center\Databases`.

Chapter 28: Voice and Multimedia Contact Server with Avaya Aura® Media Server configuration requirements

This section provides the configuration requirements for a Voice and Multimedia Contact Server with Avaya Aura® Media Server. Install this server to provide context-sensitive and skill-based routing for customer voice and multimedia contacts. This server provides routed contact support for voice calls, email messages, Web communications, voice mail messages, scanned documents, fax messages, and SMS text messages. SIP-enabled Voice and Multimedia Contact Server also supports Instant Message (IM) contact routing. This server provides extensive tools for agent management, real-time and historical reporting, and graphical tools to create contact flows and treatment rules. Use this server for license management, networking, Open Interfaces Web Service and third-party application interfaces integration.

This server includes the following Avaya Aura® Contact Center components:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Avaya Aura® Contact Center Orchestration Designer (OD)
- Contact Center Multimedia (CCMM)
- Avaya Aura® Media Server (Avaya Aura® MS)

Voice and Multimedia Contact Server with Avaya Aura® Media Server is supported only on the Microsoft Windows Server 2012 Release 2 operating system.

The Voice and Multimedia Contact Server with Avaya Aura® Media Server server does not support High Availability. This server type does not support virtualization.

If you access Contact Center Manager Administration from a browser on the server, Avaya recommends that you limit the number of on-demand and scheduled historical reports run on the server. Running historical reports can increase the CPU usage on the server. In addition, Avaya recommends that you limit the number of real-time displays that you start. Viewing real-time displays also increases the CPU usage on the server.

You can use the instance of Contact Center Manager Administration on this server to create reports only for this server. You can use the instance of Contact Center Manager Administration on this server to manage agents and supervisors only for this server. Do not use Contact Center Manager Administration on this server to manage or create reports for other servers.

In a small to medium solution using one of these servers, agents download and install Agent Desktop software from this server.

In a voice-only solution, multimedia contacts are not supported. Therefore, in a voice-only solution without multimedia licenses, the CCMM Administration utility blocks access to the multimedia features and functions. In a voice-only solution that uses Agent Desktop, use the CCMM Administration utility to configure Agent Desktop features and functions.

To enable the multimedia features in the CCMM Administration utility, obtain and install a multimedia-enabled Avaya Aura® Contact Center license. Once you have obtained a multimedia license, install the new license file on the server, and reconfigure the Contact Center Manager Server server and license settings. You must also refresh all the servers in Contact Center Manager Administration. Once you have installed a multimedia-enabled license, the system enables all the multimedia features and functions.

Operating System requirements

Configure the Microsoft Windows Server 2012 Release 2 operating system to support Avaya Aura® Contact Center. For more information, see Windows Server 2012 R2 common specifications on page 245.

Server requirements

The Voice and Multimedia Contact Server with Avaya Aura® Media Server hardware specification depends on your solution type, agent count, and call flow rate.

Note:

Voice and Multimedia Contact Server with Avaya Aura® Media Server is not supported on a virtual machine.

Avaya Aura® Contact Center defines three server specification levels based on agent count and call flow rates: Entry-level, Mid-range, and High-end. The following table shows the server specification levels supported by the Voice and Multimedia Contact Server with Avaya Aura® Media Server software.

Table 41: Voice and Multimedia Contact Server with Avaya Aura® Media Server supported server specifications

Platform	Physical Server			VMware virtual machine			Hyper–V virtual machine		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	No	Yes	Yes	No	No	No	No	No	No

For more information about Avaya Aura® Contact Center physical server specifications, see Physical server specifications on page 261.

Avaya Aura® Media Server media files and media management

Avaya Aura® Media Server media files are WAV audio files that contain speech, music, feature tones, or signaling tones. Avaya Aura® Media Server supports custom (customer generated) media files and default (canned) media files.

Use Contact Center Manager Administration (CCMA) *Prompt Management* to configure the media files for the following:

- Locale-specific voice announcement and prompt files
- Scripted music files
- Barge-in notification tone
- Observation notification tone
- Call Force Answer Zip notification tone
- Custom Zip notification tones
- Whisper Skillset announcement

Avaya Aura® Media Server provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. Create your Avaya Aura® Media Server media files using this encoding.

Content Store

The Avaya Aura® Media Server Content Store provides a persistent storage capability for configuration data and media files. You use the Contact Center Manager Administration (CCMA) *Prompt Management* interface to configure and manage the contents of the Content Store. If you have more than one Avaya Aura® Media Server, you can designate one server to be the primary Avaya Aura® Media Server. You can then configure the other Avaya Aura® Media Servers to replicate (copy) the configuration data and media files from the Content Store on the primary Avaya Aura® Media Server. This configures all of the Avaya Aura® Media Servers with the same media files

and allows them to provide a pool of common media processing resources. Content Store replication also provides storage resiliency, if one Avaya Aura® Media Server fails the remaining Avaya Aura® Media Servers are configured correctly and can continue processing media and contact center calls.

Custom media

Avaya Aura® Media Server stores (customer generated) custom media files in a media Content Store. Typically, you record your own announcements and using CCMA *Prompt Management*, store the WAV media file recordings in the Avaya Aura® Media Server Content Store.

The music media files used to provide scripted music in Orchestration Designer applications are another example of custom media.

In an Avaya Aura® Media Server cluster-based solution, you configure your custom media files only on the primary Avaya Aura® Media Server Content Store. The custom media files are automatically replicated to all other Avaya Aura® Media Servers in the cluster.

In Avaya Aura® Media Server Mission Critical High Availability-based solutions, you configure your custom media files only on the primary server of the Avaya Aura® Media Server Content Store Master Pair. The custom media files are automatically replicated to the backup Avaya Aura® Media Server, and to all other Avaya Aura® Media Server High Availability pairs configured in the solution.

Custom media organization

Avaya Aura® Media Server organizes custom media in the Content Store within a content namespace. A content namespace is a logical area in the Content Store. The content namespace name must match the contact center SIP domain name; that is, the Local SIP Subscriber Domain Name in Contact Center Manager Server – Server Configuration.

Within the content namespace you use content groups to subdivide the media into logical groups. You can create locale-specific content groups for treatments such as RAN.

Avaya Aura® Media Server supports the following locales:

Locale	Language	Country
de_de	German	Germany
en_ca	English	Canada
en_gb	English	United Kingdom
en_ie	English	Ireland
en_in	English	India
en_us	English	United States
es_es	Spanish	Spain
es_mx	Spanish	Mexico
fr_ca	French	Canada
fr_fr	French	France
it_it	Italian	Italy
ja_jp	Japanese	Japan

Locale	Language	Country
ko_kr	Korean	Korea
pt_br	Portuguese	Brazil
ru_ru	Russian	Russia
zh_cn	Chinese (Simplified)	China
zh_tw	Chinese (Simplified)	Taiwan

To use treatments in Orchestration Designer (OD) flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the media files in the Avaya Aura® Media Server locale-specific content group. The OD flow applications or scripts reference these routes to access the treatment files on the Avaya Aura® Media Server.

Music media organization

Avaya Aura® Media Server stores music media files in content groups in a reserved namespace, named *streamsource*, in the Content Store. These content groups can be collections of music files of a specific genre, pop, rock, or classical for example, or any other group classification. To use scripted music in OD flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to one of the Avaya Aura® Media Server streamsource content groups. The OD flow applications or scripts reference these routes to access the scripted music provided by Avaya Aura® Media Server.

Default media files

Avaya Aura® Media Server contains a set of country and language specific default media files for all supported locales. The default media files contain numerical values, busy tones and ring-back tones. You can use these default “canned” media files in your Contact Center solution, or you can replace them with your own recordings.

The following are examples of the Avaya Aura® Media Server default or canned locale specific media files:

- Single digit playback (zero.wav, one.wav, two.wav ... nine.wav)
- Busy tone wav file (busy.wav)
- Ringback wav file (ringback.wav)

The default media files are stored in the *prompts* section of the Avaya Aura® Media Server Content Store. The canned media files are stored in Linear 16-bit PCM recording format. You use Avaya Aura® Media Server Element Manager to replace the existing default “canned” media files with your own files.

Default media files are stored in the Avaya Aura® Media Server Content Store and are therefore replicated to other Avaya Aura® Media Servers in resilient or clustered solutions.

The following languages use different WAV file names for the following numbers:

	Zero	One	Two	Three	Four	Five	Six	Seven	Eight	Nine
ja_jp Japanese	zero	ichi	ni	san	yo	go	roku	nana	hatchi	kyu

	Zero	One	Two	Three	Four	Five	Six	Seven	Eight	Nine
ko_kr Korean	young	il	yi	sam	sa	o	yuk	chil	pal	gu
zh_cn & zh_tw Chinese	ling	yi	er	san	si	wu	liu	qi	ba	jiu
ru_ru Russian	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9

All audio media files must have a .wav file name extension, for example hatchi.wav, jiu.wav, and seven.wav. The extension is removed when you upload the file using Element Manager.

Communication Control Toolkit supported SIP functionality

The tables in this section indicate which functions are supported by Communication Control Toolkit. Avaya Agent Desktop is a client of Communication Control Toolkit so they support the same features.

Important:

In SIP-enabled contact centers, 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).
- 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).

The following tables list the basic Communication Control Toolkit call control functions.

Table 42: Basic Communication Control Toolkit and Avaya Agent Desktop functions

Event	SIP-enabled Avaya Aura®
Make Call	Yes
Hold Current Call	Yes
Unhold Call	Yes (Retrieve Call)
Drop Current Call (Release)	Yes
Blind Transfer Call	No
Initiate Supervised Transfer	Yes

Event	SIP-enabled Avaya Aura®
Complete Transfer	Yes
Initiate Conference Call	Yes
Complete Conference Call	Yes
Call Forward	No
Cancel Call Forward	No
Join Conference	Yes
Deflect Calls	No
Get Status	Yes
Get Call Capabilities	Yes
Get Data	Yes
Delete Data	Yes
Append Data	Yes
Make Set Busy (Do Not Disturb)	No
Get/Set UUI	No
Send DTMF (for example, credit card number to IVR)	Yes
Mute/Unmute	Yes (on Contact Center calls only)
Consult	Yes
Park/Unpark	No
Message Waiting Indicator	No
HER (Host Enhanced Routing)	No
Answer	Yes

The fast transfer functionality does not support completing a fast transfer call to an external trunk number. This functionality is for predictive dialing environments in which the application sends a MakeCall request to an external customer number and, when the customer answers, the application sends the FastTransfer request to blind transfer the customer to a live agent.

The following table lists the Contact Center specific functions supported by Avaya Agent Desktop and Communication Control Toolkit.

Table 43: Contact Center-specific functions

Event	SIP-enabled Avaya Aura®
Agent Login	Yes
Agent Logout	Yes
Set Ready	Yes
Set Not Ready	Yes
ACD Set Activity Code	Yes
ACD Set Not Ready/Reason Code	Yes
ACD Set After Call Work Item Code	Yes

Event	SIP-enabled Avaya Aura®
Work Ready Key support	No
Agent Whisper	Yes
Observe call	Yes
Set Call treatment	Yes
Barge In	Yes
Call Supervisor	Yes
Emergency Key	Yes
Redirect to another skillset	No (must transfer to a CDN)
Return a call to the queue skillset that it came from	No
Redirect to another skillset	No
Return a call to the queue skillset that it came from	No

The following table indicates which events are delivered by Communication Control Toolkit.

Table 44: Communication Control Toolkit events

Event	SIP-enabled Avaya Aura®
Ringing Event	Yes
Dialtone Event	No
Busy Event	No
Offering Event	Yes
Ringback Event	Yes
Inbound Connected Event	Yes
Outbound Connected Event	Yes
Connected Event	Yes
Disconnected Event	Yes
Held Event	Yes
Unheld Event	Yes
OnHold Pending Conference Event	Yes
Onhold Pending Transfer Event	Yes
Transferred Event	Yes
Conference Event	Yes
Initiated Transfer Event	Yes
Initiated Conference Event	Yes
Session Disconnect Event (includes shutdown)	Yes
Device Forward Event	No
Status Change Event	Yes
Notice Message Waiting Event	No

Event	SIP-enabled Avaya Aura®
Notice No Message Waiting Event	No
Agent Logged out Event	Yes
Agent Logged in Event	Yes
Agent Ready Event	Yes
Agent Not Ready Event	Yes
Agent Busy Event	No
Agent Work Ready Event	No
Activity Code Entered	Yes
WalkAway Activated	No
WalkAway Return	No
Emergency Invoked	No
Call Supervisor Invoked	No

Email message memory requirements

In contact center solutions that support the email contact type, you must engineer your server to support email attachments.

The maximum attachment size formulas use the following variables and the approximate values, to calculate how much memory to reserve to process an email message.

Variable	Description	Value
Encoding adjustment	The factor by which the attachment size increases when the attachment is encoded and attached to an email message.	1.3 (this can vary slightly based on the encoding used)
Memory adjustment	The factor by which the encoded size increases when an email message is loaded into the internal representation of the email message in memory.	1.2 (this factor decreases slightly, the larger the email is, but it remains as a fixed value)
Buffer memory	The memory, which is fairly static, required by the parts of the application not involved in processing inbound email messages.	20 MB

When the following sections specify an attachment size, they mean the total size of all attachments of an email message. Also, the size of the body of an email lowers the supported attachment size by the size of the content of the message. In most cases, the content of an email is negligible compared to large attachments.

JVM size – Buffer memory / Memory adjustment / Encoding adjustment = Maximum attachment size

JVM sizes (MB)	Maximum attachment sizes (MB)
128	69.2
256 (default)	151.3
512	315.4
1024	643.6

Minimum JVM size formula

Attachment size * Encoding adjustment * Memory adjustment + Buffer memory = Minimum JVM size

Attachment sizes (MB)	Minimum JVM sizes (MB)
10	35.6
20	51.2
30	66.8
40	82.4
50	98
60	113.6
70	129.2
80	144.8
90	160.4
100	176
500	800

Calculating disk storage requirements

This section lists the database files used by Contact Center Multimedia and provides database capacity calculations.

Required database files

Contact Center Multimedia includes the following database files:

- CACHE.DAT in the *<Database Drive>*:Avaya\Contact Center\Databases\CCMM \MULTIMEDIA\DATA folder. This stores the two CACHE.DAT Contact Center Multimedia folders and files, one for code and one for data.
- Avaya\Contact Center\Databases\Journals folder is created during installation. This folder contains the Database Journal Files used for High Availability.

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

The CACHE.DAT file grows dynamically as the volume of data in the database grows. Initially it is just under 45 MB. One million contacts take approximately 20GB of space.

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 20GB space.

Email attachment storage

Email attachments are stored in the attachment folder. The 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
   * number of days before purging
```

Example

Following is the 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, and attachments are stored for 10 days before they are deleted.

```
Disk space for email attachments in MB
   = 9 000 * 0.3 * 0.5 * 10
   = 13500 MB
```

Third-party software requirements

This section describes the third-party software requirements for the Voice and Multimedia Contact Server.

Warning:

You must install and actively manage a spam filter to remove spam messages from all contact center mailboxes. Unsolicited bulk spam messages to your Contact Center, if not filtered out, can impact performance or can cause damage to your contact center solution.

Important:

If your contact center uses an Avaya Aura® Communication Manager, Avaya Agent Desktop client computers do not support the following applications running concurrently with Avaya Agent Desktop:

- Avaya one-X® Communicator, if the administrator has enabled your Avaya Agent Desktop embedded softphone.
- IP Agent.
- IP Softphone.
- Any other non-Avaya softphone applications.
- Avaya one-X® Agent. In a Multimedia-only Contact Center deployment, where the Contact Center agents are configured for Multimedia contact types only, running Avaya Agent Desktop concurrently with Avaya one-X® Agent on a client computer is supported.

Third-party backup software

Two types of backups are available on Contact Center Manager Server:

- Full (offline) backup
- Database (online) backup

Use third-party backup software only for full (offline) backups. To create a full backup, you must use a third-party backup utility such as Microsoft backup utility. See the third-party documentation for information about the full backup procedure, and *Avaya Aura® Contact Center Server Administration* for information about procedures that you must perform before a full backup. If you use a third-party backup utility, it must comply with the general third-party software guidelines specified in Third-party software requirements on page 253.

You must shut down all Contact Center Manager Server services before you perform a full backup. Some third-party backup utilities can provide an online backup of all files, Contact Center Manager Server does not support an online backup from these third-party backup utilities.

Avaya recommends that you back up your database daily.

If you plan to back up your Contact Center Multimedia database across the network, be aware that disk capacity affects the speed of the backup and restore. To reduce the speed of a database back up or restore, follow disk capacity requirements on the remote locations.

Voice and Multimedia Contact Server with Avaya Aura® Media Server antivirus software

This section describes the Voice and Multimedia Contact Server with Avaya Aura® Media Server antivirus software requirements.

For antivirus software requirements, see Additional guidelines for the use of antivirus software on page 254.

Several maintenance tasks are automatically activated at 12:00 midnight. Therefore, you must schedule virus scans at a time other than midnight.

Exclude the following files and folders from scans (both real-time and scheduled):

- Exclude all files of type LOG, or exclude all files with a specific extension “*.log”. Avaya recommends this setting when your antivirus application supports it.
- `F:\Avaya\Contact Center\Database\` (including sub-directories)
- `<additional database drive>:\Avaya\Contact Center\Databases\` (including sub-directories)
- `C:\Avaya\Logs\` (including sub-directories)
- `D:\Avaya\Logs\` (including sub-directories)

- `D:\Avaya\Contact Center\` (including sub-directories)
- The Avaya log Archive folder. Generally, `D:\Avaya\Logs\Archive\`
- `D:\Avaya\Cache\CacheSys\mgr\Backup\`
- `cache.dat`. Exclude all files named `cache.dat` in any directory or sub-directory (use your antivirus wildcard convention)
- The folder where you store Service Packs and patches

Contact Center Multimedia interacts with an external email system and enables agents to send attachment files from their computers to the Contact Center Multimedia server. Both methods of retrieving data are potential sources of software infection.

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the email server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Contact Center Multimedia server do not have a virus. Contact Center Multimedia does not block specific attachment file types. Third-party antivirus software must be installed on the Portal Server according to guidelines in this document for such utilities.
- Exclude the Contact Center Multimedia partition from being scanned.
- Ensure the antivirus software is configured to permit outbound email messages. For example, configure the McAfee antivirus software *Access Protection* option not to block *Prevent mass mailing worms from sending mail*. Alternatively, add the Contact Center Multimedia “EmailManager.exe” process to the McAfee *Processes to exclude* list.
- If firewalls on individual computers are enabled on the Agent Desktop computer, the Report Listener might be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.
- You must not enable the Microsoft Updater to Auto-Run. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

Warning:

Running a Virus Scan on the Contact Center Multimedia attachment folder, which contains thousands of files, can use significant CPU time on a server and can cause drastic slowdown in agent's response times. Avaya recommends that you run scans, if necessary, during off-peak hours.

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in `<Install_drive>:\Avaya\Cache\CacheSys`. Databases and journal files are installed in `<Install_drive>:\Avaya\Contact Center\Databases`.

For Avaya Aura® Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

Avaya Aura® Media Server on Windows, default locations to exclude:

- `D:\Avaya\MAS\Multimedia_Applications\MAS\platdata`
- `D:\Avaya\MAS\Multimedia_Applications\MAS\common\log`

If you do not install Avaya Aura® Media Server in the default location, adjust these file and folder paths to match your actual installation.

Chapter 29: Network Control Center server configuration requirements

This section provides the configuration requirements for a Network Control Center server. Install this server to add networking, network skill-based routing, and consolidated reporting support for a number of Voice and Multimedia Contact Servers operating as a single distributed contact center. Use this server to configure contact routing between the Voice and Multimedia Contact Server nodes of a distributed contact center solution.

This server includes the following Avaya Aura® Contact Center components:

- Contact Center Manager Server (CCMS) (Network Control Center version)
- Contact Center Manager Administration (CCMA)
- Contact Center License Manager (LM)
- Avaya Aura® Contact Center Orchestration Designer (OD)

The Network Control Center (NCC) server is supported only on the Microsoft Windows Server 2012 Release 2 operating system.

You can use the instance of Contact Center Manager Administration on this server to manage remote Contact Center Manager Server networked and not networked servers. The instance of CCMA on a Network Control Center server can administer and generate reports for a maximum of 20 CCMS servers.

Note:

All nodes in an Avaya Aura® Contact Center networking deployment, including the Network Control Center server, must be installed on operating systems from the same language family. Contact Center Manager Administration does not support displaying names from two different languages families. For example, a single Contact Center Manager Administration does not support one node with a French operating system and another node with a Russian operating system.

Note:

Avaya Aura® Contact Center supports networked calls between AML-based and SIP-enabled nodes. The Network Control Center (NCC) software must be the most recent release, relative to the other nodes on the network.

Operating System requirements

Configure the Microsoft Windows Server 2012 Release 2 operating system to support Avaya Aura® Contact Center. For more information, see Windows Server 2012 R2 common specifications on page 245.

Server requirements

The Network Control Center server specification depends on your solution type, agent count, and call flow rate. You can install Network Control Center software on a physical server or on a virtual machine.

Avaya Aura® Contact Center defines three server specification levels based on agent count and call flow rates: Entry-level, Mid-range, and High-end. The following table shows the server specification levels supported by Network Control Center.

Table 45: Network Control Center supported server specifications

Platform	Physical Server			VMware virtual machine			Hyper–V virtual machine		
Solution level	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CS 1000 AML	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

For more information about Avaya Aura® Contact Center physical server specifications, see Physical server specifications on page 261.

For more information about Avaya Aura® Contact Center VMware virtual machine specifications, see VMware Virtual Machine specifications on page 292.

For more information about Avaya Aura® Contact Center Hyper–V virtual machine specifications, see Hyper-V virtualization support on page 322.

Third-party software requirements

Due to the mission-critical, real-time processing that Avaya Aura® Contact Center applications perform, you must not install any other application class software on the server. You can install certain utility class software on the server, providing it conforms to the following guidelines, see Generic guidelines for utility-class software applications on page 253.

Network Control Center server antivirus software

This section describes the Voice and Multimedia Contact Server antivirus software requirements.

For antivirus software requirements, see Additional guidelines for the use of antivirus software on page 254.

Several maintenance tasks are automatically activated at 12:00 midnight. Therefore, you must schedule virus scans at a time other than midnight.

Avaya recommends that you exclude the following files and folders from scans (both real-time and scheduled):

- Exclude all files of type LOG, or exclude all files with a specific extension “*.log”. Avaya recommends this setting when your antivirus application supports it.
- `F:\Avaya\Contact Center\Database\` (including sub-directories)
- *<additional database drive>*`:\Avaya\Contact Center\Databases\` (including sub-directories)
- `C:\Avaya\Logs\` (including sub-directories)
- `D:\Avaya\Logs\` (including sub-directories)
- `D:\Avaya\Contact Center\Common Components\CMF\logs\`
- `D:\Avaya\Contact Center\Manager Server\iccm\data\` (including sub-directories)
- `D:\Avaya\Contact Center\Manager Server\iccm\logs\` (including sub-directories)
- `D:\Avaya\Contact Center\Manager Server\iccm\sgm\config\`
- The Avaya log Archive folder. Generally, `D:\Avaya\Logs\Archive\`
- `D:\Avaya\Cache\CacheSys\mgr\Backup\`
- `D:\Avaya\Contact Center\apache-tomcat\logs\`
- `cache.dat`. Exclude all files named `cache.dat` in any directory or sub-directory (use your antivirus wildcard convention)
- The folder where you store Service Packs and patches

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in *<Install_drive>*`:\Avaya\Cache\CacheSys`. Databases and journal files are installed in *<Install_drive>*`:\Avaya\Contact Center\Databases`.

Chapter 30: Avaya Aura® Media Server on Linux configuration requirements

This section provides the configuration requirements for an Avaya Aura® Media Server Release 7.7 Linux server. Each SIP-enabled contact center requires one or more Avaya Aura® Media Server in the solution. Avaya Aura® Media Server supports SIP-enabled voice contact routing, and it provides media processing capabilities in SIP-enabled contact centers.

Avaya Aura® Media Server is supported only in SIP-enabled contact centers.

In an Avaya Aura® Contact Center solution, Avaya Aura® Media Server uses standard Session Initiation Protocol (SIP) for signaling, and Real-time Transport Protocol (RTP) or Secure Real-time Transport Protocol (SRTP) to transport audio.

Standalone Avaya Aura® Media Server Release 7.7 is supported on the Red Hat Enterprise Linux 6.x 64-bit operating system. In a Contact Center High Availability solution, Avaya Aura® Media Server is supported only when installed standalone on a Linux operating system.

Avaya Aura® Contact Center does not support standalone Avaya Aura® Media Server on Windows.

Licensing requirements

SIP-enabled Contact Centers use WebLM licensing. When you configure a Media Server in Contact Center Manager Administration, Contact Center License Manager automatically pushes license keys to that Avaya Aura® Media Server. When Avaya Aura® Contact Center uses WebLM licensing, Avaya Aura® Media Server does not require a license file or any specific licensing configuration.

Server requirements

The Avaya Aura® Media Server server specification depends on your solution type, agent count, and call flow rate. Avaya Aura® Contact Center defines three server specification levels based on agent count and call flow rates: Entry-level, Mid-range, and High-end.

You can install Avaya Aura® Media Server software standalone on the following server specifications.

Table 46: Avaya Aura® Media Server supported server specifications

Platform	Physical Server			VMware virtual machine	
Solution level	Entry-level	Mid-range	High-end	4 vcpu guest	8 vcpu guest
Aura SIP	No	Yes	Yes	Yes	Yes
Avaya Aura® Media Server in a HA pair	No	No	Yes	Yes	Yes

Note:

Avaya Aura® Media Server is not supported on a Hyper-V virtual machine.

For more information about Avaya Aura® Media Server physical server specifications see Physical server specifications on page 261.

For more information about Avaya Aura® Media Server VMware virtual machine specifications see VMware Virtual Machine specifications on page 292.

Third-party software requirements

Due to the mission-critical, real-time processing that Avaya Aura® Contact Center applications perform, you must not install any other application class software on the server. You can install certain utility class software on the server, providing it conforms to the following guidelines, see Generic guidelines for utility-class software applications on page 253.

Antivirus software

For Avaya Aura® Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

Avaya Aura® Media Server on Linux, default locations to exclude:

- `/opt/avaya/ma/MAS/platdata`
- `/opt/avaya/ma/MAS/common/log`

If you do not install Avaya Aura® Media Server in the default location, adjust these file and folder paths to match your actual installation.

For additional antivirus software requirements, see Additional guidelines for the use of antivirus software on page 254.

Chapter 31: Administration client configuration requirements

This section provides the configuration requirements for the browser-based administration client computers. The number of these client computers is usually proportional to the number of agents in the contact center.

The following Avaya Aura® Contact Center servers use Contact Center Manager Administration and require one or more browser-based client computer:

- Voice and Multimedia Contact Server
- Voice Contact Server
- Multimedia Contact Server
- Network Control Center Server

The following Avaya Aura® Contact Center servers require one or more browser-based administration client computer:

- Avaya Aura® Media Server

Install this client computer to configure and administer Avaya Aura® Contact Center resources, to monitor performance, to generate (real-time and historical) reports. You can also use this client computer upload and download data using the Configuration Tool spreadsheets.

Client hardware requirements

The following table lists the hardware requirements for administration client.

This specification applies to the Supervisor Client PC but can also apply to computers that run Agent Desktop Displays.

Table 47: Administration client hardware requirements

Hardware item	Minimum requirements	Additional information
CPU	1 Gigahertz (GHz) or faster CPU with support for PAE, NX, and SSE2	Physical Address Extension (PAE), NX processor bit (NX), and Streaming SIMD Extensions 2 (SSE2) are features of the processor.

Hardware item	Minimum requirements	Additional information
		Dual- and quad-CPU systems are supported with or without Hyperthreading enabled. AMD processors of the same or higher specification are also supported.
RAM	1 Gigabyte (GB) (32-bit) or 2 GB (64-bit)	Additional memory is required, if you run other memory intensive applications.
Hard disk space	60 GB	60 GB is recommended only to store large reports.
Hard disk partitioning	No specific partitioning requirements	—
Hard disk speed	2.5 inch disk minimum speed: 10000 RPM 3.5 inch disk minimum speed: 7200 RPM	—
Floppy drive	Not required	If a floppy drive is installed, it must be A.
DVD ROM	Not required	
Network interface	One network interface card	100 Mb/s Ethernet or higher is recommended.
Video card	Microsoft DirectX 9 graphics device with WDDM driver	1024 x 768 pixels minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—

Client operating system requirements

The following table lists the operating system requirements for administration client computers.

Table 48: Administration client operating system requirements

Operating system	International versions supported (See Note)	Minimum service pack
Windows 7 (32-bit and 64-bit)	English	
Windows 8.1 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT)	

Operating system	International versions supported (See Note)	Minimum service pack
	Dutch (NL) LA Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN) Traditional Chinese (Zh-TW) Japanese (JA) Korean (KO)	
Windows 10 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) LA Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN) Traditional Chinese (Zh-TW) Japanese (JA) Korean (KO)	
Windows Server 2012 R2 Standard and Data center	English French (FR) German (DE) Italian (IT) Dutch (NL) LA Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN) Traditional Chinese (Zh-TW) Japanese (JA) Korean (KO)	

Operating system	International versions supported (See Note)	Minimum service pack
Note: The client operating system must be of the same language family as the associated server.		

The following table lists the compatibility between the Contact Center Manager Administration language patches and the operating system language family. Only languages compatible with the operating system language family can be enabled on the Contact Center Manager Administration server.

OS language	FR	DE	ES	PT-BR	IT	Zh-CN	Zh-TW	JA	RU	KO
English	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
Any 1 Latin language	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
Simplified Chinese	No	No	No	No	No	Yes	No	No	No	No
Traditional Chinese	No	No	No	No	No	No	Yes	No	No	No
Japanese	No	No	No	No	No	No	No	Yes	No	No
Russian	No	No	No	No	No	No	No	No	Yes	No
Korean	No	No	No	No	No	No	No	No	No	Yes

For Contact Center Manager Administration (CCMA), only languages that are compatible with the local operating system of the CCMA server can be enabled. For example, you can enable the simplified Chinese language on a simplified Chinese OS, however you cannot enable German on a simplified Chinese OS.

The CCMA client operating system must be of the same language family as the associated server. For example, if CCMA is installed on an English language OS, if Spanish and English are enabled in the CCMA Language Settings utility, and if Spanish is the preferred language in Internet Explorer on the CCMA client computer, then CCMA appears in Spanish in the CCMA client browser.

Third-party software requirements

This section describes the third-party software requirements for the administration client computer.

The following components are required on the administration client PC:

- Microsoft Internet Explorer 10.0 (32-bit version only), and 11.0 (32-bit version only).

Note:

You must run Internet Explorer in compatibility mode for Contact Center Manager Administration and Communication Control Toolkit.

- Microsoft Excel 2007 or later (for Configuration Tool only)

Contact Center Manager Administration supports only the 32-bit version of Microsoft Internet Explorer.

Contact Center Manager Administration does not support Microsoft Edge.

Administration Client Citrix support

Both Contact Center Manager Administration (CCMA) and Agent Desktop Displays (ADD) are supported in Citrix deployments. A Citrix server solution uses software to deliver on-demand Windows applications to physical desktops. This allows client users to access and use programs which are available on the Windows Server 2012 R2 operating system of the Citrix server.

Users access Contact Center Manager Administration through a Citrix client on their client computer, connecting through an Internet Explorer browser that runs on the Citrix server. The browser is available to users through a Citrix client on their client computer. In a client Citrix deployment of CCMA, you must install ActiveX controls on the Citrix server.

On the CCMA server the Agent Desktop Displays folder is typically located in:

`D:\Avaya\Contact Center\Manager Administration\Apps\ADD` folder.

You must copy this folder onto the Citrix server and install the Agent Desktop Displays application on the Citrix server. You must then configure your Citrix server to publish ADD as a published application. On the Citrix server, select the users allowed to access the ADD published application.

For more information about Citrix application publishing, see your Citrix documentation.

Contact Center Manager Administration and Agent Desktop Displays are supported only with the following versions of Citrix server:

- Citrix XenApp 6.0
- Citrix XenApp 6.5
- Citrix XenApp 7.6

Avaya Aura® Contact Center supports only the Multicast option for Real-Time Displays (RTDs) in a Citrix environment. Avaya Aura® Contact Center does not support the Unicast option for Real-Time Displays (RTDs) in a Citrix environment.

Important:

No Avaya Aura® Contact Center client components, other than Avaya Agent Desktop, Contact Center Manager Administration, and Agent Desktop Displays, are supported in a Citrix

deployment. This includes Orchestration Designer (OD), Outbound Campaign Management Tool (OCMT), and the CCMM Administration utility.

Chapter 32: Agent Desktop client requirements

This section provides the requirements for the Avaya Agent Desktop client computers. Avaya Agent Desktop is a single-interface client application used by contact center agents to interact with customers.

There are two ways in which you can deploy Avaya Agent Desktop. You can use the click-once deployment or an MSI file. With a click-once deployment, agents download and install Avaya Agent Desktop client software from an Avaya Aura® Contact Center server:

- In a small to medium solution using a Voice and Multimedia Contact Server, agents download and install Avaya Agent Desktop software from the Voice and Multimedia Contact Server.
- In a large solution using a Multimedia Contact Server, agents download and install Avaya Agent Desktop software from the Multimedia Contact Server.

In a deployment using an MSI file, administrators can push Avaya Agent Desktop to agent PCs using a silent install.

Note:

Agent Desktop does not support Network Address Translation (NAT).

Agent Desktop inter-operation with Avaya Co-Browsing Snap-in

Avaya Aura® Contact Center supports inter-operation between Agent Desktop and Avaya Co-Browsing Snap-in.

Agents engaged with a customer on a voice contact or web chat contact can initiate a Co-Browsing session by starting their browser, navigating to an Avaya Co-Browsing Snap-in URL, and generating a Co-Browsing session. The agent sends the session key to the customer, for example by calling it out in a voice call or copying it into a web chat message. The customer can join the session, and both agent and customer can utilize the Co-Browsing features.

There is no requirement for a license or any configuration in Avaya Aura® Contact Center to support inter-operation with the Avaya Co-Browsing Snap-in. You must provision and license a separate EDP stack to use Avaya Co-Browsing Snap-in.

Avaya Agent Desktop localized languages

Avaya Agent Desktop is supported in the following localized languages:

- English
- French
- German
- Italian
- LA Spanish
- Brazilian Portuguese
- Russian
- Simplified Chinese
- Traditional Chinese
- Japanese
- Korean

A single Avaya Aura® Contact Center solution, with the localization language patches installed, supports all of the Agent Desktop localized languages. For example, a single English language Voice and Multimedia Contact Server supports the English, Chinese, French, Korean, and Russian language versions of Agent Desktop client software.

To support the localized Avaya Agent Desktop client software:

1. On each Agent Desktop client computer, configure the language locale setting.
2. Download the Agent Desktop software from the Avaya Aura® Contact Center server to each client computer. The downloaded Agent Desktop package includes all of the supported languages.
3. When the agent starts Agent Desktop on the client computer, the client computer's language locale setting determines which language Agent Desktop uses. For example, client computers with a Korean language locale setting, use the Korean language version of Agent Desktop, regardless of the Avaya Aura® Contact Center server language.

Install the localization language patches to enable the supported Agent Desktop localized languages. The Avaya Aura® Contact Center language patches contain all supported languages.

Avaya Aura® Contact Center supports Agent Desktop client operating systems that use a different language family to the Contact Center server.

Client hardware requirements

Agent Desktop requires TCP/IP network access back to the Contact Center Multimedia, Contact Center Manager Administration, and Communication Control Toolkit servers— Avaya recommends 100 Mb/s connectivity.

The following table lists the hardware requirements for Agent Desktop.

Table 49: Agent Desktop client hardware requirements

Hardware item	Minimum requirements	Additional information
CPU	1 Gigahertz (GHz) or faster CPU with support for PAE, NX, and SSE2	Physical Address Extension (PAE), NX processor bit (NX), and Streaming SIMD Extensions 2 (SSE2) are features of the processor. Dual- and quad-CPU systems are supported with or without Hyper-Threading enabled. AMD processors of the same or higher specification are also supported.
RAM	1 Gigabyte (GB) (32-bit) or 2 GB (64-bit)	Additional memory is required, if you run other memory intensive applications at the same time as Agent Desktop.
Hard disk space	16 GB (32-bit) or 20 GB (64-bit)	—
Hard disk partitioning	No specific partitioning requirements	—
Hard disk speed	2.5 inch disk minimum speed: 10000 RPM 3.5 inch disk minimum speed: 7200 RPM	—
Floppy drive	Not required	If a floppy drive is installed, it must be A.
DVD ROM	Not required	
Network interface	One network interface card	100 Mb/s Ethernet or higher is recommended.
Video card	Microsoft DirectX 9 graphics device with WDDM driver	1024 x 768 pixels minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—

Client operating system requirements

The following table lists the operating system requirements for the Avaya Agent Desktop client computers.

Table 50: Avaya Agent Desktop client computer operating system requirements

Operating system	International versions supported	Minimum service pack
Microsoft Windows 7 (32-bit and 64-bit) Note 1	English French German Italian Dutch LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese Korean	—
Microsoft Windows 8.1 (32-bit and 64-bit)	English French German Italian Dutch LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese Korean	—
Microsoft Windows 10 (32-bit and 64-bit)	English French German Italian	

Operating system	International versions supported	Minimum service pack
	Dutch LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese Korean	
Note 1: If you are using Agent Desktop in *My Computer* mode on a client computer with the Microsoft Windows 7 operating system, you must install Windows 7 Service Pack 1 or later.		

Third-party software requirements

This section describes the third-party software requirements for Agent Desktop client computers.

Agent Desktop supports only Microsoft Internet Explorer 10.0 (32-bit version only), and 11.0 (32-bit version only).

Agent Desktop does not support Microsoft Edge.

If you are using the Avaya Device Media Call Control (DMCC) Call Recorder in beep tone mode, a simple call is displayed as a conference call on the agent phone, whereas Agent Desktop and Contact Center Real Time Reporting report the call as a simple two party call.

Important:

If your contact center uses an Avaya Aura® Communication Manager, Agent Desktop client computers do not support the following applications running concurrently with Agent Desktop:

- Avaya one-X® Communicator
- IP Agent
- IP Softphone
- Any other non-Avaya softphone applications
- Avaya one-X® Agent. In a Multimedia-only Contact Center deployment, where the Contact Center agents are configured for Multimedia contact types only, running Agent Desktop concurrently with Avaya one-X® Agent on a client computer is supported.

Agent Desktop uses the .NET Framework v4.5.2, the Windows Installer 4.5 Redistributable, the Microsoft Visual C++ 2005 SP1 Redistributable Package (x86), and the Microsoft Visual C++ 2008 Redistributable Package (x86). After you install these components, further client deployments are through Microsoft Internet Explorer URL or SMS deployment.

Agent Desktop headset support

Where Agent Desktop is deployed with an Avaya Aura® Communication Manager, you can use Agent Desktop in embedded soft phone mode. While using Agent Desktop in embedded soft phone mode, you can perform telephony operations (for example, call answer or hold) using buttons on certain third-party headsets. If you want to use third-party headsets to perform telephony operations, you must install the required third-party software on the client computer and you must register the headset interface dll. Avaya Aura® Contact Center includes an .msi file that performs this automatic registration. This .msi file, AAADHeadsetSupport.msi, is available at http://support.avaya.com.

For more information on registering third-party headsets, see *Avaya Aura® Contact Center Installation*.

Agent Desktop client network infrastructure requirements

Agent Desktop is a client application which communicates with several Avaya Aura® Contact Center (AACC) servers. For optimal Agent Desktop operation, the underlying contact center network infrastructure must provide adequate latency and bandwidth between the agent computer and the Contact Center servers (including, if applicable, Instant Messaging/Presence provider servers).

This section provides a high-level overview of the data that is passed between Agent Desktop and the Contact Center servers. It also sets out the recommended network values and likely impacts on agents if these values are not met. This section also describes the performance of Agent Desktop in varying Round Trip Time (RTT) and bandwidth environments.

Important:

Agent Desktop performance degrades as network Round Trip Time increases and network bandwidth decreases.

Network Latency

Network latency is a measure of the time delay experienced in a system, measured in Round Trip Time (RTT). RTT is the average Round Trip (packet) Time as measured using the ping command for a 1024-byte (1KB) data size.

For optimal performance, Avaya recommends a RTT of less than 80ms from the Agent Desktop client computer to the following Contact Center servers:

- Communications Control Toolkit (CCT) server
- Contact Center Multimedia (CCMM) server
- Contact Center Management Server (CCMS)

The RTT from the Agent Desktop client PC to the CCT and CCMM servers must be less than 120ms. For network environments with an RTT greater than 120ms, refer to the Citrix deployments of Agent Desktop in the next section. In Citrix deployments of Agent Desktop, the My Computer embedded softphone mode is not supported. In Citrix deployments, Agent Desktop can use either the Desk Phone or the Other Phone mode.

RTT impacts on Voice traffic

This section describes how the underlying RTT and latency of the network affects the experience of handling voice traffic in Agent Desktop.

Agent Desktop used with a physical desk phone

In Avaya Aura® Contact Center, the CCT server sends Computer Telephony Integration (CTI) signals to Agent Desktop, for example to prompt Agent Desktop to alert an incoming contact. These CTI signals are passed across the network as data. However, if the agent is using a physical desk phone connected to an Avaya CS 1000 or Avaya Aura® Unified Communications platform, voice packets are transported across a network using H.323 or SIP. Avaya CS 1000 deskphones that require custom data ports are isolated from the Ethernet network and these deskphones do not consume data bandwidth.

The following table details the time taken for the contact to alert on the Agent Desktop, compared to the time taken for the same contact to ring on the agent's phone, where the phone is subject to a constant RTT of 1ms.

RTT (ms)	Delay between desk phone ring and call alert on Agent Desktop	Delay between clicking Accept button on Agent Desktop and active voice path
1ms LAN	<0.5 Seconds	<0.5 Seconds
50ms	0.5 Seconds	1.0 Seconds
120ms	1.0 Seconds	2.5 Seconds

Agent Desktop used in VoIP or Softphone configuration

Where Agent Desktop is deployed with an Avaya Aura® Unified Communications platform, it can be used as a soft phone to handle the voice media stream using Voice over IP (VoIP). To use Agent Desktop as an embedded softphone, select "My Computer" mode on Agent Desktop at logon time. In softphone mode, Agent Desktop telephony is controlled by Avaya Aura® Communication Manager, so the network topology between Agent Desktop and CM must be provisioned as per standard Avaya Aura® voice provisioning.

Packet Loss impacts on VoIP quality

When using Agent Desktop with an embedded softphone in Local Area Network (LAN) or Wide Area Network (WAN) conditions, to maintain acceptable VoIP audio quality, Avaya recommends that packet loss (or jitter) is 0.5% or less.

The following tables show how Packet Loss impacts on VoIP quality and RTT between the Agent Desktop and the Communication Manager (CM) server.

Agent Desktop audio quality results at 5% jitter (E = Excellent; G = Good; F = Fair):

Packet Loss (%)	Network Latency (RTT)			
	0 ms	50 ms	100 ms	150 ms
0.0	E	E	E	E
0.5	E	E	E	E
1.0	E	E	E	E
1.5	G	G	G	G
2.0	G	G	G	G

Agent Desktop audio quality results at 10% jitter (E = Excellent; F = Fair; P = Poor):

Packet Loss (%)	Network Latency (RTT)			
	0 ms	50 ms	100 ms	150 ms
0.0	E	E	F	P
0.5	E	E	F	P
1.0	E	E	F	P
1.5	E	E	F	P
2.0	E	E	F	P

RTT impact on Multimedia Contacts

Contact Center Multimedia contacts are also affected by network latency. Agent Desktop downloads Customer contacts from the CCMM server and displays their contents as soon as they are fully retrieved.

The table below shows how varying RTTs affect multimedia contact display times – in this case, email contacts – on Agent Desktop. The “Customer Details/Customer History Display” column indicates how much time passes between the email being opened on Agent Desktop and the additional context information being loaded and displayed. These sample times are for ideal laboratory conditions.

RTT (ms)	Email Display	Customer Details/Customer History Display
1ms LAN	2 Seconds	0 Seconds
50ms	3 Seconds	Additional 3 Seconds
100ms	4 Seconds	Additional 4 Seconds
120ms	4 Seconds	Additional 5 Seconds

This data was generated using a 20KB email message, a customer history containing 30 contacts of 20KB each, in a network where bandwidth is not limiting the data transfer. Email messages of different sizes generate different results.

Bandwidth

The network bandwidth available to Agent Desktop client computers for communication with Avaya Aura® Contact Center servers is critical to Agent Desktop performance. If voice traffic is carried on the same network, this traffic is often prioritized above other network traffic – this bandwidth is therefore not available to Agent Desktop. In many cases agents use other third party applications over the same network. The bandwidth requirements of these third party applications must be considered as part of the overall bandwidth calculations (in addition to bandwidth allocated for voice soft phones and for Agent Desktop).

Several factors affect the recommended bandwidth for Agent Desktop. Depending on which Contact Center Multimedia (CCMM) features are in use on a given Customer deployment, not all factors apply. Indicative calculations to estimate the actual bandwidth usage are presented below for the various contact types and features. To calculate the required bandwidth, the relevant figures for the deployed features and supported contact types can be combined to derive an overall figure.

The network usage can be one of two types:

Constant traffic	These require dedicated, permanently available network use for the lifetime of the consumption. Examples of this type of traffic include; statistics display in Agent Desktop, update of live Web chat contacts.

	Many factors influence constant traffic levels, for example the number of agents with a large number of assigned skillsets, the number of active supervisors running RTDs in unicast mode, and large numbers of skillsets in use (large data packet) even for multicast.
Bursty traffic	The display of multimedia contacts and multimedia contact history is bursty traffic. A significant amount of data is downloaded to the Agent Desktop over a number of seconds. The frequency of these download is driven by agent activity. These require high usage of the available network for short times to download bursts of data. The time window that this data takes to download depends on the available network bandwidth at that time. Since this is not constant network consumption, a Kilo bits per second value is not reflective of the bandwidth required and a Kilo bit value has been provided instead.

Bandwidth impacts on Voice

If the agents are using a physical desk phone for voice or any other application which utilizes network bandwidth, this needs to be factored into the engineering of the network to meet the expected performance levels on Agent Desktop.

Where Agent Desktop is deployed with an Avaya Aura® Communication Manager, the Agent Desktop can be used as an embedded soft phone, handling the voice media stream as well. In softphone mode Agent Desktop communicates directly with Avaya Aura® Communication Manager, so the network topology between Agent Desktop and CM must be provisioned as per standard Aura voice provisioning.

Retrieve Customer History on voice contacts

The Agent Desktop Customer History feature enables agents to retrieve voice callers' multimedia Customer history, from the CCMM server, when a voice contact is accepted. Agent Desktop Customer History is an optional feature which is enabled in the CCMM Administration tool. These historical contacts can be of any multimedia contact type. Agent Desktop Customer History requires adequate bandwidth to function and it must be included in your network bandwidth planning calculations.

To calculate the impact of a voice callers' multimedia Customer history on bandwidth, consider voice contacts as an additional Multimedia contact type and add the number of voice contacts to your multimedia calculation for bandwidth calculations.

Multimedia Contact bandwidth requirements

This section details the bandwidth requirement of Agent Desktop Customer History for the following multimedia contact types:

- Email messages
- Fax messages
- Scanned Documents (SD)
- SMS text messages
- Outbound contacts
- Web Communications (WCs)
- Instant Messages (IMs)

This section also details the bandwidth requirement for voice contact types if multimedia history display is enabled.

Some multimedia contact supports attachments and these attachments must also be included in network calculations:

- Email contacts are of variable size. The average email size is a reasonable estimate, and is used for Agent Desktop calculations.
- Fax messages are delivered as email attachments. Fax messages must be included in the attachment size and rate estimates.
- Outbound contacts from Avaya Aura® Contact Center solution do not have attachments.
- SMS test messages from customers. SMS test messages do not have attachments.
- Web chat messages do not have attachments.
- Instant Messages (IMs) from customers do not have attachments.

The Agent Desktop Customer History feature enables agents to retrieve multimedia Customer history (containing up to 30 previous contacts), from the CCMM server, when a multimedia contact is accepted. Agent Desktop Customer History requires adequate bandwidth to function and it must be included in your network bandwidth planning calculations. Retrieving Agent Desktop Customer history from the Contact Center Multimedia (CCMM) server uses the bursty type of network data, and where the Customer history feature is enabled, it must be included in all network bandwidth calculations.

Example of calculating the bandwidth requirements of Agent Desktop Customer history downloads (based on ideal laboratory conditions):

N = Number of agents working on multimedia (MM) contacts. If the feature to display multimedia history with voice calls is activated, then N must include voice agents.

C = Maximum number of multimedia contacts per hour for the entire contact center solution. If the feature to display multimedia history with voice calls is activated, then C must include voice traffic per hour to all those agents.

avg_contact_size = average size of a contact in Kbits (not Kbytes). (Kbits = KBytes * 8). In many cases this is the average size of the incoming or outgoing email.

att_rate_in = percentage of incoming contact attachments. Contact attachments apply to email messages and fax messages.

att_rate_out = percentage of incoming email messages that are responded to with agent attached attachments in the reply.

avg_att_size = average size of an attachment in Kbits . Contact attachments apply to email messages and fax messages.

Note:

In-line attachments must also be included in the bandwidth calculations as regular attachments.

A key factor in calculating the minimum bandwidth for processing multimedia contacts is an assessment of the number of active agents that accept contacts in any one second period. The available bandwidth is shared across all of these agents in this time period.

The long term average number of agents active in any one second is calculated as follows:

$n_{average}$ = Roundup(C / 3600)

This equates to the average number of agents clicking the Accept button on the Agent Desktop at any one time. However, since the length of time it takes an agent to handle a contact is random, the number of agents clicking the Accept button is random. It is incorrect to engineer a bandwidth solution based solely on this average, as nearly 50% of the time more than $n_{average}$ agents are clicking the Accept button.

Therefore the number of active agent per second is calculated with a factor F as follows:

n_{active} = Roundup(F* C / 3600)

where F is an engineering factor between 3 and 10. A higher value for F must be used when N, the total number of agents processing multimedia contacts and multimedia history with voice contact, is lower than 50. The choice of value F is your decision. F reflects the amount of extra bandwidth to build into your network to handle both the inherently random distribution of agent activity which results in natural peaks of use and any data spike events attributable to your particular Contact Center business models, such as initial shift start times, promotions and emergencies. A higher value reduces the level of bandwidth limitation caused by the overlapping of multiple agent download of multimedia contacts.

Once F is defined, the minimum bandwidth (in Kbits per second) can be estimated as follows:

$BWMM_{min}$ =

n_{active} * ((avg_contact_size * 64) + 2000) + avg_att_size * (att_rate_in% + att_rate_out%) / 100) Kbps

Important:

The minimum recommended bandwidth available for processing multimedia contacts $BWMM_{min}$ must be greater than 10 Mbits per second.

The time to download and display contacts on Agent Desktop is directly impacted by the bandwidth available between the CCMM server and Agent Desktop at the time when the contact is accepted in Agent Desktop. The impact of bandwidth limitation is observed as a delayed display of contact and contact history in the Agent Desktop.

The following table demonstrates the impact of limiting bandwidth on multimedia contact display times on Agent Desktop. The data was generated using a 20KB email message, a Customer history of 30 contacts of 20KB size each, with a fixed RTT of 80ms.

Available bandwidth	Email display	Customer Details/Customer History Display
1Mbps	3 Seconds	Additional 6 Seconds
3Mbp	3 Seconds	Additional 3 Seconds
5Mbps	3 Seconds	Additional 2 Seconds

Retrieve Customer History on Voice contacts

This optional feature enables Agent Desktop to retrieve voice callers' multimedia Customer history (containing up to 30 previous contacts), from the CCMM server, at the time a voice contact is accepted. These historical contacts can be of any multimedia contact type. If this feature is activated, the size of this history can be added to your network planning by considering voice as an additional multimedia contact type and adding the number of voice contacts to your multimedia calculation.

Instant Messaging (IM) and Web Communication (WC) network bandwidth calculation

Processing instant messages and web communications, after they have been received by the agent requires a constant level of bandwidth.

Network usage type: Constant

c = Number of IM/WC contacts per hour

avg_session_length = Average length in seconds of IM/WC session

Data size: 50 Kbps per active IM/WC contact

IM/WC network bandwidth requirement (Kbps):

IM/WC_{BW} = (c * 50Kbps * avg_session_length)/ 3600

Presence network bandwidth calculation

Presence updates require a constant level of bandwidth.

Network usage Type: Constant

N = Number of agents working on MM contacts

avg_pres = Average number of presence updates per user per hour

Data size: 7 Kb per Presence update

Presence network bandwidth requirement (in Kbps) = (N* 7Kb * avg_pres)/ 3600

CCMM Search network bandwidth calculation

Bandwidth must be provided for an agent carrying out multimedia searches.

Network usage Type: Bursty

N = Number of agents running searches

average_search = Average number of searches per hour

Data transmitted: 1280Kb per search

CCMM Search bandwidth requirement (in Kbps) = (1280Kb * average_search * N)/3600

CCMM Pull Mode network bandwidth calculation

Pull Mode allows agents to work outside the normal Avaya Aura® Contact Center routing mode. They personally select individual contacts from the Avaya Aura® Contact Center queues. Their view of the Avaya Aura® Contact Center queue is automatically updated using the same web services as the Avaya Aura® Contact Center CCMM search feature, and so uses the same bandwidth.

N = Number of agents working in Pull Mode

c = Number of contacts per hour per agent

Data transmitted: 1280Kb per search

CCMM Pull Mode search bandwidth requirement (in Kbps) = (1280Kb * c * N)/3600

Web Statistics network bandwidth calculation

Network usage Type: Bursty

N = Number of agents

avg_skills = Average number of skillsets per agent

Data transmitted: 3.2 Kb per skillset once a minute

Web Statistics bandwidth requirement: (3.2 Kb * avg_skills * N)/60

Agent Desktop downloads by agent

Agent Desktop is a smart client which is downloaded from the CCMM server over the network onto each agent computer on initial install. On each software update (service pack or patch) the updated Agent Desktop is re-downloaded onto each agent computer. The download size is approximately 90Mbytes. The download requirements of Agent Desktop must be considered when planning the bandwidth requirements to remote agents.

Summary of total bandwidth requirements

You must sum up all the applicable bandwidth demands listed above to arrive at a minimum bandwidth for the site. Calculate the cumulative bandwidth for all multimedia features.

Example One:

```
In this example contact center the Customer has 40 agents processing both voice and
multimedia contacts.
The maximum multimedia traffic rate in any one hour is 380 multimedia contacts.
The maximum voice rate in any one hour is 200 voice contacts.
The customer has enabled the Customer history feature to display multimedia history when
voice calls are received.

This customer is using IM, Presence and Web statistics. Agent are not using Pull Mode.

Example contact center data:

N_max = 40
c = 380 multimedia contacts + 200 voice contacts = 580 per hour.
c = 580.
avg_contact_size = 10KBytes = 80Kb

avg_att_size = 0KBytes

Calculation:

    As N_max is less than 50, set F =10

    The guidance on minimum bandwidth is therefore

    n_active = 10 * 580 / 3600 = 1.61

     BWMM_min = n_active * ( (avg_contact_size * 64) + 2000) + (avg_att_size * (att_rate_in%+
att_rate_out%)/100)

     BWMM_min = 1.61 * ( (80 * 64) + 2000) + (0)

     BWMM_min = 11463.2Kbps

    11463.2Kbps / 1024 = 11.192Mbps

    This is greater than 10Mbps, so 11.192Mbps is the bandwidth for this feature.
    If BWMM_min was less than 10Mbps then set the feature bandwidth to 10Mbps.


Calculating Instant Messaging (IM) network bandwidth requirements:

    c (Number of IM contacts per hour) = 200
    avg_session_length (Average length in seconds of IM session) = 240
    Data size: 50 Kbps per active IM contact
```

```
    Network bandwidth requirement:
    Bandwidth = (c * 50Kbps * avg_session_length)/ 3600
    Bandwidth = (200 * 50Kbps * 240)/ 3600
    Bandwidth = 666 Kbs = .67 Mbps
    Bandwidth = 0.67 Mbps


Calculating Presence network bandwidth requirements:

    N (Number of agents working on MM contacts) = 40
    avg_pres (Average number of presence updates per user per hour) = 4000
    Data size: 7 Kb per Presence update

    Network bandwidth requirement:
    Bandwidth = (N* 7Kb * avg_pres)/3600
    Bandwidth = (40* 7Kb * 4000)/ 3600
    Bandwidth = 311Kbps = .311 Mbps
    Bandwidth = 0.311 Mbps


CCMM Search network bandwidth requirements:

    N (Number of agents running searches) = 40
    avg_search (Average number of searches per hour) = 12
    Data transmitted: 1280Kb per search

    Network bandwidth requirement:
    Bandwidth = (1280 * avg_search * N)/ 3600
    Bandwidth = (1280 * 12 * 40)/ 3600
    Bandwidth = 170 kbps
    Bandwidth = 0.17 Mbps


Web Statistics network bandwidth requirement:

    N (Number of agents) = 40
    avg_skills (Average number of skillsets per agent) = 25
    Data transmitted: 3.2 Kb per skillset once a minute

    Network bandwidth requirement:
    Bandwidth = (3.2 Kb * avg_skills * N)/60
    Bandwidth = 53Kbps = .053Mbps
    Bandwidth = 0.053Mbps


Total multimedia minimum network bandwidth calculation:

To calculate the total minimum network bandwidth requirement for the example customer
site, add the bandwidth (BW) requirements for each multimedia feature used.

    Feature                         Bandwidth required
    Voice                     =     As per standard Avaya provisioning
    Multimedia                =     11.19
    IM                        =     00.67
    Presence                  =     00.311
    CCMM Search               =     00.170
    Web Statistics            =     00.053

    Total                           12.4 Mbps + Voice BW + Third-party BW
```

The total minimum network bandwidth requirement for all the multimedia features on the example customer site is 12.4 Mbps.

Important:

If agents are using other applications that require network bandwidth, subtract the bandwidth these applications use from the overall bandwidth to give the available bandwidth for the Avaya Agent Desktop application.

Example Two:

In this example contact center the Customer has 100 agents processing multimedia contacts. The maximum multimedia traffic rate in any one hour is 2000 multimedia contacts.

This customer is using IM, Presence and Web statistics. Agents are not using Pull Mode.

Example contact center data:

N_{max} = 100
c = 2000 multimedia (MM) Contacts per hour.
avg_contact_size = 20KBytes = 160Kb
avg_att_size = 100KBytes = 800Kb
att_rate_in = 10%
att_rate_out = 10%

Calculation:

As N_{max} is greater than 50, set F =3

The guidance on minimum bandwidth is therefore:

n_{active} = Roundup(F* C / 3600)

n_{active} = 3 * 2000 / 3600 = 1.666

$BWMM_{min}$ = n_{active} * ((avg_contact_size * 64) + 2000) + (avg_att_size * (att_rate_in%+ att_rate_out%)/100)

$BWMM_{min}$ = 1.666 * ((160* 64) + 2000) + (800 * 0.2))

$BWMM_{min}$ = 20658.4Kbps

20658.4Kbps / 1024 = 20.17Mbps

This is greater than 10Mbps, so 20.17Mbps is the bandwidth for this feature.
If $BWMM_{min}$ was less than 10Mbps then set the feature bandwidth to 10Mbps at this stage.

Calculating Instant Messaging (IM) network bandwidth requirements:

c (Number of IM contacts per hour) = 500
avg_session_length (Average length in seconds of IM session) = 240
Data size: 50 Kbps per active IM contact

Network bandwidth requirement:
Bandwidth = (c * 50Kbps * avg_session_length)/ 3600
Bandwidth = (500 * 50Kbps * 240)/ 3600
Bandwidth = 1666.6 Kbs = 1.67 Mbps
Bandwidth = 1.67 Mbps

Calculating Presence network bandwidth requirements:

N (Number of agents working on MM contacts) = 100
avg_pres (Average number of presence updates per user per hour) = 6000

```
    Data size: 7 Kb per Presence update

    Network bandwidth requirement:
    Bandwidth = (N* 7Kb * avg_pres)/3600
    Bandwidth = (100* 7Kb * 6000)/ 3600
    Bandwidth = 1166.6Kbps = 1.17 Mbps
    Bandwidth = 1.17 Mbps


CCMM Search network bandwidth requirements:

    N (Number of agents running searches) = 100
    avg_search (Average number of searches per hour) = 12
    Data transmitted: 1280Kb per search

    Network bandwidth requirement:
    Bandwidth = (1280 * avg_search * N)/ 3600
    Bandwidth = (1280 * 12 * 100)/ 3600
    Bandwidth = 426.6 Kbps
    Bandwidth = 0.427 Mbps


Web Statistics network bandwidth requirement:

    N (Number of agents) = 100
    avg_skills (Average number of skillsets per agent) = 50
    Data transmitted: 3.2 Kb per skillset once a minute

    Network bandwidth requirement:
    Bandwidth = (3.2 Kb * 50 * 100)/60
    Bandwidth = 266Kbps = .266Mbps
    Bandwidth = 0.266Mbps


Total multimedia minimum network bandwidth calculation:

To calculate the total minimum network bandwidth requirement for the example customer
site, add the bandwidth (BW) requirements for each multimedia feature used.

    Feature                    Bandwidth required
    Voice                =     As per standard Avaya provisioning
    Multimedia           =     20.17
    IM                   =     01.67
    Presence             =     01.17
    CCMM Search          =     00.427
    Web Statistics       =     00.266

    Total                =     23.703 Mbps + Voice BW + Third-party BW
```

Reference material:

Kb = kilobit

KB = kilobyte

Kbps = kilobit per second

Mb = megabit

Mbps = megabit per second

1Mb = 1024 Kb (and 1MB = 1024 KB)

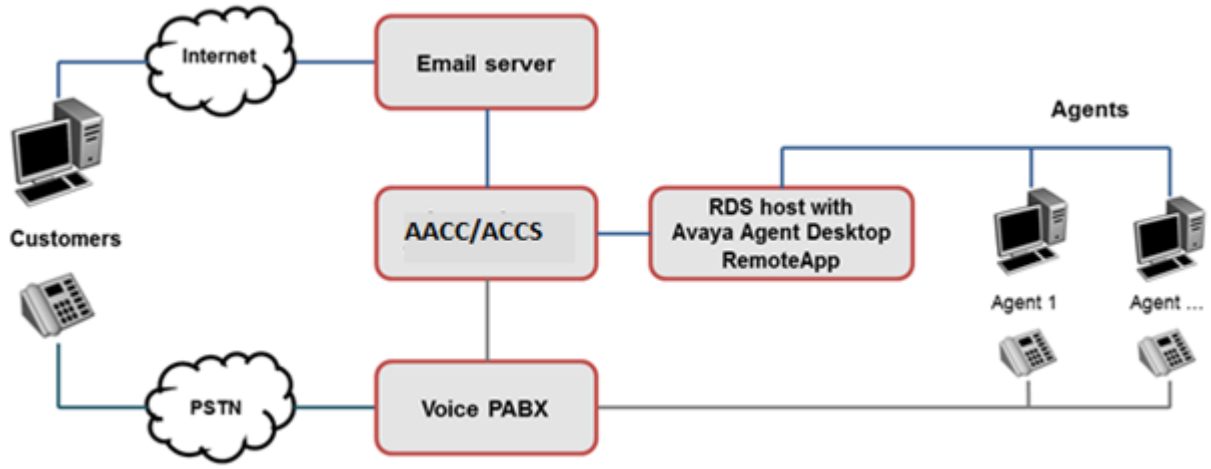
Remote Desktop Services support

Avaya Aura® Contact Center (AACC) supports using Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop.

Remote Desktop Services, formerly known as Terminal Services, allows a server to host multiple simultaneous client sessions. In the Remote Desktop Services (RDS) environment, an application runs entirely on the Remote Desktop Session Host (RD Session Host) server. The RDS client performs no local processing of application software. The server transmits the graphical user interface to the client. The client transmits the user's input back to the server. With RDS, only software user interfaces are transferred to the client system. All input from the client system is transmitted to the server, where software execution takes place.

You must use the Agent Desktop MSI package for Remote Desktop Services deployments. How you deploy and use Agent Desktop RDS clients depends on your solution requirements and virtualization infrastructure. For more information about building a client infrastructure using RDS, refer to the Microsoft Remote Desktop Services product documentation.

The following diagram shows a typical Remote Desktop Services solution with Agent Desktop hosted on the RDS Session Host server.



Remote Desktop Services requires careful up-front planning and engineering. It requires some additional maintenance and full organizational support to deliver an enterprise grade contact center agent and customer experience.

RemoteApp:

RemoteApp allows you to make programs that are accessed remotely through Remote Desktop Services appear as if they are running on the end user's local computer. These programs are referred to as RemoteApp programs. Instead of being presented to the user in the desktop of the Remote Desktop Session Host (RD Session Host) server, the RemoteApp program is integrated with the client's desktop. The RemoteApp program runs in its own resizable window, can be dragged between multiple monitors, and has its own entry in the taskbar. If a user is running more

than one RemoteApp program on the same RD Session Host server, the RemoteApp program shares the same Remote Desktop Services session.

Limitations:

The following limitations apply when you use Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop:

- Agent Desktop My Computer embedded softphone mode is not supported. Agents must use a desk phone, or use a supported softphone concurrently with Agent Desktop.
- Avaya recommends that the RDS server hosting Agent Desktop is located in the same Local Area Network (LAN) as the CCMM server. If the RDS server hosting Agent Desktop is not in the same LAN as the CCMM server, then the AACC bandwidth, Round Trip Time, and networking requirements apply.
- AACC supports the Multicast option only for Real-Time Displays (RTDs) in a RDS environment. Unicast is not supported in a RDS environment.
- You cannot use the AACC or CCMM server as the RDS host.
- Agents must define default template or attachment folders in Agent Desktop preferences to an AppData folder on the RDS host. Agents do not have access to shared or mapped drives. For more information on configuration settings for temporary folders on the RDS Host Server, refer to the Microsoft Remote Desktop Services product documentation.

For information about how to use Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop, see *Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications* or *Deploying Avaya Aura® Contact Center DVD for Avaya Communication Server 1000*.

VMware Horizon View VDI support

Avaya Agent Desktop supports agent desktop virtualization using VMware Horizon View. VMware Horizon View is a Virtual Desktop Infrastructure (VDI) solution that provides centralized user and virtual desktop management.

Using virtualization in a contact center enterprise solution requires careful up-front planning, engineering, and implementation. While the technical and business advantages are clear, virtualization imposes extra considerations when designing the contact center solution architecture.

Avaya Agent Desktop supports the following VDI infrastructure:

- VMware vCenter, Release 5.0 or later
- VMware Horizon View, Release 5.2 or later
- VMware Horizon View Client for Windows, Release 5.2 or later.

How you deploy and use Avaya Agent Desktop VDI clients depends on your solution requirements and virtualization infrastructure. For more information about building a virtual client infrastructure using VMware Horizon View, refer to the VMware product documentation.

Overview of Avaya Agent Desktop (Agent Desktop) VDI deployment:

1. Before implementing Virtual Desktop Infrastructure, install and commission one or more Agent Desktop clients to confirm Avaya Aura® Contact Center and Agent Desktop are working.
2. Deploy and integrate VMware vCenter and VMware Horizon View servers. Avaya recommends that you apply virtualization planning, engineering, and deployment with full organizational support for virtualization rather than organically growing a Virtual Desktop Infrastructure.
3. Using vCenter, create a master Agent Desktop client computer:
    a. Create a client computer that meets or exceeds the minimum Agent Desktop hardware and operating system requirements.
    b. Install VMware Tools on the client computer.
    c. Install VMware Horizon View Tools on the client computer.
    d. Install Agent Desktop using either the click-once deployment or an MSI file on the client computer.
4. Create a template and snapshot of this Agent Desktop master computer.
5. Using VMware Horizon View, add one of more pools for the Agent Desktop VDI clients.
6. Associate the agent domain accounts with the Agent Desktop VDI client pools.
7. On each agent computer or thin client, install VMware Horizon View Client for Windows, Release 5.2 or later.
8. Avaya Aura® Contact Center agents can then use VMware Horizon View Client software to log on to a VDI client computer and use Agent Desktop.

In VMware Horizon View deployments of Avaya Agent Desktop, you must use a desk phone. The Avaya Agent Desktop *My Computer* embedded softphone mode is not supported in virtualized desktop deployments.

Client Citrix support

Avaya Aura® Contact Center supports Agent Desktop as a Citrix-published application. A Citrix server solution uses software to deliver on-demand Windows applications to physical desktops. This allows client users (agents in this case) to access and use programs that are available on the Windows Server 2012 R2 operating system of the Citrix server.

On the Contact Center Multimedia (CCMM) server the Avaya Agent Desktop MSI installer is located in the `D:\Avaya\Contact Center\Multimedia Server\Agent Desktop\client` folder.

Use this MSI package to install Agent Desktop on your Citrix server. Then configure your Citrix server to publish Agent Desktop as a published application, accessed from this Agent Desktop folder on the Citrix server. On the Citrix server select the users (agents) allowed to run the Agent

Desktop published application. For more information about Citrix application publishing, see your Citrix documentation.

Avaya recommends that the Citrix server publishing Agent Desktop is located in the same Local Area Network (LAN) as the CCMM server. If the Citrix server publishing Agent Desktop is not in the same LAN as the CCMM server, then the Avaya Aura® Contact Center bandwidth, Round Trip Time, and networking requirements apply. For more information about these networking requirements, see;

- Agent Desktop client network infrastructure requirements on page 406
- Network setup on page 252

Agent Desktop is supported only with the following versions of Citrix server:

- Citrix XenApp 6.0
- Citrix XenApp 6.5
- Citrix XenApp 7.6

In Citrix deployments of Agent Desktop, the My Computer embedded softphone mode is not supported. In Citrix deployments, Agent Desktop can use either the Desk Phone or the Other Phone mode.

In Citrix deployments, the Agent Desktop published application supports all the contact types that Avaya Aura® Contact Center supports.

Avaya Aura® Contact Center supports only the Multicast option for Real-Time Displays (RTDs) in a Citrix environment. Avaya Aura® Contact Center does not support the Unicast option for Real-Time Displays (RTDs) in a Citrix environment.

Chapter 33: Contact Center Agent Browser application requirements

This section provides information on the configuration requirements for the Contact Center Agent Browser application.

Voice-only Contact Center agents can use the Agent Browser application to log on to Contact Center and perform basic tasks. The Agent Browser application does not provide call control, multimedia features, or supervisor functions. Agent must use a supported desktop phone or softphone for call control. The Agent Browser application supports the following tasks:

- logging on and off
- changing the agent status
- setting not ready reason codes
- setting activity codes
- setting after call work item codes
- calling your supervisor
- handling an emergency

The Contact Center Agent Browser application is supported in SIP-enabled Contact Center solutions only. All agents require an associated Windows account, configured in CCMA, to log on to the Agent Browser application.

Agents access the Agent Browser application through a web browser, using the Contact Center server Fully Qualified Domain Name (FQDN). In High Availability solutions, agents must log on to the Agent Browser application using the FQDN of the High Availability pair.

In the event of a switchover to a Remote Geographic Node (RGN) server, agents must log on to the Agent Browser application using the FQDN of the RGN server.

The Agent Browser application does not support telecommuter mode.

You must access the Agent Browser application using HTTPS only. You must also install a valid TLS certificate, issued by a trusted Certificate Authority (CA), in Security Manager. To avoid certificate security warnings, install the root certificate of the CA on all client devices used to access the Agent Browser application. For more information, see Secure TLS communications in Contact Center on page 441.

If you use a mobile device to access the Agent Browser application, Avaya recommends using a medium size screen of 992 pixels or higher. Some mobile devices automatically lock after a defined

timeout period — the Agent Browser application has no control over the automatic locking of mobile devices.

Language support

The Contact Center Agent Browser application supports the following languages:

- English
- French (FR)
- German (DE)
- Italian (IT)
- LA Spanish (ES)
- Brazilian Portuguese (PT-BR)
- Russian (RU)
- Simplified Chinese (Zh-CN)
- Traditional Chinese (Zh-TW)
- Japanese (JA)
- Korean (KO)

You can set the application language on the Settings menu of the Agent Browser application.

Web browser requirements

The Agent Browser application is hosted on the Internet Information Services (IIS) that is running on the Contact Center server. Agents access the application through a web browser. The following table lists the supported browsers.

Browser	Versions supported	Operation system
Microsoft Internet Explorer	11.0	• Windows 7 • Windows 8.1 • Windows 10
Microsoft Edge	20.10240	• Windows 10
Google Chrome	43.0.23	• Windows 7 • Windows 8.1 • Windows 10 • Android 4.4.2 • Android 5.0.1 • iOS 8.3 • OS X Yosemite 10.10.3

Browser	Versions supported	Operation system
Mozilla Firefox **Important:** The Agent Browser application does not support using the “Search for text when I start typing” feature in Firefox.	38.0.5	• Windows 7 • Windows 8.1 • Windows 10
Safari	8.0.5	• iOS 8.3 • OS X Yosemite 10.10.3

Chapter 34: Contact center email server configuration requirements

You can use Contact Center Manager Administration to configure mailboxes, general settings, and rules that are required and optional for routing email messages.

This section provides an overview of the email server requirements, including the use of aliases. Contact Center Multimedia (CCMM) pulls email from any POP3 or IMAP/SMTP compatible email server. It polls the mailboxes at a specified interval.

Warning:

You must install and actively manage a SPAM filter to remove SPAM messages from all contact center mailboxes. Unsolicited bulk SPAM messages to your Contact Center, if not filtered out, can impact performance or can cause damage to your contact center solution.

Microsoft Exchange Server

Contact Center Multimedia supports the following versions of Microsoft Exchange Server,

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013

Contact Center Multimedia does not support Microsoft Exchange Server 2003.

Receiving email messages originating from a Web page

If your website generates email messages destined for a CCMM monitored mailbox, you must ensure that the FROM address of the generated email messages is set to the email address of the Web user. Do not generate email messages with a generic From address such as webmaster@company.com as this might lead to database instability due to the high volume of email messages from a single email address.

Hosted email providers

CCMM supports hosted email providers that permit a POP3 or IMAP & SMTP connection. CCMM supports hosted email providers that require TLS or STARTTLS access. CCMM does not support hosted email providers that require SSL access.

SPAM handling

Short Pointless Annoying Messages (SPAM) are unsolicited, indiscriminate, or junk email messages. You must install and actively manage a SPAM filter to remove SPAM messages from all contact center mailboxes. Unsolicited SPAM messages to your Contact Center, if not filtered out,

can impact performance or can cause damage to your contact center solution. Do not use CCMM as a SPAM filtering tool.

Email server requirements

Contact Center Multimedia uses the POP3 or IMAP/SMTP protocols to retrieve and send email. You must enable these protocols on your mail server. Contact Center Multimedia can support SMTP Authentication, POP3 or IMAP/SMTP over TLS, POP3 or IMAP/SMTP over STARTTLS, and the use of nonstandard ports for these protocols.

Email settings

Use the E-mail General Settings window to configure the following settings:

- The Mailbox Scan Interval is the interval between the scans made to the email server to check for new email messages. The default value is 60 seconds.
  - Configure the specific intervals in the Contact Center Multimedia Administrator application.
- The Attachment Files are the locations on the Contact Center Multimedia server where the attachments to email messages are stored. A URL is provided for agents to access the folder on the Web server. These values are provided by default.

  To change these folder names, you must ensure that the new folder exists on the file system with the correct path to the folders, the folder is shared, a parallel IIS virtual folder is created, and that all of the permissions are correct. No verification is performed in the Contact Center Multimedia Administrator application to ensure that the new values are correct, so the values need to checked carefully. The default values for the folder, where <Server name> is the name of the Contact Center Multimedia server, are:
  - Inbound URL: `http://<Server name>/inboundattachment`
  - Inbound Share: `<Database Installation Drive>:\AVAYA\CONTACT CENTER \EMAIL ATTACHMENTS\INBOUND`
  - Outbound URL: `http://<Server name>/outboundattachment`
  - Outbound Share: `<Database Installation Drive>:\AVAYA\CONTACT CENTER \EMAIL ATTACHMENTS\INBOUND`

    Caution:

    Risk of backup failure

    Use the default attachment locations defined during installation. If required, you can choose a different location for the inbound and outbound shared email folders. If you choose a different location, you must ensure that you perform the following activities:

1) Create the inbound email attachment folder with the path `Email Attachments/Inbound`.

2) Create the Outbound folder with the path `Email Attachments/Outbound`.

3) Share the inbound and outbound folders with IUSR_<Servername>.

4) Configure the folders in the email attachment locations in the Contact Center Multimedia Administrator application.

- The AutoNumber Outgoing E-mail is the customer identification number and can optionally be included in the message subject of all email messages.
- The Include E-mail Body in Keyword Search specifies that the keyword search for rules is applied to both the subject and the body of the email message. You can also select the number of characters in the email message to search.

Aliases

An alias is an alternative name for a mailbox. Sending an email to either an alias or the mailbox itself has the same result; that is, the email is stored in the same place.

For example, if you have a mailbox named `sales@avaya.com`. This mailbox has two aliases—`contactcentersales@avaya.com` and `mcssales@avaya.com`. If you send an email to either one of these addresses (`sales@avaya.com`, `contactcentersales@avaya.com`, `mcssales@avaya.com`), the email is sent to the same destination, which is `sales@avaya.com`.

Using an alias

Aliases are useful for email filtering. For example, if an alias address is defined for only a short promotion period, you can discard any email messages that arrive at that alias after the promotional time has passed.

Impact of an alias addresses on Contact Center Multimedia

Alias addresses are a useful pre-routing tool for email. Given the example in the previous section, you can configure three email routing rules. Email messages arriving with an address `contactcentersales@avaya.com` can be routed to the skillset EM_ContactCenterSales. Email messages arriving with the address `mcssales@avaya.com` can be routed to the skillset EM_MCSSales. If an email message arrives at the address `sales@avaya.com`, you cannot be sure of its content (at least without further keyword searching); therefore, route it to a general skillset such as EM_DefaultSales.

Note:

If a customer sends a single email to multiple aliases, Contact Center creates a contact for each alias. However, Contact Center recognizes only the first alias, so Contact Center treats all the contacts as if delivered to the first alias.

For example, a customer sends an email with both `contactcentersales@avaya.com` and `mcssales@avaya.com`, in the To: address field. In Contact Center, both these aliases map to a single mailbox. Contact Center creates two identical contacts, both with `contactcentersales@avaya.com` as the To: address. Contact Center processes both contacts using the rules and routing for `contactcentersales@avaya.com`.

Contact Center Multimedia and alias configuration

As an alias is only an alternative name for a mailbox, it is not polled. Therefore, Contact Center Multimedia must be aware of all possible aliases to ensure powerful routing. Define an alias in the same way as a physical mailbox. The only difference is you select Alias rather than Mail Store when configuring the mailbox. This informs Contact Center Multimedia that this is an alias address and there is no physical mailbox to poll. The email itself is retrieved from the physical mailbox with which the alias is associated. When you define all the possible aliases (as well as the physical mailboxes) in this list, the aliases become available to the Rules Wizard to selectively apply keyword searching, including address matching and other criteria to make routing decisions.

For more information about defining an alias, see *Avaya Aura® Contact Center Server Administration*.

Outgoing email

Configure outgoing email mailbox settings to identify who responds to the customer's email message.

The response can contain the email address to which the customer sent the original email message, or a general corporate email address that is configured for each skillset.

Agent-initiated messages are always sent from an email address associated with a skillset.

After you define the rules for email routing, all email are routed to a skillset. To determine the mailbox that is set as the originator, map the skillset to a mailbox. For detailed information, see *Avaya Aura® Contact Center Server Administration*.

Mailbox requirements

Contact Center Multimedia logs onto nominated mailboxes on your mail server and retrieves email at defined intervals. Email is then routed to agents. To route an email, Contact Center Multimedia requires the mailbox name and password. In addition, Contact Center Multimedia requires the possible alias names used for a mailbox to ensure correct routing of email.

Chapter 35: Performance optimization

This section provides information about performance optimization.

Contact Center Manager Server services performance impact

Contact Center Manager Server services Meridian Link Services (MLS) and Host Data Exchange impact performance. This section describes the performance of these two services, for which many contact centers require detailed information.

Host Data Exchange

The host data exchange (HDX) server enables the values of script variables to be sent to or received from a third-party provider application.

The following conditions apply:

- Third-party provider applications reside on a third-party host computer, and, therefore, are often referred to as host applications.
- Avaya provides a provider application that can co-reside with Contact Center Manager Server. The Database Integration Wizard (DIW) provides an easy-to-use tool for configuring and customizing the Avaya provider application. (Using the Database Integration Wizard can result in additional contact center subnet traffic.) For more information, see the *Avaya Aura® Contact Center Server Administration*.

For example, a script can

- obtain a credit card number from a caller using IVR
- query the provider application using the HDX API to determine the account balance of the caller
- use the account balance as a variable in the script

An API known as the service provider API enables a Contact Center Manager user to write custom applications (provider applications) that register with the HDX server to handle back-end processing for the script elements.

Two service elements can be invoked in the script:

- Send Info
- Send Request/Get Response

The Send Info command sends data to the provider application or the HDX server. The Send Request/Get Response command sends information to and receives information from the provider application. The Send Request/Get Response operation uses approximately twice as much CPU resources as the Send Info operation.

Cautions

If the provider application runs on a slow platform, or if it runs on the same platform as other CPU-intensive applications, the provider application might not be able to handle the Send Request commands quickly enough. As a result, a high volume of messages can become queued in the HDX server. If the queue reaches its size limit, the HDX server terminates the provider session. When this situation occurs, the provider application receives a DXM_SERVER_SHUTDOWN message from the API.

A DXM_SERVER_SHUTDOWN message means either of the following:

- The session is terminated because the provider application is too slow to respond.
- Communication is down because the HDX server is terminated.

If the provider application is too slow, either reduce the incoming Contact Center Manager Server call rate or run the provider application alone on a faster computer.

Guidelines to minimize capacity requirements

The engineering models used to calculate the capacity requirements of your contact center assume that you follow certain guidelines to minimize the load on your server. These guidelines apply to both stand-alone and co-resident servers.

Steady state operation

Steady state refers to an operational state in which average values of the capacity parameters do not change with time. For example, CPU usage can vary widely; however, if you examine the average values of CPU usage measured at consecutive intervals of 20 minutes, during a period of steady state operation, these average values are approximately the same.

Guidelines for steady state operation

To ensure trouble-free operation of the server, adhere to the following guidelines for steady state operation:

- Processor CPU—Average CPU usage for any interval of 20 minutes during the peak hour under steady state operation must not exceed 50 percent.
- Server RAM memory—Average pages per second (found in the Memory Object of the Performance Monitor) for any interval of 20 minutes during the peak hour under steady state operation must not exceed five.
- Server virtual memory—Committed Bytes (found in the Memory Object of the Performance Monitor) must not exceed 90 percent of the Commit Limit (also found in the Memory Object of the Performance Monitor).
- Physical and virtual memory—The Microsoft recommendations for physical RAM and virtual memory sizing must be adhered to for optimal performance.

Guidelines for non-steady state operation

A number of non-steady state processes can impact the steady state call processing activity of the server. To minimize their impact, Avaya recommends a number of restrictions:

- All non-steady state processes
  - Run only one non-steady state process at any given time.
  - Do not run other applications between 12:00 midnight and 12:30 a.m. During this time, the Historical Data Manager (HDM) service performs data consolidation for monthly, weekly, and daily data. CPU usage for this activity is high.
- Activation of the Master script
  - Do not activate the Master script during a busy period.
  - If you must activate the Master script during a busy period, activate all primary and secondary scripts first.

    Important:

    If the server is not processing calls, you can activate the Master script without first activating the primary and secondary scripts.
- Validation of large scripts
  - Do not validate the Master script or any large script during a busy period.
- Agent-to-supervisor assignments
  - Do not run multiple agent-to-supervisor assignments concurrently.

- Agent-to-skillset assignments
  - Do not run multiple agent-to-skillset assignments concurrently.
- Generation of large reports
  - Generate large reports one after the other rather than concurrently.
- Extraction of large amounts of data from the database
  - Generate large data extractions one after the other rather than concurrently.
- Mass logon and logoff of agents
  - Spread agent logon/logoff activity over a period of 5 to 15 minutes, and do not perform this activity during the peak busy hour.
- Database backup
  - Perform online (for example, database) backups during off-peak hours.
- Checking files for viruses
  - Perform this activity during off-peak hours.

Contact Center Manager Administration performance

This section describes performance impacts to Contact Center Manager Administration server.

Contact Center Manager Administration contact center server network impact

The network impact from Contact Center Manager Administration on the contact center LAN or WAN can be divided into two parts:

- RSM multicast data sent from Contact Center Manager Server to Contact Center Manager Administration.

  Important:

  RSM compression is a new option that can now be configured on the Contact Center Manager Server. However, Contact Center Manager Administration does not support RSM compression. If the compression is configured, Contact Center Manager Administration real-time displays do not work.

- Consolidated Real-Time Display (CRTD) data

  Contact Center Manager Administration consolidates multicast traffic into a single stream, and sends it to the client PCs in either multicast or unicast format.

Important:

Because the unicast option has a significant impact on network bandwidth requirements and CPU usage, Avaya recommends that you use multicast mode of network communication where possible.

In a network Contact Center Manager Server environment, Contact Center Manager Administration can consolidate traffic from multiple contact center servers. The RSM multicast data streams can originate at local and remote sites, and can be directed to both local clients and remote clients. In this environment, the consolidated display data is known as Network Consolidated Real-Time Display (NCRTD) data.

NCRTD multicast characterization

The inputs required to characterize the NCRTD multicast traffic are:

- send rates (time intervals in seconds) for each of the following statistics:
  - Agent
  - Application
  - Skillset
  - Nodal
  - IVR
  - Route
- the number configured for the following parameters:
  - Active agents
  - Applications
  - Skillsets
  - IVR queues
  - Routes

  Important:

  Number of nodes is always equal to 1.
- the number of data streams sent for each of the listed statistics. This value is 0, 1, or 2 for each type of statistic. The two types of data streams are Moving Window and Interval-to-date.

NCRTD unicast characterization

The inputs required to characterize unicast traffic are the same as those for multicast traffic, with the following additional input: number of unicast connections for each type of statistic (Agent, Application, Skillset, Nodal, IVR, and Route). A separate unicast data stream is required for each unique unicast display on each client. The number of possible unique displays for each client is 12—six for Moving Window statistics and six for Interval-to-date statistics. If more than one identical display for a particular statistic type is required on a given client, then only one unicast stream is sent for both.

For example, if two Agent/Moving Window displays are opened by the same client, only one Agent/Moving Window data stream is sent. However, if another client PC opens an Agent/Moving Window

data stream, a new unicast stream is sent from the server. Two identical streams are open at this point.

Each RTD adds a number of bytes to each update packet in the unicast stream. The following table details the number of bytes that each RTD adds, depending on the RTD type.

RTD type	Number of bytes
Application	162
Skillset	190
Agent	63
IVR	44
Nodal	24
Route	13

Contact Center Manager Administration client performance

The following section describes performance impacts to Contact Center Manager Administration client.

Contact Center Manager Client CPU impact

The real-time displays have the largest impact on CPU performance on Contact Center Manager Client. The input parameters used to calculate Contact Center Manager Client CPU requirements are:

- the refresh rate (assumed identical for each display)
- the number of lines displayed (overall displays, including fixed header rows)

Contact Center Manager Administration CPU load reduction

There are several ways to reduce CPU load on the Contact Center Manager Administration server and client.

Contact Center Manager Administration server

To minimize CPU load, make the following adjustments in Contact Center Manager Administration:

- Reduce real-time display refresh rates.
- Stagger scheduled historical reports so that they are not scheduled to run at the same time.
- Schedule large reports to run at off-peak hours.
- Schedule antivirus scanning to occur at off-peak hours.
- Perform backup and restore procedures at off-peak hours.
- Schedule skillset assignments to run at different times, and not all at the same time. For example, for skillset assignments needed by 09:00, schedule the assignments to run between 08:50 and 09:00 at 2-minute intervals.

Contact Center Manager Administration client

To minimize CPU load, make the following adjustments in Contact Center Manager Administration client:

- Reduce real-time display refresh rates.
- Configure the client to display less data by using data partitioning and filtering.

If the parameters are exceeded, you can use more than one Contact Center Manager Administration, and you can split Contact Center Manager Administration users across the multiple Contact Center Manager Administration servers.

Contact Center Multimedia customer contact ratio

The customer to contact ratio in Contact Center Multimedia (CCMM) must not exceed a ratio of 1:1000 (or 1 customer record per 1000 contacts). To avoid exceeding the ratio, whenever possible, each contact must generate a new customer record. Email manager creates a new customer record automatically when a unique from address is found. The ratio allows sufficient scope for multiple threads of conversation with a single customer (where agent and customer exchange a number of email messages).

Contacts in CCMM are generated from a variety of sources:

- standard email messages
- Web chat
- external websites using the Customer Interfaces Web services
- document imaging servers

- SMS/Fax gateways that generate email traffic

When a contact is generated in CCMM, a customer record is created to capture details of the sender and capture the details of the service request. You must ensure that each new sender is unique where possible to ensure correct threading of contacts and efficient system operation.

It is critical that you do not define a single sender (e.g. fax mailbox) for all contacts. This leads to an unsustainable ratio of customers to contacts in the CCMM database. The SMS/Fax gateway or other sending application must use the From address of each email message placed in the mailbox so that it identifies the originator of the email message, rather than an address that represents the gateway machine.

Example: An SMS or Fax from +353875555555@sms.company.com instead of gateway@sms.company.com must be recorded under +353875555555@sms.company.com to reduce the customer to contact ratio. Reducing the customer to contact ratio ensures logical threading of customer messages at the agent desktop as well as efficient system operation.

This consideration applies to all types of contacts: Web chat / callback requests must also create unique customer records rather than converging all requests on a single customer record.

Contact Center Multimedia bandwidth recommendations

Avaya recommends that the average contact center subnet usage not exceed 30 percent of the total bandwidth. This includes all the traffic (even customer traffic).

The email servers can be remote, but, if they are, the latency and bandwidth of the connection to these servers result in slower throughput of the overall system.

Communication Control Toolkit guidelines to minimize capacity requirements

The engineering models used to calculate the capacity requirements of your contact center assume that you follow certain guidelines to minimize the load on your server.

Steady state operation

Steady state refers to an operational state in which average values of the capacity parameters do not change with time. For example, CPU usage can vary widely at different consecutive time intervals; however, if you examine the average values of CPU usage taken over consecutive 20-minute intervals, during a period of steady state operation, these average values are approximately the same.

Guidelines for steady state operation

To ensure trouble-free operation of the server, adhere to the following guidelines for steady state operation:

- Processor CPU—Average CPU usage over an interval of 20 minutes during the peak hour under steady state operation must not exceed 70 percent.
- Server RAM memory—Average pages per second (found in the Memory Object of the Performance Monitor) over an interval of 20 minutes during the peak hour under steady state operation must not exceed 5.
- Server virtual memory—Committed Bytes (found in the Memory Object of the Performance Monitor) must not exceed 90 percent of the Commit Limit (also found in the Memory Object of the Performance Monitor).
- Physical and virtual memory—For optimal performance, you must adhere to the Microsoft recommendations for physical RAM and virtual memory sizing.

Guidelines for non-steady state operations

Non-steady state processes can impact the steady state call processing activity of the server. To minimize their impact, Avaya recommends a number of restrictions:

- Database backup

  Perform database backups during off-peak hours.

- Checking files for viruses

  Perform this activity during off-peak hours.

Network Traffic

Communication Control Toolkit uses remote method calls between the client PC and the Communication Control Toolkit server. Avaya recommends that you design and develop the applications to minimize the number of remote calls and, therefore, reduce the demands on the underlying network and increase the application responsiveness.

The following network traffic measurements were taken using the Full API Reference Client and logging on to the Communication Control Toolkit server as a user with a single AgentTerminal assigned (representing the normal deployment of a Communication Control Toolkit application).

The following table provides a measurement of the network traffic generated by various call scenarios using the Full API Reference Client. These network traffic statistics provide a representation of what load the Communication Control Toolkit imposes on the network.

Table 51: Network traffic statistics

Scenario	Rx by server (bytes)	Tx by server (bytes)	Total (bytes)
Connect to the CCT server (does not include traffic required to perform user authentication)	8227	7090	15 317
Disconnect from the CCT server	1629	1243	2872
Answer and drop an incoming call	4171	7324	11 495
Make and drop an outgoing call	4332	6726	11 058

Part 5: Security

Chapter 36: Security

This section provides information about the server port requirements of Avaya Aura® Contact Center.

For more information about Avaya Aura® Contact Center security, see *Avaya Aura® Contact Center Security* available from the Avaya Support website at http://support.avaya.com.

Contact Center server security

The system handles security based on whether you work with a stand-alone server or a network configuration.

Stand-alone server security

Regularly perform the following tasks to protect your Contact Center servers:

- Update Microsoft operating system updates on a timely basis.
- Limit administrative access to the database containing the CTI data store to specific administrative Windows user accounts.
- Ensure all services providing a network interface (such as the CTI service provider) run using either the Windows Network Service account or another privileged account. The Windows Network Service account is a built-in account with a security context that provides the least privileges required to run a typical network service.
- Disable all nonessential network services.

Network security

The various network interfaces are secured using the following mechanisms.

Interface	Network security mechanism
CTI API	The secure TCP transport layer described in the .NET Framework section provides network security for the CTI API interface.

Interface	Network security mechanism
AML	No specific network security mechanism is used. Because it is a proprietary protocol, exposure is limited as it runs over the ELAN subnet.

Server Message Block signing

Contact Center installs and updates modify the Windows Server 2012 local group policy to enable Server Message Block (SMB) signing. SMB signing places a digital tag into each server message block, which helps prevent man-in-the-middle attacks on network file sharing.

If you do not want to use SMB signing, you can disable it by modifying the Windows Server 2012 local group policy.

Secure TLS communications in Contact Center

Contact Center includes a number of services that you can secure by using the HTTPS protocol. At the installation stage, you can now use the Ignition Wizard to create a security store, generate a Certificate Signing Request (CSR) and import a Certificate Authority root certificate. Alternatively, you can skip security configuration at the installation stage and configure your security certificates later using Security Manager.

You must have a good understanding of HTTPS security to plan and configure Contact Center. For an overview of HTTPS security and associated terminology, see HTTPS and Transport Layer Security basics on page 441.

HTTPS and Transport Layer Security basics

HTTPS is a secure protocol for Web communications. HTTPS provides both authentication of the Web server, and encryption of communications between the server and the client in both directions. HTTPS uses connections encrypted by the Transport Layer Security (TLS) protocol.

When a client initiates a secure connection with a server using TLS, the server returns its public cryptographic key in a server certificate. To ensure the integrity of the server certificate, it must be signed by a third party, called a Certificate Authority (CA). The client must have a root certificate from the CA that provided the signed server certificate. If the client has a matching root certificate it can trust the server certificate, so it completes the connection and secure communication is established.

Encryption levels, TLS versions, and SSL

Contact Center supports both the SHA1 and SHA2 cryptographic hash functions, with key sizes of 1024, 2048, or 4096. However, the SHA1 hash function and the 1024 key size do not provide the

current industry-recommended level of encryption. Contact Center supports SHA1 and a 1024 key size only to provide backward compatibility.

Avaya recommends that you use only SHA2 and either a 2048 or 4096 key size. The default values for new security stores are SHA2 with a 2048 key size.

Secure Sockets Layer (SSL) also is obsolete, having a number of known weaknesses. Contact Center now uses only Transport Layer Security (TLS) for secure communications. Note that TLS is an extension of the older SSL protocol, and the industry frequently accepts and uses the term ‘SSL’ to refer to TLS.

Contact Center implements Transport Layer Security (TLS) version 1.2 as the default minimum version negotiated for secure communications. This is to avoid security vulnerabilities that exist in TLS 1.0. For backward compatibility and inter-operation with third-party or custom applications connecting to Contact Center, Administrators can set lower versions of TLS on certain communication channels. When a lower version of TLS is available, Contact Center still negotiates the highest level of TLS that the other application can support.

Server certificate

The server certificate, sometimes called a signed certificate or an identity certificate, is the certificate that the server sends to a client that requests a secure service (HTTPS). The server certificate combines a public key used for encryption with an organization’s details, and is signed by a Certificate Authority (CA) to allow clients to verify that it is valid. The client can use the server certificate to encrypt the data it sends to the server.

Certificate Authority

A Certificate Authority (CA) is a third-party organization that provides digital certificates that certify the owner of a public key for cryptography used in secure communications. If you use a single CA for all your security setup, it reduces you workload for security configuration, because you need to copy just a single root certificate to all clients. The root certificates for many well know CAs are frequently already embedded in common operating systems for clients and servers.

Root certificate

The root certificate proves the authenticity of the signed server certificate. It contains a digital signature from a Certificate Authority (CA). To trust the server certificate sent to them by the server, clients must have a copy of the root certificate with the digital signature of the CA that signed the server certificate. Root certificates exported from different security stores work in the same way if they contain a digital signature from the same CA.

Server Certificate name

Each server certificate has a name, which normally derives from the server Fully Qualified Domain Name (FQDN). If a server certificate name does not match the name of the website or web service to which the client connected, the client generates a warning. This impacts Contact Center as follows:

- In HA systems, you need to commission your own certificates with Subject Alternative Names (SANs) to use the managed name of the campus HA pair. Therefore you must decide on the active, standby, and managed names before you set up your own security stores.

Subject Alternative Name

A Subject Alternative Name (SAN) is an extension to HTTPS that allows various values to be associated with a security certificate. These values are called "Subject Alternative Names", or

SANs. There are several types of SAN values, but for Contact Center only the DNS name type is relevant.

In Contact Center you use SANs on security certificates to include the HA managed name as well as the Contact Center server common name in the server certificate, so that secure connections continue during a HA switchover and clients do not see warning messages.

When you create the Contact Center security store in Security Manager, you can add the SANs necessary for HA.

Contact Center security store

Contact Center includes a security store to enable secure communications over Transport Layer Security (TLS), both between Contact Center applications and with external clients or third party applications. Customers must create a security store using either the Ignition Wizard or Security Manager, with a server certificate and root certificate from a Certificate Authority (CA).

Contact Center also uses the Internet Information Services (IIS) security store for some services. On a Contact Center server, Security Manager controls both the IIS security store and the Contact Center security store. These two stores always use the same server certificate.

The CCT and CCMS Open Interfaces use a unique CMF security store. You can configure or manage this store either through the CCMS Server Configuration interface or the CCT Server Configuration interface. You can import the server certificate from Security Manager into this store.

Avaya Aura® Media Server (MS) also has a security store. You configure this store through Avaya Aura® MS Element Manager. On a Voice and Multimedia Contact Center with Avaya Aura Media Server, where Avaya Aura® MS is co-resident with Contact Center, you can import the server certificate from Security Manager into this store.

The following table outlines which security stores are present on each Contact Center server type:

Server type	Contact Center security store	IIS security store	CMF security store	Avaya Aura® MS security store
Voice and Multimedia Contact Center with Avaya Aura Media Server	Yes	Yes	Yes	Yes
Voice and Multimedia Contact Center without Avaya Aura Media Server	Yes	Yes	Yes	No
Voice Contact Server / NCC	Yes	Yes	Yes	No
Multimedia Contact Server	Yes	Yes	No	No
Avaya Aura Media Server	No	No	No	Yes

The following table lists the applications that use the security stores on the Contact Center servers, the services impacted, and the management tool for the store:

Security store	Applications	Services that use this store	Managed by
Contact Center security store	CCMS, CCT	AES CTI link Agent Greeting CCT Web Administration	Contact Center Security Manager
Windows 2012 IIS security store	CCMA, CCMM	CCMA CCMM Administration Agent Desktop Agent Browser application Agent Greeting Multimedia Services Orchestration Designer Outbound Campaign Management Tool Contact Center Web Services	Contact Center Security Manager
CMF security store	CCMS, CCT	CCT Open Interfaces CCMS Open Interfaces (WS Open Interfaces) Open Queue Landing pads	CCMS Server Configuration or CCT Server Configuration
Avaya Aura® MS security store	Avaya Aura® MS	Avaya Aura® MS SOAP service Avaya Aura® MS SIP services Element Manager	Avaya Aura® MS Element Manager

Contact Center services that can use TLS security

The following table lists all the Contact Center services that must be secure, or can be secure, showing those that require manual input and management by the customer.

Contact Center Service	PABX type	Always secure, uses CC Security Manager	Secure by default, managed by CC Security Manager	Security optional, managed by Security Manager	Security optional, uses CMF security store
AES CTI connection	UC only	Y			
Agent Browser application	UC only	Y			
Agent Desktop	UC and CS1000		Y		
Agent Greeting recorder	UC only		Y		
CCMA Administration	UC and CS1000		Y		
CCMM Administration	UC and CS1000		Y		
Orchestration Designer	UC and CS1000		Y		
Outbound Campaign Management Tool	UC and CS1000		Y		
Contact Center Web Services	UC and CS1000		Y		
CCT Web Administration	UC and CS1000		Y		
Secure Real Time Transport on voice segments	UC only			Y	
CCT Open Interfaces	UC and CS1000				Y
CCMS Open Interfaces (WS Open Interfaces)	UC and CS1000				Y

- You must use a certificate for AES CTI services and the Agent Browser application. You generate this certificate in Contact Center Security Manager.

  The CTI connection between AACC and AES requires Mutual Transport Layer Security (MTLS). The AES server has a server certificate and must have the AACC root certificate. The Contact Center server has a server certificate and must have the AES root certificate. You do not need these services in a CS1000 deployment.

- You must use a certificate for Web Services, unless you turn off Web Services security. You use the certificate in Security Manager.
- You must use a certificate for Avaya Aura® MS. On a Voice and Multimedia Server with Avaya Aura Media Server, you can use the server certificate you created in Security Manager.
- You can use a certificate for Secure Real-Time Protocol (SRTP). You use the certificate in Security Manager.
- You can use a certificate for CCT Open Interfaces. You must add this certificate to the CMF security store, but you can use the server certificate you created in Security Manager.
- You can use a certificate for CCMS Web Services. You must add this certificate to the CMF security store, but you can use the server certificate you created in Security Manager.

Note:

The Agent Desktop Click-Once deployment does not use HTTPS. If you have Web Services security enabled, you still use HTTP to deploy the Agent Desktop prerequisites and application. After you have installed Agent Desktop, if you have Web Services security enabled, agents then use HTTPS to run the application.

Contact Center automatically backs up a new security store when you create it. This allows you to recover from situations where the store is damaged or deleted between sending the Certificate Signing Request (CSR) to a Certificate Authority (CA), and receiving a signed certificate back from the CA. The location for the security store backup is `D:\Contact Center\autoBackUpCertStore`. Do not overwrite or delete this backup location.

Contact Center Security Manager

Contact Center includes a number of services that you can secure by using the HTTPS protocol.

Contact Center Security Manager provides an interface for managing the security certificates in the Contact Center security store and the IIS security store. Contact Center supports the management of the IIS security store only through Security Manager: do not use IIS functions to manage the IIS security store on a Contact Center server.

Server certificates

Each security store must have a server certificate signed by a CA, and a root certificate from the same CA. In Contact Center, you can use the same server certificate in all the security stores on a single server. You can also generate different server certificates for each security store on a single server. You cannot use the same server certificate on two different servers.

Certificate Authority root certificates

When a client initiates a secure connection with a server, it must have a root certificate from the CA that provided the signed server certificate. If the client does not have a matching root certificate, it does not complete the connection. If the client has a root certificate from a given CA, it can trust any server certificate signed by that CA.

Avaya recommends that you use a single CA to sign all the certificates in your contact center. This simplifies the deployment process, because you need to distribute only a single root certificate to all the clients.

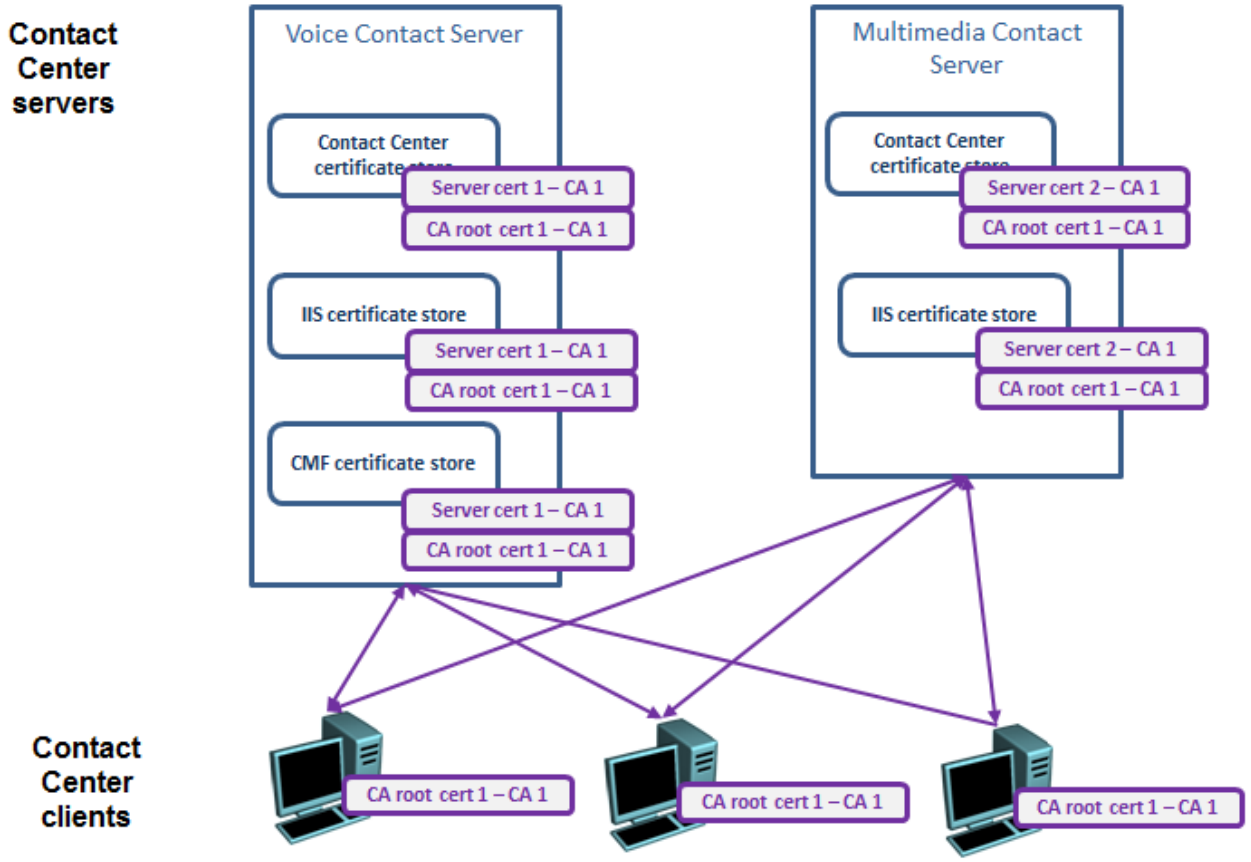


Figure 28: Example of how a single CA root certificate can work with different server certificates signed by the same CA

If you want to use different CAs to sign certificates for your different servers, you must copy the root certificate from each CA to all the clients in your contact center. For some Contact Center Web services, Contact Center servers can act as clients of other servers. Therefore you must ensure that the Contact Center servers also have the required CA root certificates.

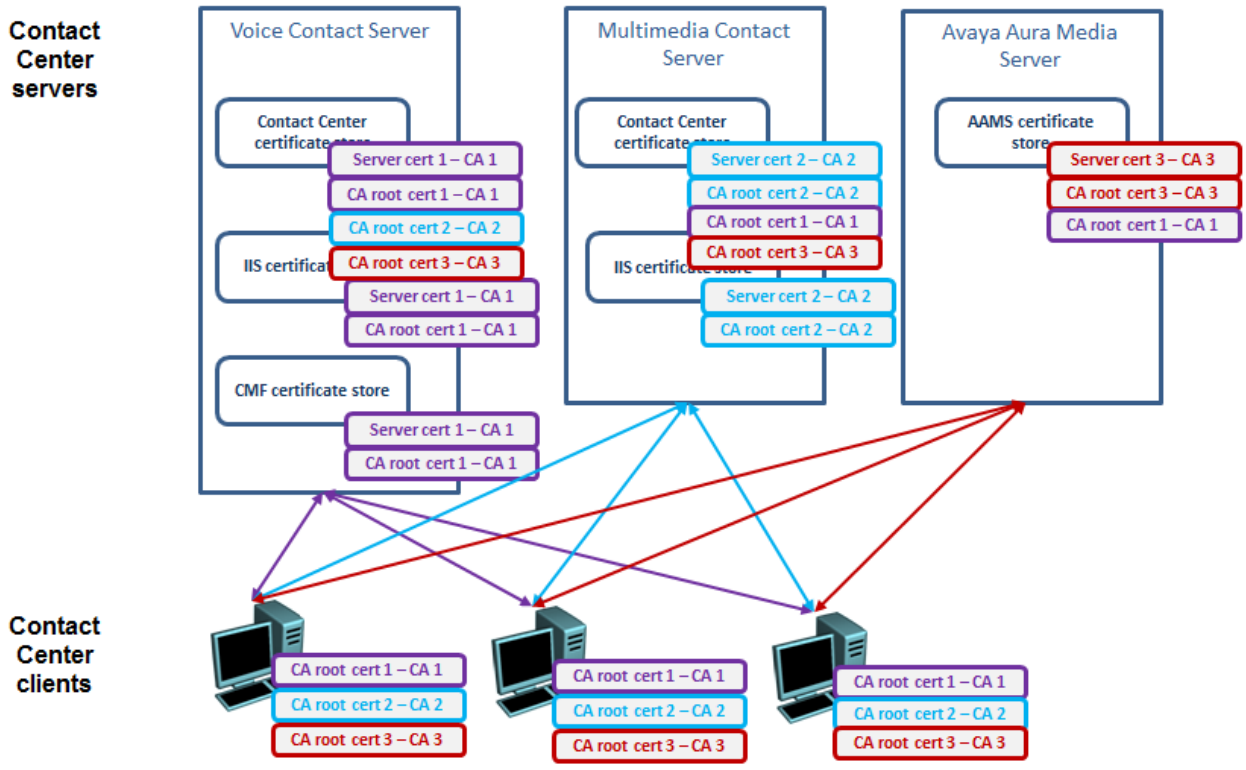


Figure 29: Example of how clients must have the CA root certificates from each CA that signed a server certificate, if the contact center uses server certificates signed by different CAs

You can distribute root certificates to client computers using a Group Policy on Microsoft Windows Server 2012.

Multimedia Contact Server deployments with TLS security

Where you are deploying Contact Center to use both a Voice Contact Server and a Multimedia Contact Server, you must configure security on both servers. The Multimedia Contact Server must have a unique server certificate: you cannot use the same server certificate on different Contact Center servers.

TLS security in a High Availability environment

If you implement High availability, Contact Center clients and servers must be able to communicate with the active contact center server and the managed name of the HA server pair.

In a High Availability (HA) system, you must create a new security store for each server, specifying Subject Alternative Names (SANs). Create the security store for each HA server in the pair, with the common name of the Contact Center server, and a SAN for :

- the Contact Center server name
- the managed name of the HA pair

This ensures clients connecting to Contact Center using the managed name do not get warnings that the server certificate name does not match the server name.

Avaya recommends that you plan your HA active, managed, and standby names in advance of creating a new security store. In this way you can create your security stores once using SANs during the initial commissioning, instead of deleting and re-creating security stores when you commission HA.

Migrating secured Contact Center systems

You cannot migrate a Contact Center security store from Release 6.x to Release 7.0. If you are migrating a secure Contact Center system from Release 6.x, you must create a new security store on the Release 7.0 Contact Center server.

If you migrate to a Multimedia server type from an unsecured Release 7.0 Multimedia server type, from an Avaya NES R6.x or R7.x Multimedia server, or AACC R6.x Multimedia server type, then you must turn off Web Services security before restoring the old CCMM database. This applies to the following Release 7.0 server types:

- Voice and Multimedia Contact Server with Avaya Aura Media Server
- Voice and Multimedia Contact Server without Avaya Aura Media Server
- Multimedia Contact Server

You can commission Web services security after the migration.

Contact Center Security store notifications

Security certificates contain an expiration date and they are not valid after this date. If the security certificates used by Contact Center expire, the contact center loses call control and stops functioning.

Security Manager provides a security store inspection utility to help you monitor and maintain valid security certificates. You can use Security Manager to schedule a security store inspection task. Security Manager adds the scheduled task to the underlying Windows Task Scheduler. The scheduled task runs the security store inspection utility once a week. The inspection utility checks the status of the security certificates in the Contact Center security store. If any of the security certificates are due to expire within a month, the inspection utility sends a notification email to the contact center administrator. The contact center administrator must then refresh the security certificates.

Security Manager provides the notification email; it cannot renew expired security certificates. For uninterrupted Contact Center functionality, if you receive an email about upcoming certificate expiration dates, you must renew the security certificates before they expire. Security Manager uses the Microsoft Windows Task Scheduler to schedule the weekly security store inspection. You must ensure that there is a Microsoft Windows user account that has the necessary privileges from which Security Manager can schedule a task on Windows Task Scheduler. You can use the Windows administrator account that you used to install Contact Center to add a task to Windows Task Scheduler.

Security Manager uses a specified Simple Mail Transport Protocol (SMTP) server to send the notification emails to the administrator's email address. Contact Center does not provide this SMTP server. You must provision this SMTP server and ensure that the Contact Center server can communicate with it at all times. Contact Center does not support Transport Layer Security (TLS) connectivity to this SMTP server.

Avaya Security Advisories

Avaya Security Advisories are posted on the Avaya Security Support website at https://support.avaya.com/security. From the Avaya Support website, you can register to receive email notifications of Avaya Security Advisories.

The amount of time it takes to receive an Avaya Security Advisory varies depending on the vulnerability classification of the advisory. For more information about vulnerability classifications, responses, and maintenance policies, refer to the following documents:

- *Avaya's Product Security Vulnerability Response Policy*
- *Avaya's Security Vulnerability Classification*
- *Avaya's Maintenance Contract Requirements for Product Support*
- *Avaya Product Security Support Flow*

Secure Access Link feature

Avaya Aura® Contact Center supports Avaya Secure Access Link (SAL). SAL is a remote-access architecture that provides simplified network management and increased support options for greater security, reliability and flexibility. SAL gives you complete control of when and how Avaya, or any other service partner, can access your equipment. You can take advantage of channel-neutral support by enabling self-service, Avaya, and/or business-partner support of your networks. For more information about Avaya Secure Access Link, see http://support.avaya.com.

Secure RTP in Contact Center

Avaya Aura® Contact Center (AACC) supports implementing Secure Real-Time Transport Protocol (SRTP) for voice contacts within the contact center.

Secure Real-Time Transport Protocol (SRTP) is an extension to the Real-time Transport Protocol (RTP) to support secure real-time communications. The primary use of SRTP is to encrypt and authenticate voice over IP (VOIP) on the network.

The use of SRTP depends on implementing Transport Layer Security (TLS) to securely exchange SRTP encryption keys between VOIP endpoints. For effective implementation of SRTP, all legs of the VOIP communication must implement TLS. If a link does not implement TLS, then the SRTP keys in the SIP INVITE become visible, compromising the security of the SRTP stream. TLS implementation is on a link by link basis: for example the TLS link between an agent phone and Communication Manager is different to the TLS link between Communication Manager and Avaya Aura® Media Server, even though both are supporting the same real-time voice stream. Therefore it is possible that an SRTP session can start in a situation where one of the links does not have TLS: this allows for the potential tapping of the session on the unsecured link.

Important:

While TLS secures the keys on the network link, the AACC logs store all SIP messaging. As a result, SRTP keys are visible to anyone with access to the AACC logs. However, if the AACC server is not sufficiently secure to protect the log files, then the overall security policy has a significant flaw. It is important to note that SRTP keys change for each new voice call, even if the endpoints are the same. Therefore, any SRTP keys recovered from logs are useful for snooping only for the duration of the voice call.

Implementing SRTP provides encryption and authentication to the voice streams, but does not provide any security beyond that. It is important to recognize that securing voice streams is not the same as having a secure contact center.

All the servers and endpoints implementing SRTP must have certificates from the same Certificate Authority (CA).

Important:

Implementing SRTP for Contact Center provides security only for the legs of the call within the Contact Center solution. It does not, for example, secure the leg of the call between the customer telephone and the contact center PABX.

Implementation considerations

Before implementing SRTP in Contact Center, you must have TLS on the following links:

- Communication Manager to Session Manager
- Agent telephones to Communication Manager
- Session Manager to Contact Center
- Contact Center to Application Enablement Services
- Contact Center to Avaya Aura® Media Server

To provide SRTP for routed Contact Center voice calls, you must configure SRTP on the following links:

- Agent telephones to Communication Manager
- Agent telephones to Avaya Aura® Media Server
- DMCC interface from Communication Manager to Avaya Contact Recorder (if used)

Note:

Supported agent telephones include H.323 phones, SIP phones, and the Avaya Agent Desktop embedded softphone. If your Contact Center agents use the Agent Desktop embedded softphone, you must configure the Media Encryption settings on the Group Policy administrative template. For more information, see *Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications*.

Secure communications for third-party or custom applications

Avaya Aura® Contact Center supports Transport Layer Security (TLS) for use in secure communications. Contact Center does not support Secure Sockets Layer (SSL). Third-party or custom applications connecting securely to Contact Center must support TLS 1.0 or later.

Before migrating from a previous Release, check third-party or custom applications that connected securely to Contact Center, to ensure that these applications support TLS.

Contact Center Manager Server port requirements

Contact Center Manager Server uses ports for communication between its own components. Most ports do not have implications for external network components like firewalls; however some ports might be used externally and therefore can affect an external firewall. In particular, port 10000 is a hard-coded port used to enable interoperability between Contact Center applications and external third-party applications (applications developed using the Real-Time Data (RTD) API).

No third-party application installed on Contact Center Manager Server can use the ports listed in the following table as it can cause the Contact Center Manager Server application to malfunction.

The following table shows the ports that Contact Center Manager Server uses.

Table 52: Contact Center Manager Server port usage

CCMS port number	Functionality
445	TCP port used Windows File and Printer Sharing for Microsoft Networks. Required when copying data between active and standby servers using Windows File Sharing.

CCMS port number	Functionality
1550	HDX CAPI
1972	Caché database, and Caché shadowing
3389	Remote Desktop Connection for support
3998	License Manager destination port—This is the first of 10 consecutive ports required for license management.
3999–4007	License Manager client source port
4422	HDX NameService
5060–5061	SIP Proxy
5080	SIP – Agent Greeting
5081	SIPS – Agent Greeting
8444	Local WebLM Port
8081	HTTP – Agent Greeting
8445	(HTTPS) for Agent Greeting recorder web application on Tomcat
9070-9073	Web Services Open Interfaces
9086	CC Web Statistics
9089	Avaya Aura® Experience Portal Basic Ports application
9100	XMPP Web Service Server Port
9120	XMPP Web Service Client Port
10000	Hardcoded Toolkit Name Service
10001–10082	Networking
10038	NCP_CHANNEL—This channel is used to communicate between the NCP of one node to the NCP of another node. The NCP on one node sends sanity messages to the other node through this port.
10039	ASM_CHANNEL—Different modules like NCP and TFE send messages to ASM through this channel.
10040	NCP_ASM_CHANNEL—ASM uses this channel to send messages to NCP.
10060	ASM_Service—The ASM service runs on this port. The Service Control Manager can send messages such as START, STOP, and RESTART to the ASM service through this port.
10062	NCP_Service—The NCP service runs on this port. The Service Control Manager can send messages such as START, STOP, and RESTART to NCP on this port.
12668–12670	TraceControl
52233	Avaya WebLM Server (remote)
57012	System Management and Monitoring Component (SMMC) system tray. Used by the High Availability feature.

Contact Center Manager Administration port requirements

The following table shows the ports that Contact Center Manager Administration uses.

Table 53: Contact Center Manager Administration port usage

CCMA port number	Functionality
TCP 80	For Internet Explorer communication.
TCP 443	For secure HTTP communication (only applicable if TLS is enabled for secure Internet Information Services (IIS) communication).
TCP Port 445	Windows File and Printer Sharing for Microsoft Networks. Required when copying data between active and standby servers using Windows File Sharing.
TCP Port 3389	For remote desktop connection.
TCP Port 25 (SMTP)	For the Historical Reporting component to send email notifications when reports are printed and saved.
TCP Port 8200	For the Emergency Help component on the client PC.
UDP ports 6020, 6030, 6040, 6050, 6060, 6070, 6080, 6090, 6100, 6110, 6120, 6130	For CCMA to receive IP multicasting data from CCMS (needed for Real-Time Reporting and Agent Desktop Displays).
UDP ports 7 020, 7030, 7040, 7050, 7060, 7070, 7080, 7090, 7100, 7110, 7120, 7130	For the CCMA server to send IP multicasting data to client PCs (needed for Real-Time Reporting and Agent Desktop Displays).
UDP ports 7025, 7035, 7045, 7055, 7065, 7075, 7085, 7095, 7105, 7115, 7125, 7135, 7140, 7150, 7145 and 7155	For the CCMA server to send IP unicast data to client PCs. This is an optional method of sending the data required for Real-Time Reporting. If you do not use the multicast method, then you must configure the unicast option. You can also use a combination of the two methods.
TCP Port 10000	Used by the Nameservice process on the CCMA server (nbnmsrvc.exe). It permits communication between the CCMA server and the server in Contact Center Manager Server. **Important:** The default port for the third-party software. This conflicts with the default port used by the CCMA Toolkit NameService. To avoid issues with CCMA functionality when using Veritas Backup Exec, you must change the default port of Veritas Backup Exec to another port number that is not being used by the network.
Default UDP port 3998	License Manager destination port.
Default UDP ports 3999 - 4007	License Manager destination source port.

Contact Center Multimedia port requirements

The following table lists the configurable Multimedia ports.

Table 54: Contact Center Multimedia ports

Port	Host	Client	Network interface	Functionality
1972	Contact Center Multimedia	Contact Center Manager Administration Server	Contact Center Multimedia Caché database	Port opened on database for reporting. Caché database, and Caché shadowing in High Availability solutions.
445	Windows File and Printer Sharing for Microsoft Networks.	Windows File and Printer Sharing for Microsoft Networks.	Windows File and Printer Sharing for Microsoft Networks.	Windows File and Printer Sharing for Microsoft Networks. Required when copying data between active and standby servers using Windows File Sharing.
110	Email server	Email Manager	Email server POP3	Receiving email
143	Email server	Email Manager	Email server IMAP	Receiving email
995	Email server	Email Manager	POP3 over TLS (optional)	Receiving secure email (optional)
993	Email server	Email Manager	IMAP over TLS (optional)	Receiving secure email (optional)
110	Email server	Email Manager	POP3 over STARTTLS (optional)	Receiving secure email (optional)
143	Email server	Email Manager	IMAP over STARTTLS (optional)	Receiving secure email (optional)
25	Email server	Email Manager	SMTP	Sending email
25	Email server	Email Manager	SMTP over TLS (optional)	Sending secure email (optional)
80	Contact Center Multimedia Server	Any Web services client (Agent Desktop, OCMT, and third-party Web services)	SOAP protocol	Accessing http Web services
29373	Communication Control Toolkit Server	Agent Desktop	Communication Control Toolkit	Remote access from clients to Communication

Port	Host	Client	Network interface	Functionality
				Control Toolkit server (for Agent Desktop application)
57012	System Management and Monitoring Component (SMMC) system tray	System Management and Monitoring Component (SMMC) system tray	System Management and Monitoring Component (SMMC) system tray	High Availability

Communication Control Toolkit port requirements

The following table shows the port numbers required for Communication Control Toolkit (CCT).

Table 55: Communication Control Toolkit port usage

CCT port number	Functionality
445	Windows File and Printer Sharing for Microsoft Networks. Required when copying data between active and standby servers using Windows File Sharing.
1972	Caché database, and Caché shadowing High Availability solutions.
3000	For TAPI switch connection through MLS (CCMS server). This port is required for the contact center subnet.
3998	License Manager (LM) destination port, which is the first of 10 consecutive ports required for license management.
3999 - 4007	LM client source ports.
5000	To connect to the server in CCMS.
8081	Change to "Default HTTP port of the Apache Tomcat Server which hosts the CCT Web Administration.
8085	For CCT services to access the CCT database.
8098	For the Contact Management Framework on the CCT server.
8099	For the Contact Management Framework on the CCT server.
8087	For CCT CMF component.
8445	Default HTTPS port of the Apache Tomcat Server which hosts the CCT Web Administration.
9000	For CCT WebAdmin component.
9010	For CCT CMF component.
9080–9083	CCT WebServices
11110	Used by the CCT Server service for the CMF Web Service - Callback port.

CCT port number	Functionality
11111	Used by the CCT Server service for the CMF Web Service - Web server port.
29373	Listens for requests from CCT client applications.
29374	Data Access Layer Service listens for requests from CCT Remote Administration Console.
57012	System Management and Monitoring Component (SMMC) system tray. Used by the High Availability feature.

Avaya Aura® Media Server port requirements

The following table shows the port numbers required for Avaya Aura® Media Server on Windows Server 2012 R2.

Table 56: Avaya Aura® Media Server port usage–Windows Server 2012 R2

Port	Type	Permit in TCP Filter	Description
1027	TCP	Yes	License Server
1028	TCP	No	System Monitor mchb
3306	TCP	Yes	MySQL
3389	TCP	Yes	Remote Desktop
3867	SCTP	No	Diameter over SCTP
3868	TCP	No	Diameter over TCP
3869	TCP	No	Diameter over TLS
4001	TCP	No	IvrMP MSLink
4004	TCP	No	Sip UA MSLink
4005	TCP	No	Resource Manager ExtSess
4014	TCP	No	SIP UA cmd i/f
4015	TCP	No	Resource Manager and i/f
5070	TCP	Yes	SIP over TCP
5070	UDP	No	SIP over UDP
5071	TCP	Yes	SIP over TLS
7080	TCP	No	ConfMP MSLink
7150	TCP	Yes	(HTTP) for Web UserAgent
7151	TCP	Yes	(HTTPS) for Web UserAgent
7410	TCP	Yes	SoapServer
7411	TCP	Yes	SoapServer TLS
11004	TCP	No	DiamC MSLink

Port	Type	Permit in TCP Filter	Description
11014	TCP	No	DiamC cmd i/f
19899	TCP	Yes	Resource Manager CPLink
19999	TCP	Yes	IvrMP ssdata
20005	TCP	Yes	CStore MSLink
20007	TCP	Yes	CStore RTFT
20009	TCP	Yes	IvrMP RTFT
20011	TCP	No	Resource Manager IPC
21000	TCP	No	Voice XML Interpreter IPC

The following table shows the port numbers required for Avaya Aura® Media Server on Linux.

Table 57: Avaya Aura® Media Server port usage–Linux

Port	Type	Permit in TCP Filter	Description
1027	TCP	Yes	License Server
1028	TCP	No	System Monitor mchb
3306	TCP	Yes	MySQL
3867	SCTP	No	Diameter over SCTP
3868	TCP	No	Diameter over TCP
3869	TCP	No	Diameter over TLS
4001	TCP	No	IvrMP MSLink
4004	TCP	No	Sip UA MSLink
4005	TCP	No	Resource Manager ExtSess
4014	TCP	No	SIP UA cmd i/f
4015	TCP	No	Resource Manager cmd i/f
5060	TCP	Yes	SIP over TCP
5060	UDP	No	SIP over UDP
5061	TCP	Yes	SIP over TLS
7080	TCP	No	ConfMP MSLink
7150	TCP	Yes	(HTTP) for Web UserAgent
7151	TCP	Yes	(HTTPS) for Web UserAgent
7410	TCP	Yes	SoapServer
7411	TCP	Yes	SoapServer TLS
8080	TCP	Yes	EM HTTP
8443	TCP	Yes	EM HTTP(s)
11004	TCP	No	DiamC MSLink

Port	Type	Permit in TCP Filter	Description
11014	TCP	No	DiamC cmd i/f
19899	TCP	Yes	Resource Manager CPLink
19999	TCP	Yes	IvrMP ssdata
20005	TCP	Yes	CStore MSLink
20007	TCP	Yes	CStore RTFT
20009	TCP	Yes	IvrMP RTFT
20011	TCP	No	Resource Manager IPC
21000	TCP	No	Voice XML Interpreter IPC

UDP Port Range is required for media processing. All starting UDP ports are configurable.

Table 58: Required UDP Port Range

Operating System	UDP Port Range
Windows Server 2012 R2	20000 to 45499
Linux	6000 to 32599

Agent Desktop network ports

Agent Desktop uses the following network ports to communicate with the other Contact Center applications and servers.

Feature	Server	Port number
HTTP (Web services)	CCMM	80
HTTPS (Web services)	CCMM	443 (if TLS is enabled on the CCMM server)
CCT	CCT	29373
Web Reporting P2P IMs	CCMS	7081
Voice History (security enabled)	CCMS	443
Voice History (security disabled)	CCMS	80
Aura Presence	Aura Presence Server	5222 (fixed, jabber protocol)
Web Statistics	CCMS	9086
Spark – embedded phone	Communication Manager	6225 – 65535 range

Avaya Aura® Presence Services port requirements

The following table shows the port numbers required for Avaya Aura® Presence Services.

Table 59: Presence Services server port usage

Port	Type	Permit in TCP Filter	Description
5222	XMPP	Yes	Presence Services uses this port to communicate with all XMPP endpoints, including the Contact Center servers, customer-facing servers, and agent desktops.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z