



Avaya Aura[®] Contact Center Fundamentals and Planning

Release 6.4
44400-211
Issue 05.05
May 2015

© 2015 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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

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

Licenses

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

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

applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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.

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: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your

company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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	18
Related resources	18
Viewing Avaya Mentor videos	18
Support	19
Chapter 2: New in this release	20
Features	20
Advanced Screen pops	21
After Call Work Item codes	22
Agent Desktop log file and workflow collection	22
Agent Desktop VMware Horizon View VDI support	23
Avaya Media Server instance licensing	23
Avaya Media Server Zoning	23
Call Join support	23
Extended Email Capacity	24
Force Agent Logout and Change Agent State	24
Hardware Appliance	24
Improved Activity Codes	25
Licensing changes	25
Microsoft Lync Server IM messages	26
Multimedia data management and purging	26
Open Virtual Appliance deployment	26
Phonebook enhancements	27
Proactive Outreach Manager	28
Prompt Management	28
Reporting Source of Call Disconnect for SIP-enabled contact centers	28
Secure RTP in Contact Center	28
Security framework changes	29
Shortcut keys in Agent Desktop	29
Social Networking contact type	29
Supervisor approval of email messages	30
Third call appearance button	30
Toll Free Queuing	31
Increase in call variable limit	31
Whisper Skillset	31
Windows 8.1 Support	31
AML to SIP Migration	31
CCMA password complexity	32
Increase CDN limit for AML-based Contact Center	32
Increase maximum open duration for Multimedia contacts	32
Monitoring of non-skillset calls	32

Part 1: Avaya Aura Contact Center overview	34
Chapter 3: Avaya Aura® Contact Center feature description	35
Contact Center components	38
Contact Center client components	39
Installation configurations	39
Installation configurations for Avaya Aura® Unified Communications platform	41
Installation configurations for Avaya Communication Server 1000 platform	42
Installation configurations for Avaya Aura® Call Center Elite	42
Installation configurations for Multimedia only	43
Avaya Aura® Contact Center domain and workgroup support	43
Avaya Aura® Contact Center firewall considerations	45
Installation process	45
Common utilities	45
Avaya Contact Center Update Manager	46
System Control and Monitor Utility	46
Contact Center Process Monitor	46
Database Maintenance	46
High Availability	47
Grace Period Reset	47
Trace Control Utility	47
Automated Log Archiver	48
Upgrades versus migrations	48
Supported migration options	49
Security framework deployments	52
Chapter 4: SIP-enabled Contact Centers	55
Avaya Aura® Unified Communications platform SIP-enabled contact center	55
Avaya Aura® Communication Manager	56
Avaya Aura® SIP Enablement Services	57
Avaya Aura® Application Enablement Services	57
Avaya Aura® Session Manager	58
Avaya Aura® System Manager	58
SIP-enabled contact center call flow	59
SIP network components	60
Contact Center SIP domain	62
Chapter 5: Avaya Communication Server 1000 AML-based contact center	64
Avaya Communication Server 1000 Switch	65
Switch features	65
Meridian Link Services	66
Supported switch platforms	66
Avaya CallPilot® communication	66
Communication with the Contact Center	66
Chapter 6: Routing options	68

CDNs and SIP Route Points.....	68
Contact routing at the switch.....	69
ACD routing.....	69
Skill-based routing.....	69
Contact queuing and presentation.....	70
Multiple skillsets.....	70
Open Queue.....	71
Network Skill-Based Routing.....	71
Destination sites.....	72
Chapter 7: Contact Center Manager Server.....	73
Installation options.....	73
Components.....	73
Operations performed on the server.....	74
Process voice and multimedia contacts.....	75
Contact routing and queuing.....	75
Multicast communication.....	75
Network routing.....	76
Optional configuration tools.....	77
Programming interfaces.....	77
Web services.....	78
Chapter 8: License Manager.....	79
Installation options.....	79
User configuration.....	79
Operations performed on the server.....	80
Configure and view licenses.....	80
Configure license alarms.....	80
Choose licensing types.....	81
Manage standby license manager.....	82
Update licensing grace period.....	82
Chapter 9: Contact Center Manager Administration.....	84
Installation options.....	84
Default users.....	85
Components.....	85
Operations performed with Contact Center Manager Administration.....	86
Control access to configuration components.....	87
Perform off-line configuration.....	87
Manage users and skillsets for users.....	88
Create script or flow applications.....	88
Report real-time data.....	88
Review real-time reports in Agent Desktop Display.....	89
Report historical data.....	90
Configure emergency support for agents.....	91
Monitor configuration changes.....	91

Create outbound campaigns.....	91
Prompt Management	91
Optional tools.....	92
Data extraction.....	92
AD-LDS replication.....	92
Logon warning message.....	93
Security framework.....	93
Chapter 10: Contact Center Server Utility.....	94
Installation options.....	94
Components.....	94
Operations performed on the server.....	95
Monitor and maintain user permissions.....	95
Configure access classes.....	96
Reset passwords.....	96
Monitor system configuration settings and performance.....	96
Manage alarms and events.....	97
Chapter 11: Communication Control Toolkit.....	99
Installation options.....	99
Modes of operation.....	99
Components.....	100
Operations performed on the server.....	101
Monitor call data.....	101
Configure resources.....	102
Communication Control Toolkit API.....	104
Chapter 12: Contact Center Multimedia.....	105
Installation options.....	105
Default users.....	106
Folder structure.....	106
Components.....	106
Contact Center Multimedia components.....	107
Operations performed on the server.....	109
Configure email settings.....	110
Configure IM settings.....	111
Configure Web communications settings.....	112
Configure outbound settings.....	113
Configure Social Network settings.....	113
Social Media Analytics.....	116
Configure Predictive Outbound settings.....	116
Configure voice mail settings.....	118
Configure scanned document settings.....	118
Configure SMS text settings.....	119
Configure faxed document settings.....	120
Configure Agent Desktop settings.....	121

Configure General settings.....	122
Handle contacts.....	123
View and update customer information.....	124
Create callbacks.....	124
Report multimedia data.....	124
Multimedia data management and purging.....	125
Optional configuration tools.....	128
Contact Center Standby server.....	128
Web services.....	128
Open interfaces for email.....	128
Chapter 13: Avaya Media Server.....	130
Avaya Media Server media files and media management.....	130
Network configurations.....	134
Standalone Avaya Media Server.....	134
Avaya Media Server cluster.....	135
Avaya Media Server High Availability pair.....	138
Multiple Avaya Media Server High Availability pairs.....	140
Avaya Media Server Remote Geographic Node deployment.....	143
Avaya Media Server Zoning.....	144
Chapter 14: High Availability fundamentals.....	149
Campus High Availability.....	149
Contact Center application geographic redundancy.....	151
Geographic High Availability solution.....	151
Database Shadowing.....	153
Trusted IP address.....	153
Contact Center Manager Server.....	154
Contact Center Manager Administration and AD-LDS.....	154
Communication Control Toolkit.....	159
Contact Center Multimedia.....	159
Avaya Media Server.....	160
Standby server hardware requirements.....	163
Campus standby server and network configuration.....	164
Remote Geographic Node server requirements.....	164
Geographic standby server and network configuration.....	165
Simple Network Management Protocol.....	166
Licensing.....	166
Hot patching.....	166
More information.....	167
Chapter 15: Mission Critical High Availability.....	168
Mission Critical HA with Avaya Aura [®] platform resiliency.....	168
Mission Critical HA with Midsize Enterprise.....	170
Mission Critical HA without Avaya Aura [®] platform resiliency.....	171
Mission Critical HA with Avaya Aura [®] Unified Communications Virtualized Environment	173

Mission Critical High Availability overview.....	175
Mission Critical solution.....	177
Mission Critical High Availability configuration utilities.....	178
How to reinstate High Availability resiliency after a switchover.....	181
How to reinstate High Availability resiliency after a total network outage.....	182
How to manually switch over to the Remote Geographic Node of a Mission Critical solution	182
How to revert to the campus site after running the RGN for a few days.....	183
Switchover Handling Script.....	185
Avaya Aura [®] platform campus resiliency.....	187
High Availability campus site.....	187
Communication Manager survivability overview.....	189
Session Manager redundancy overview.....	189
Application Enablement Services Fast Reboot High Availability (FRHA) overview.....	190
Application Enablement Services Machine Preserving High Availability overview.....	191
Avaya Aura [®] Solution for Midsize Enterprise 6.2 Fast Reboot High Availability (FRHA) overview.....	193
Avaya Aura [®] platform geographic resiliency.....	194
Campus site and remote geographic site.....	194
Communication Manager Survivable Core (ESS).....	195
Session Manager geographical redundancy overview.....	196
Application Enablement Services geographical redundancy overview.....	196
Chapter 16: Hot-standby High Availability.....	197
Switchover.....	199
Agent experience during a switchover.....	200
Administrator experience during a switchover.....	200
High Availability Utility.....	201
How to reinstate High Availability resiliency after a switchover.....	202
How to reinstate High Availability resiliency after a total network outage.....	203
How to manually switch over to the Remote Geographic Node in an AML CS1000-based solution.....	204
How to revert to the campus site after running the RGN for a few days.....	205
Chapter 17: Warm standby High Availability.....	206
Switchover.....	208
Agent experience during a switchover.....	209
Administrator experience during a switchover.....	209
High Availability Utility.....	209
How to reinstate High Availability resiliency after a switchover.....	211
How to reinstate High Availability resiliency after a total network outage.....	212
Chapter 18: Avaya Aura[®] Experience Portal Integration.....	213
Data transfer methods.....	215
Avaya Aura [®] Experience Portal Orchestration Designer.....	216
Voice XML.....	216

Call Control XML.....	216
SIP-enabled Avaya Aura® Contact Center.....	217
P-Intrinsic SIP Header.....	217
User-to-User Information.....	218
Universal Call Identifier.....	219
Avaya Aura® Contact Center Web Service Open Interfaces.....	219
Web Services Open Interfaces.....	219
Front-end Avaya Aura® Experience Portal self-service using Contact Center Web Service Open Interfaces.....	220
Call flow example using CCMS Web service Open Interfaces.....	221
Front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center.....	222
Call flow example for front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center.....	224
Back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center.....	225
Call flow example using back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center.....	227
Back-end Avaya Aura® Experience Portal using Context Creation and SIP-enabled Contact Center.....	228
Call flow example using back-end Avaya Aura® Experience Portal with the Context Creation sample application.....	230
Avaya DevConnect.....	232
Chapter 19: Avaya Aura® Call Center Elite integration.....	233
Unified Agent Desktop.....	235
Unified Agent Administration.....	236
Integrated Avaya Aura® Call Center Elite commissioning overview.....	236
Chapter 20: Technical support.....	238
Secure Access Link for remote support.....	238
Microsoft Remote Desktop Connection.....	238
Virtual Private Network.....	238
Direct-connect modem.....	240
Part 2: Interoperability.....	241
Chapter 21: Product compatibility.....	242
Avaya Aura® Unified Communications platform.....	242
Multiple AACC instances and a single UC platform.....	243
Avaya Aura® Unified Communications phones.....	244
Avaya Communication Server 1000 platform.....	245
Avaya Communication Server 1000 phones.....	247
Avaya Communication Server 1000 AML features	248
Avaya Aura® Experience Portal.....	250
Additional voice services.....	252
Unified Reporting and Performance management with Avaya IQ.....	253
Part 3: Licensing requirements.....	255

Chapter 22: Licensing requirements	256
License types	257
Nodal Enterprise licensing	257
Corporate Enterprise licensing	257
Nodal NCC licensing	258
Corporate NCC licensing	258
Essential licensing	259
Licensing mechanisms	259
WebLM licensing mechanism	260
PLIC licensing mechanism	261
How to obtain an Avaya Aura [®] Contact Center license	261
How to obtain a license for a nodal SIP-enabled solution	262
How to obtain a license for a nodal AML-based solution	264
How to obtain a Corporate license	265
How to obtain a license for a multimedia only solution	266
License Manager installation location in a solution	267
Avaya Media Server licensing considerations	268
Licensed packages and features	268
Agent Greeting	268
Avaya Media Server Zoning	268
Contact Recording	269
Multiplicity	269
Networking	269
Offsite Agent	269
Open Interfaces Open Queue	270
Open Interfaces Universal Networking	270
Open Queue	270
Outbound	270
Report Creation Wizard	270
Standby Server High Availability	271
TLS SRTP Signaling and Media Encryption	271
Universal Networking	271
Web Based Statistics	271
Changes to Announcement and Dialog treatment licensing	271
About the license file	273
Interpretation of the license file	273
Contact Center License Manager license identifiers	274
Licensing requirements for Agent Desktop features	277
Licensing grace period	283
Emergency license files	284
License manager statistics	284
Real-time statistics	285
Supported License Manager servers	285

Part 4: Performance specifications	286
Chapter 23: Maximum capacities	287
Maximum capacity overview	287
Maximum agent capacity and call rate values	288
Orchestration Designer application Variables and Intrinsic	295
Email limits and capacity values	296
Contact Center Manager Server Call load	297
Call complexity	297
Call rate	299
Contact Center Multimedia disk storage requirements	299
Required database files	300
Email attachment storage	300
Communication Control Toolkit capacity	301
Call Attached Data considerations	302
CTI application performance impact	302
Access from an external client PC	303
Access from a browser on the Contact Center Manager Server server	303
Landing Pads	303
Open Interfaces Web Service data limits	304
Outbound capacity	304
Chapter 24: Server Specifications	305
Server types and server specifications overview	305
Entry-level solution and server specification	308
Mid-range solution and server specification	311
High-end solution and server specification	317
Server performance and BIOS settings	326
Server firmware	326
Power and performance management	327
Disk caching and RAID	327
Non-Uniform Memory Architecture (NUMA) and memory	328
Performance management and VMware	328
Virtualization technology	328
Hyper-Threading	329
Unused hardware devices	329
Summary	329
Avaya Media Server and Contact Center on one VMware host	330
Hardware Appliance capacity limits	332
Hardware Appliance server specification	333
Chapter 25: SIP Contact Center configuration requirements	335
General requirements	335
SIP-enabled Contact Center feature limitations	335
Dependent platform and switch compatibility	336
Upgrade path	336

Digital Signal Processing Considerations.....	337
Voice over Internet Protocol.....	337
PABX Digital Signal Processors.....	338
Avaya Aura® Shuffling.....	339
PABX DSP consumption examples.....	339
Avaya Communication Server 1000 DSP.....	340
Avaya Aura® Unified Communications platform DSP.....	340
Dialed Number Identification Service.....	340
DNIS Options in SIP-enabled contact centers.....	341
Incoming SIP Invite message with DNIS information in the To header.....	341
Avaya Communication Server 1000 systems.....	341
Incoming SIP Invite message with DNIS information in the History-Info header.....	341
Midsize Business Template systems.....	342
Session Manager systems.....	343
Office Communications Server 2007 hardware requirements.....	343
Chapter 26: Server virtualization support.....	345
VMware support.....	346
VMware features.....	354
VMware vSphere host considerations.....	355
Guidance for storage requirements.....	356
VMware Contact Center Guest Operating Systems.....	357
Overview of commissioning Contact Center with VMware.....	357
Performance monitoring and management.....	359
High Availability and virtualization.....	360
Avaya Aura® Contact Center VMware Snapshot considerations.....	360
Avaya Media Server VMware Snapshot considerations.....	361
VMware networking best practices.....	361
Time synchronization considerations.....	362
Troubleshooting VMware.....	362
Hyper-V support.....	363
Virtual Machine hardware requirements.....	364
Chapter 27: Common server requirements.....	366
Server naming requirements.....	367
Common server disk partitioning requirements.....	367
Operating system requirements.....	368
Operating system installation and configuration.....	369
Microsoft security hotfixes.....	369
Avaya Security Advisories.....	370
Operating system updates.....	370
Service updates.....	370
Service packs.....	371
Java Runtime Environment updates.....	371
Dynamic Host Configuration Protocol support.....	371

Network setup.....	372
Network configuration.....	372
Domains and Windows Server 2008 Release 2 security policies.....	372
Third-party software requirements.....	373
Generic guidelines for utility-class software applications.....	373
Additional guidelines for the use of antivirus software.....	374
Simple Network Management Protocol (SNMP) alerting on virus confirmation.....	375
Remote support access tool.....	375
Hardware requirements.....	375
Redundant Array of Independent Disks (RAID).....	375
Storage Area Network (SAN).....	375
Uninterruptible Power Supply.....	376
Chapter 28: High Availability server requirements.....	377
Mission Critical High Availability.....	377
Hot-standby High Availability.....	380
Warm standby High Availability.....	381
Avaya Aura® Unified Communications platform and Contact Center High Availability.....	382
Avaya Communication Server 1000 and Contact Center High Availability.....	383
High Availability levels supported.....	383
Standby server requirements.....	384
Remote Geographic Node server requirements.....	384
Campus network requirements.....	385
Geographic network requirements.....	386
Chapter 29: Voice and Multimedia Contact Server without Avaya Media Server configuration requirements.....	387
Hardware requirements.....	388
Communication Control Toolkit components.....	389
Communication Control Toolkit supported functionality.....	389
Client Terminal Relationships.....	393
Email message memory requirements.....	394
Calculating disk storage requirements.....	395
Network configuration.....	396
Network interface card binding order.....	396
Maximum acceptable use.....	397
Contact modeling limitations in a network environment.....	397
Contact modeling.....	397
Third-party software requirements.....	397
Third-party backup software.....	398
Voice and Multimedia Contact Server antivirus software.....	398
Chapter 30: Voice Contact Server configuration requirements.....	401
Hardware requirements.....	402
Communication Control Toolkit components.....	402
Communication Control Toolkit supported functionality.....	403

Client Terminal Relationships.....	407
Network configuration.....	408
Network interface card binding order.....	408
Maximum acceptable use.....	408
Contact modeling limitations in a network environment.....	408
Contact modeling.....	408
Third-party software requirements.....	408
Third-party backup software.....	409
Voice Contact Server antivirus software.....	410
Chapter 31: Multimedia Contact Server configuration requirements.....	411
Hardware requirements.....	412
Email message memory requirements.....	412
Calculating disk storage requirements.....	414
Third-party software requirements.....	414
Third-party backup software.....	415
Multimedia Contact Server antivirus software.....	416
Chapter 32: Voice and Multimedia Contact Server with Avaya Media Server configuration requirements.....	417
Hardware requirements.....	418
Avaya Media Server software components.....	419
Avaya Media Server media files and media management.....	419
Communication Control Toolkit supported SIP functionality.....	422
Email message memory requirements.....	426
Calculating disk storage requirements.....	427
Third-party software requirements.....	428
Third-party backup software.....	428
Voice and Multimedia Contact Server with Avaya Media Server antivirus software.....	429
Chapter 33: Avaya Media Server on Linux configuration requirements.....	431
Avaya Media Server software components.....	431
Licensing requirements.....	432
Hardware requirements.....	432
Third-party software requirements.....	432
Antivirus software.....	433
Chapter 34: Multimedia Complement for Elite server configuration requirements..	434
Hardware requirements.....	435
Email message memory requirements.....	435
Calculating disk storage requirements.....	436
Third-party software requirements.....	437
Third-party backup software.....	438
Multimedia Complement for Elite server antivirus software.....	438
Chapter 35: No Switch Configured Multimedia Only configuration requirements...	441
Hardware requirements.....	442
Email message memory requirements.....	442

Calculating disk storage requirements.....	444
Third-party software requirements.....	444
Third-party backup software.....	445
No Switch Configured Multimedia Only antivirus software.....	446
Chapter 36: Network Control Center server configuration requirements.....	448
Hardware requirements.....	449
Third-party software requirements.....	449
Network Control Center server antivirus software.....	449
Chapter 37: Knowledge Worker Server configuration requirements.....	451
Hardware requirements.....	451
Communication Control Toolkit Knowledge Worker supported functionality.....	452
Third-party software requirements.....	453
Knowledge Worker Server antivirus software.....	453
Network configuration.....	454
Network interface card binding order.....	454
Communication Control Toolkit and Avaya Communication Server 1000 Telephony Manager on the ELAN subnet.....	454
Maximum acceptable use.....	455
Knowledge worker environment requirements.....	455
Chapter 38: Administration client configuration requirements.....	456
Client hardware requirements.....	456
Client operating system requirements.....	458
Administration Client Citrix support.....	460
Third-party software requirements.....	461
Chapter 39: Agent Desktop client requirements.....	462
Avaya Aura [®] Agent Desktop localized languages.....	462
Client hardware requirements.....	463
Client operating system requirements.....	465
Agent Desktop client network infrastructure requirements.....	466
VMware Horizon View VDI support.....	477
Client Citrix support.....	479
Agent Desktop thick client deployment.....	479
Third-party software requirements.....	480
Chapter 40: Contact center email server configuration requirements.....	482
Email server requirements.....	483
Email settings.....	483
Aliases.....	484
Using an alias.....	484
Impact of an alias addresses on Contact Center Multimedia.....	484
Contact Center Multimedia and alias configuration.....	485
Outgoing email.....	485
Mailbox requirements.....	485
Chapter 41: Microsoft Lync Server requirements.....	486

Licensing requirements.....	488
Chapter 42: Avaya Aura® Presence Services requirements.....	489
Avaya Aura® Presence Services overview.....	489
Hardware requirements.....	491
Operating system requirements.....	491
Licensing requirements.....	492
High Availability.....	492
Chapter 43: Performance optimization.....	493
Contact Center Manager Server services performance impact.....	493
Host Data Exchange.....	493
Guidelines to minimize capacity requirements.....	495
Steady state operation.....	495
Guidelines for steady state operation.....	495
Guidelines for non-steady state operation.....	495
Contact Center Manager Administration performance.....	496
Contact Center Manager Administration contact center server network impact.....	496
Contact Center Manager Administration client performance.....	498
Contact Center Manager Client CPU impact.....	498
Contact Center Manager Administration CPU load reduction.....	499
Contact Center Manager Administration server.....	499
Contact Center Manager Administration client.....	499
Contact Center Multimedia customer contact ratio.....	499
Contact Center Multimedia bandwidth recommendations.....	500
Communication Control Toolkit guidelines to minimize capacity requirements.....	500
Steady state operation.....	501
Guidelines for steady state operation.....	501
Guidelines for non-steady state operations.....	501
Network Traffic.....	501
Part 5: Security.....	503
Chapter 44: Security.....	504
Contact Center server security.....	504
Stand-alone server security.....	504
Network security.....	504
Avaya Security Advisories.....	505
Secure Access Link feature.....	505
Secure RTP in Contact Center.....	505
Contact Center Manager Server port requirements.....	507
Contact Center Manager Administration port requirements.....	508
Contact Center Multimedia ports.....	509
Communication Control Toolkit port requirements.....	511
Avaya Media Server port requirements.....	511
Agent Desktop network ports.....	514
Avaya Aura® Presence Services port requirements.....	514

Chapter 1: 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.

Related resources

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: New in this release

The following sections describe the new features and changes in Avaya Aura® Contact Center Release 6.4.

Features

New features in the Release 6.4 base build

See the following sections for information about new features in the AACC Release 6.4 base build:

- [Advanced Screen pops](#) on page 21
- [After Call Work Item codes](#) on page 22
- [Agent Desktop log file and workflow collection](#) on page 22
- [Agent Desktop VMware Horizon View VDI support](#) on page 23
- [Avaya Media Server instance licensing](#) on page 23
- [Avaya Media Server Zoning](#) on page 23
- [Call Join support](#) on page 23
- [Extended Email Capacity](#) on page 24
- [Force Agent Logout and Change Agent State](#) on page 24
- [Hardware Appliance](#) on page 24
- [Improved Activity Codes](#) on page 25
- [Licensing Changes](#) on page 25
- [Microsoft Lync Server IM messages](#) on page 26
- [Multimedia archive and purge](#) on page 26
- [Open Virtual Appliance deployments](#) on page 26
- [Phonebook enhancements](#) on page 27
- [Proactive Outreach Manager](#) on page 28
- [Prompt Management](#) on page 28
- [Reporting Source of Call Disconnect for SIP-enabled contact centers](#) on page 28
- [Secure RTP in Contact Center](#) on page 28

- [Security framework changes](#) on page 29
- [Shortcut keys in Agent Desktop](#) on page 29
- [Social Networking contact type](#) on page 29
- [Supervisor approval of email messages](#) on page 30
- [Third call appearance button](#) on page 30
- [Toll Free Queuing](#) on page 31
- [Whisper Skillset](#) on page 31

New features in Release 6.4 Feature Pack 1

See the following sections for information about new features added by Feature Pack 1 (Service Pack 13):

- [Increase in call variable limit](#) on page 31
- [Windows 8.1 support](#) on page 31

New features in Release 6.4 Feature Pack 2

See the following sections for information about new features added by Feature Pack 2 (Service Pack 14):

- [AML to SIP migration](#) on page 31
- [CCMA password complexity](#) on page 32
- [Increase CDN limit for AML-based Contact Center](#) on page 32
- [Increase maximum open duration for Multimedia contacts](#) on page 32
- [Monitoring of non-skillset calls](#) on page 32

Advanced Screen pops

A screen pop is a third-party application that administrators configure using the Multimedia Administration tool. Agent Desktop displays screen pops when a contact alerts or is answered. Administrators can configure these screen pops to display relevant information about the alerting or answered contact based on the intrinsic, such as Skillset, To Address, and DNIS associated with the contact.

Note:

In an AML-based Contact Center intrinsic on voice calls are set only for CDN calls. In a SIP-enabled Contact Center intrinsic on voice calls are set for both CDN and personal calls.

Administrators can configure two types of screen pops: Basic and Advanced. Administrators can use Advanced screen pops to configure individual screen pops to open on specific intrinsic conditions. Advanced screen pops provide administrators with greater range and flexibility with respect to conditions and triggers for opening a particular screen pop.

For information about how to configure screen pops, see *Avaya Aura® Contact Center Server Administration* (44400-610). For more information on how Avaya Aura® Agent Desktop displays screen pops, see *Avaya Aura® Agent Desktop User Guide* (44400-114).

After Call Work Item codes

Agents must enter After Call Work Item (ACW) codes to perform post call processing work such as adding contact information to a CRM system.

Prior to Avaya Aura® Contact Center Release 6.3 SP 10, after call work time was calculated, when an agent entered the Not Ready state for the first time after releasing any contact, except DN calls, whether or not the agent entered the Not Ready code. ACW time ended when the agent left the Not Ready state, placed or received a DN call, or logged off.

When the agents released any contact in Avaya Aura® Contact Center Release 6.3 SP 10, the system automatically used the default ACW code (00000) and placed the agents into after call work state.

In Avaya Aura® Contact Center Release 6.4 Agent Desktop, a new control, **Set ACW Code** is available on the Agent Desktop Top bar menu that agents can use to track ACW time. Alternatively, if administrators select the **Enter ACW using Not Ready Without Reason Code** option under **Global Settings** (use **CCMA > Configuration > Global Settings**), agents who do not enter ACW code after releasing the contact are put into the ACW state automatically by the system using the default ACW code 00000 immediately upon completion of the contact.

Important:

If you are upgrading from a release prior to Avaya Aura® Contact Center Release 6.3 SP 10, where agents used Not Ready reason codes to track after call work, you must upgrade the existing Not Ready codes to be of type ACW. You must also retrain agents to use the new control **Set ACW Code**, on Agent Desktop to set ACW codes. If you continue to use Not Ready reason codes for after call work, it impacts reporting and after call work is not reported correctly.

In a Multimedia Complement for Elite solution, the **Set ACW Code** is not available on Agent Desktop and therefore Agent Desktop does not support this after call work functionality. Agent Desktop reason codes work in the same way as previous releases.

For information about ACW codes, see *Avaya Aura® Agent Desktop User Guide* (44400-114) and *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611).

Agent Desktop log file and workflow collection

The Agent Desktop log file and workflow collection feature allows agents to easily collect all Agent Desktop logs and relevant screen captures. Agents can upload this information directly to the Contact Center Multimedia (CCMM) server with a single click. This feature makes it easier for support staff to quickly gather all the information they need to debug issues on Agent Desktop. For more information about Agent Desktop log file and workflow collection, see *Avaya Aura® Contact Center Troubleshooting* (44400-712).

Agent Desktop VMware Horizon View VDI support

Avaya Aura® 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.

For more information about building a virtual Avaya Aura® Agent Desktop client infrastructure using VMware Horizon View, see [VMware Horizon View VDI support](#) on page 477.

Avaya Media Server instance licensing

Avaya Aura® Contact Center uses WebLM licensing to limit the number of Avaya Media Server instances in a solution. This limit is based on the VALUE_CCTR_AMS_INSTANCE license key number in the WebLM xml license file.

In your WebLM license file, ensure the VALUE_CCTR_AMS_INSTANCE value is equal to the number of Avaya Media Server servers in your solution. For example, an Avaya Media Server High Availability pair requires two Avaya Media Server instance licenses. For more information about the WebLM license file values, see [Contact Center License Manager license identifiers](#) on page 274.

Avaya Media Server Zoning

Avaya Media Server (Avaya MS) Zoning allows contact center administrators to target a specific Avaya MS instance or prioritized list of instances when anchoring incoming contact center calls. The administrator targets the Avaya MS instances through the use of a new scripting command in Avaya Aura® Orchestration Designer (OD). For more information, see [Avaya Media Server Zoning](#) on page 144.

Call Join support

Call Join allows an agent to conference together two previously unrelated voice calls. If an agent is active on a call and has one or two other unrelated calls on hold, Avaya Aura® Contact Center supports joining two calls together and adding parties to the conference until there are six parties live on the conference. Agents must use their desk phones to add and drop calls from the conference. The surviving call after a call join has taken place is the oldest call. Avaya Aura® Contact Center and Avaya Aura® Agent Desktop support Call Join. Avaya Aura® Contact Center agents using Avaya Aura® Agent Desktop with Proactive Outreach Manager (POM) do not support Call Join.

Avaya Aura® Contact Center Release 6.4 supports Call Join when integrated with Avaya Aura® Unified Communications Release 6.2 or later.

Avaya Aura® Contact Center supports Call join only in SIP-enabled contact center solutions using Communication Manager.

Call Join is supported on Communication Manager agent stations with two or three call appearance lines. Call Join is supported out of the box; it does not require configuration.

For more information about Call Join, see *Avaya Aura® Agent Desktop User Guide* (44400-114).

Extended Email Capacity

Currently, the maximum capacity of Open Queue is 20 000 contacts. Email Manager observes the current number of contacts queued and stops processing email messages from the mail server after the number of contacts reaches the upper limit.

The Extended Email Capacity feature increases the email backlog capacity to 100 000 contacts. Contact centers that have large email volumes can use the Extended Email Capacity feature to pull email messages that are present in the CCMM database. Agents can then view email contacts in the CCMM database and search or extract these contacts, while on a voice call with a customer.

By default, the Extended Email Capacity feature is disabled. Customers who require the email backlog capacity to be more than 20 000 must enable this feature. For more information about Extended Email Capacity, see *Avaya Aura® Contact Center Server Administration* (44400-610).

Force Agent Logout and Change Agent State

The Force Agent Logout feature allows a supervisor to remotely log an agent out of Contact Center from the Contact Center Manager Administration (CCMA) user interface. This allows supervisors to log out agents who forget to log out or go not-ready at the end of their shift.

The supervisor can also force an agent state change to toggle it between Ready or Not Ready from the Contact Center Real Time Displays. When they force an agent into the Not Ready state, supervisors have the option to enter a Not Ready Reason code for the agent.

Hardware Appliance

The Avaya Aura® Contact Center (AACC) Hardware Appliance delivers a fully-installed Voice and Multimedia Contact Server with Avaya Media Server solution packaged as a single hardware rack-based server ready for configuration. The AACC Hardware Appliance comprises a Dell™ R620™ server with the Windows Server 2008 operating system and the AACC software preloaded. On startup, the AACC Ignition Wizard guides the installer through the Operating System setup and AACC software configuration.

For more information about the Avaya Aura® Contact Center Hardware Appliance, see [Hardware Appliance capacity limits](#) on page 332.

For more information about the Voice and Multimedia Contact Server with Avaya Media Server, see [Voice and Multimedia Contact Server with Avaya MS configuration requirements](#) on page 417.

Improved Activity Codes

An activity code is a number that an agent can enter on a phone or on Agent Desktop to track time spent on activities and service areas, not ready reasons, and after call work.

A supervisor or system administrator configures activity codes. Administrators define activity codes in Contact Center Manager Server. Activity codes can be alphanumeric.

In Agent Desktop Release 6.3 and earlier, Agent Desktop displayed a list of codes, which were not segmented, under both the Not Ready drop-down list and the Activity Code drop-down list. A user had to segment the codes into Not Ready Codes and Activity Codes based on the naming convention.

In Contact Center Release 6.4, administrators provide all newly entered codes with a discrete type so that Agent Desktop displays the codes under three separate controls:

- Activity codes
- Not Ready Reason codes
- After Call Work Item (ACW) codes

Administrators configure activity codes that correspond to a contact type and a skillset. Therefore, activity codes are filtered on a contact type and skillset basis. Agent Desktop displays the activity codes list based on either the contact skillset or the contact type. For example, if you are handling email contacts, Agent Desktop populates the Activity Code list both with activity codes that correspond to the email contact type and with activity codes that map to the skillset.

Important:

If you are migrating or upgrading your contact center, the existing activity codes are not migrated automatically. However, you can use Contact Center Manager Administration to upgrade the codes. If you do not upgrade the codes to have a specific type, it can impact reporting and how after call work or post-call processing time is calculated.

For information about activity codes, see *Avaya Aura® Agent Desktop User Guide* (44400-114) and *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611).

Licensing changes

AACC Release 6.4 (or Service Pack 12) implements the following licensing changes:

- Prior to Avaya Aura® Contact Center Release 6.4 (Service Pack 12), Contact Center did not enforce the ANNC and DIALOG licenses. Avaya Aura® Contact Center now enforces these licenses.

For more information about ANNC and DIALOG licensing changes, see [Changes to Announcement and Dialog treatment licensing](#) on page 271.

- New AACC Release 6.4 (Service Pack 12) installs do not require CCMM licensing to access the following advanced Agent Desktop functionality in a voice-only configuration:
 - Web Statistics
 - Voice Contact History
 - Drop down list of Activity/Not Ready Reason Codes
 - LDAP address / Phone book
 - Configuration of screen pops in Agent Desktop

The CCMM Database and Administration tools do not require a multimedia license.

Systems installed before AACC Release 6.3 (Service Pack 8) still require CCMM licensing to access advanced Agent Desktop functionality.

Microsoft Lync Server IM messages

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

Microsoft Lync Server is shipped with a desktop client and a Web-based client. These can be used as clients for Microsoft Lync integration.

Avaya Aura® Contact Center supports Microsoft Lync Server Release 2010 and Release 2013.

For more information, see [Microsoft Lync Server requirements](#) on page 486.

Multimedia data management and purging

In Release 6.4, AACC adds a new offline database, a background offline synchronization task, and a new data management tool. The offline synchronization task automatically copies modified and closed contacts from the active MULTIMEDIA database to the OFFLINE database every night.

Administrators no longer archive contacts from the MULTIMEDIA database into an offline file. Administrators now create rules and schedules to clear closed contacts from the MULTIMEDIA database.

For more information about data management and purging Multimedia contacts, see [Multimedia Data Management and Purging](#) on page 125.

Open Virtual Appliance deployment

Avaya Aura® Contact Center supports VMware virtualized environments where some or all of the solution is virtualized. For increased productivity, efficiency, and flexibility, Avaya Aura® Contact

Center supports the VMware Virtual Appliance and Open Virtual Appliance (OVA) deployment methods.

A virtual appliance contains a pre-installed, pre-configured Operating System and an application stack optimized to provide a specific set of services. You can use a single Open Virtual Appliance (OVA) package to distribute a Virtual Appliance. An OVA package includes all of the Open Virtualization Format (OVF) information required to describe and deploy a Virtual Appliance on a VMware host. A Virtual Appliance is pre-packaged; this reduces the complexity of installation and commissioning and reduces the cost of support.

You can use an OVA package to install a Virtual Appliance on a VMware host. You install one OVA package per virtual machine. You can install multiple OVA packages on a single VMware host server, depending on the number of virtual machines (guests) on that host server. The number of virtual machines on a VMware host server depends on the virtual machines' requirements and on the host server hardware specification.

Avaya Aura® Contact Center provides two VMware Virtual Appliances; a SIP-enabled Voice and Multimedia Contact Server OVA and an Avaya Media Server OVA.

For more information, see *Avaya Aura® Contact Center Deployment using VMware in a Virtualized Environment (44400-212)*.

Phonebook enhancements

The Phonebook feature on Agent Desktop has a number of enhancements, which include the following:

- Agents can add custom contacts. Custom contacts are contacts that are not present in the LDAP directory.
- Agents can configure the display of Phonebook. Agents can add or remove columns from the Phonebook grid.
- Agents can decide how many records to display per page in Phonebook.
- Agents can click to call, transfer, and conference from Phonebook.

 Note:

Click to transfer and click to conference are not available in Call Center Elite environments.

- Agent can click to send an email directly from Phonebook.

 Note:

Click to email is not available in Call Center Elite environments.

- Agent can search and filter the list of contacts from LDAP.
- Agents can sort and order columns in Phonebook.
- Agents can tag contacts as favorites and add a contact to the speed dial list.
- Agents can view the call history of the calls made, received, and missed.

- The Call Log icon on the Agent Desktop toolbar has an indicator that informs the agents about the number of missed calls.

For more information about Phonebook enhancements, see *Avaya Aura® Agent Desktop User Guide* (44400-114).

Proactive Outreach Manager

Avaya Aura® Contact Center 6.4 now supports integration with Avaya Proactive Outreach Manager (POM) Release 3.0.1. This integration provides agents with a single desktop experience for inbound and outbound contacts. POM launches calls in anticipation of the agent becoming available, which allows Contact Centers to efficiently contact large volumes of customers. For more information on POM integration, see *Avaya Aura® Contact Center — Proactive Outreach Manager integration guide* (44400-515).

Prompt Management

Contact Center Manager Administration (CCMA) users can use the Prompt Management feature to manage prompts on one or more Avaya Media Server (Avaya MS) servers. The Prompt Management feature provides access control and partitioning. For more information on Prompt Management, see [Prompt Management](#) on page 91.

Reporting Source of Call Disconnect for SIP-enabled contact centers

The Brazilian Presidential Decree 6.523 requires that an agent must not drop a call while talking to a caller who rang the contact center. Contact Center supports Source of Call Disconnect (SOCD) reporting in Avaya Aura® Unified Communications SIP-enabled contact centers. This support for SOCD reporting has full parity with the capability of AML-based contact centers in previous releases. The SOCD information appears in the **Associated Data** field in the Call by Call and Contact Summary reports.

Important:

Avaya Communication Server 1000 SIP-enabled contact centers do not support SOCD reporting.

Secure RTP in Contact Center

In Release 6.4, 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.

For more information on this feature, see [Secure RTP in Contact Center](#) on page 505.

Security framework changes

Contact Center supports security framework deployments that use System Manager as the primary security server. This can be the System Manager of either an Avaya Aura® Communication Manager PABX or an Avaya Communication Server 1000 PABX.

You can upgrade an existing Contact Center security framework deployment, where the primary security server is a Unified Communications Management (UCM) server or a standalone Contact Center Security Framework server. However, you can no longer install a standalone Security Framework server from the Contact Center DVD.

Note:

“Security Framework server” refers to a legacy AACC Windows-based standalone server installed from the Contact Center DVD. The phrase “security framework” refers to a deployment of Contact Center that uses a primary security server to authenticate CCMA log on requests.

Shortcut keys in Agent Desktop

Shortcut keys are added to Agent Desktop to increase the accessibility compliance of Agent Desktop. Shortcut keys also decrease that time that agents take to perform common tasks, such as, Go Ready, Go Not Ready, minimize or maximize Agent Desktop, release an active call, and answer an alerting call. For more information, see *Avaya Aura® Agent Desktop User Guide* (44400-114).

Agent Desktop displays the list of the shortcut keys in a tab on the **Preferences** control.

Administrators configure shortcut keys in the CCMM Administration utility. For more information, see *Avaya Aura® Contact Center Server Administration* (44400-610).

Social Networking contact type

Contact Center Release 6.4 introduces a new Social Networking contact type. The Social Networking contact type provides close 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.

For more information about the Social Networking contact type, see [Configure Social Network settings](#) on page 113.

Supervisor approval of email messages

Supervisors can approve or reject the email messages that agents send to customers, before the email reaches the customers.

 Note:

The approval process applies to email contacts only and does not apply to other contact types such as Fax, Scanned Documents, and SMS.

Based on your quality assurance requirements, regulatory requirements or agent training requirements, some or all of the email messages are sent for supervisor approval before sending the email messages to the customer. Administrators can configure email messages targeted for supervisor approval on a per skillset basis or per agent basis. Email messages targeted for supervisor approval on a per skillset basis means that a percentage (0-100) of email messages sent from a skillset requires supervisor approval. Email messages targeted for supervisor approval on a per agent basis means that a percentage (0-100) of email messages sent by particular agents requires supervisor approval. For example, you can configure that 100% of the email messages sent by new agents require supervisor approval and 50% of email messages sent by agents who have been in the contact center for over six months, require supervisor approval.

 Important:

For approval of agent email messages, administrators must configure an approval skillset to which agent email messages are sent.

Administrators can configure up to five levels of approval before email messages are sent to the customer. The system sends the email message through a hierarchy of supervisors before the final approval is granted.

For information about how to configure supervisor approval of email messages, see *Avaya Aura® Contact Center Server Administration* (44400-610). For more information on how Avaya Aura® Agent Desktop handles the approval of email messages flow, see *Avaya Aura® Agent Desktop User Guide* (44400-114).

Third call appearance button

In a SIP-enabled contact center with an Avaya Aura® Communication Manager Release 6.3 FP3 or later, Avaya Aura® Contact Center supports a maximum of three call appearance buttons configured per agent station with Restrict Last Appearance (RLA) enabled. When Restrict Last Appearance is enabled, the last call appearance button of each agent station is always reserved for outbound calls or consults initiated by the agent.

To support Avaya Aura® Contact Center Third Line Appearance functionality, you must enable Contact Center Manager Server Third Line support and configure a third call appearance button on Communication Manager agent stations.

For more information about configuring call appearance buttons on Communication Manager agent stations, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).

For more information about enabling Avaya Aura® Contact Center Third Line Appearance functionality, see *Avaya Aura® Contact Center Commissioning* (44400-312).

Toll Free Queuing

Toll Free Queuing supports free queuing of calls on SIP-enabled contact centers. Regulations introduced in Germany in 2012 require that callers to contact centers must not be charged for their call while their reason for calling is not being attended to. The Toll Free Queuing feature enables contact centers to implement this regulation. For more information about configuring Avaya Aura® Communication Manager for Toll Free Queuing, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521). For more information about configuring Toll Free Queuing in Contact Center, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611).

Increase in call variable limit

In this release, Contact Center increases the call variable limit from 100 to 500.

Whisper Skillset

In a SIP-enabled Contact Center, Avaya Aura® Contact Center supports an optional configuration to provide Whisper Skillset to agents. The Whisper Skillset feature allows a brief skillset-specific announcement to be played to agents before they are connected to a customer call. For more information on the Whisper Skillset feature, see *Avaya Aura® Contact Center Server Administration* (44400-610).

Windows 8.1 Support

Contact Center client applications, such as Agent Desktop and Contact Center Manager Administration are now supported on Microsoft Windows 8.1 operating system.

AML to SIP Migration

Contact Center Release 6.4 includes changes to the database migration interface and new utilities to support migrating from an AML-based Contact Center to a SIP-enabled one. For more

information about migrations from AML to SIP Contact Centers, see *Avaya Aura® Contact Center Upgrade and Patches* (44400-410).

Avaya has commercial offers to protect the investment of customers migrating from AML-based to SIP-enabled Contact Centers. Refer to the AACC Offer Definition for details of the Avaya Software Investment Protection Policy (ASIPP).

CCMA password complexity

Contact Center Manager Administration (CCMA) implements new password complexity rules for CCMA user passwords. This does not affect existing users: the rules apply only when you change a password.

Increase CDN limit for AML-based Contact Center

The limit for the number of CDNs configured for an AML-based Contact Center is now 2,000, increased from the previous limit of 1,000.

Increase maximum open duration for Multimedia contacts

The limit for the maximum open duration for Multimedia contacts is now 12 hours, increased from the previous limit of one hour.

Monitoring of non-skillset calls

In a SIP-enabled contact center based on a Communication Manager PABX, Contact Center supports supervisors observing and barging-in to non-skillset calls.

You can configure beep tones for both observe and barge-in events. In the CCMA Global Settings window, you can enable beep tone and specify the Communication Manager and the CTI station and beep tone announcement extensions. Before enabling beep tone in CCMA, configure the CTI station and announcement extensions on Communication Manager.

Configuring beep tone requires an additional Communication Manager station license.

The non-skillset call monitoring feature uses a conference resource on the Media Gateway DSPs when a supervisor monitors a call. Check that your Media Gateways have adequate DSP capacity to provide the additional conference resources. The number of extra resources you need depends on the expected maximum number of simultaneous monitoring sessions, plus one additional conference resource if you implement beep tone. Refer to your Communication Manager documentation for engineering guidelines.

For more information about enabling beep tone in CCMA, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611). For more information about configuring

beep tone on Communication Manager, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).

Part 1: Avaya Aura Contact Center overview

Chapter 3: Avaya Aura® Contact Center feature description

This section describes Avaya Aura® Contact Center Release 6.4 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).
- Multimedia complement to an Avaya Aura® Call Center Elite voice-based call center. Install this server to add multimedia contact routing support to a new or existing Avaya Aura® Call Center Elite voice-based solution.
- No Switch Configured. Select this option when installing Avaya Aura® Contact Center to support only multimedia contacts. Install this server type when there is no existing voice-based call center, or when integration with a voice contact center is not required.
- Avaya Aura® Contact Center Knowledge Worker solution for AML-based Avaya Communication Server 1000. Knowledge Worker solutions support only voice calls, they do not support multimedia contacts. Knowledge Worker solutions do not support routed voice contacts or skill-based routing.

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 Media Servers in the contact center solution. Avaya 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 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 Avaya Aura® 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 Media Servers in the contact center solution. Avaya 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 Avaya Aura® 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 Avaya Aura® 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 Avaya Aura® 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 Avaya Aura® 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 Avaya Aura® 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)

AACC Multimedia Complement for Elite — Install this server to add multimedia contact routing support to a new or existing Avaya Aura® Call Center Elite voice-based solution. This server supports contact routing for web communications, fax messages, SMS text messaging, and email messages, with additional support for peer-to-peer Instant Messaging (IM). In an Elite Complement solution, agents download and install Avaya Aura® Agent Desktop software from the Multimedia Complement for Elite server. Administrators configure Agent Desktop features and functions using the CCMM Administration utility installed on the Multimedia Complement for Elite server.

A Multimedia Complement for Elite 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

No Switch Configured Multimedia Only — Install this server to provide multimedia contact routing. This server supports contact routing for web communications, fax messages, SMS text messaging, and email messages, with additional support for peer-to-peer Instant Messaging (IM). Choose this server type when there is no existing voice-based call center, or when multimedia integration with a voice contact center is not required. In a multimedia only solution, agents download and install Avaya Aura® Agent Desktop software from the No Switch Configured Multimedia Only server. Administrators configure Agent Desktop features and functions using the CCMM Administration utility installed on the No Switch Configured Multimedia Only server. A Multimedia standalone 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
- Avaya Media Server Windows version

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

Knowledge Worker Server Only — Install a Knowledge Worker server to provide Computer-Telephony Integration (CTI) functionality and call data handling capabilities. A Knowledge Worker Server has the following components:

- Communication Control Toolkit Knowledge Worker version
- Contact Center License Manager

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

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 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 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 Media Server Windows version
	Voice Contact Server Only	• Contact Center Manager Server • Contact Center License Manager • Contact Center Manager Server Utility

Table continues...

Voice platform	Server type	Components
		• Contact Center Manager Administration • Communication Control Toolkit
	Multimedia Contact Server Only	• Contact Center Multimedia
	Avaya Media Server on Linux	• Avaya 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 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
	Knowledge Worker Server Only	• Communication Control Toolkit Knowledge Worker version • Contact Center License Manager
Avaya Aura® Call Center Elite	AACC Multimedia Complement for Elite	• Contact Center Manager Server • Contact Center License Manager • Contact Center Manager Server Utility • Contact Center Manager Administration • Communication Control Toolkit • Contact Center Multimedia
No voice platform	No Switch Configured Multimedia Only	• Contact Center Manager Server • Contact Center License Manager • Contact Center Manager Server Utility • Contact Center Manager Administration • Communication Control Toolkit • Contact Center Multimedia • Avaya Media Server Windows version

Table continues...

Voice platform	Server type	Components
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.

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 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 Media Server and one or more Avaya 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 Media Server and two or more Avaya 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 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 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.]

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.]

For AML-based Avaya Communication Server 1000 platform knowledge worker solutions (non contact center solutions), use the following:

- One Knowledge Worker Server Only. [Requires one Contact Center Windows server.]

Installation configurations for Avaya Aura® Call Center Elite

Each Avaya Aura® Call Center Elite Multimedia Complement contact center solution must contain the following:

- One AACC Multimedia Complement for Elite server. This server type is suitable for multimedia only contact centers not using High Availability. [Requires one Contact Center Windows server.]

OR

- Two AACC Multimedia Complement for Elite servers. These server types are suitable for multimedia only contact centers using High Availability. [Requires two Contact Center Windows servers.]

Installation configurations for Multimedia only

Each multimedia only contact center solution must contain the following:

- One No Switch Configured - Voice and Multimedia Contact Server. This server type is suitable for multimedia only contact centers not using High Availability. [Requires one Contact Center Windows server.]

OR

- Two No Switch Configured - Voice and Multimedia Contact Servers. These server types are suitable for multimedia only contact centers using High Availability. You must uninstall Avaya Media Server software from both servers before enabling High Availability. [Requires two Contact Center Windows servers.]

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 Aura® 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 Aura® 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 Communication Server 1000 AML-based solutions using the Knowledge Worker version of Communication Control Toolkit are supported in a domain or in a workgroup. This solution type does not support High Availability.

Avaya Aura® Contact Center domain considerations

Avaya Aura® Contact Center supports only a Windows Server 2003 Active Directory domain or a Windows Server 2008 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 (CCMS, CCMA, CCT, and CCMM) 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 Aura® 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 www.avaya.com/support.
- 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 Aura® Agent Desktop client computers support both DHCP and static IP addresses.

Avaya Aura® Contact Center firewall considerations

Avaya Aura® Contact Center supplies 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.

Use the Platform Vendor Independence utility in conjunction with the guidelines stated in this document. 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 Update Manager](#) on page 46
- [System Control and Monitor Utility](#) on page 46
- [Contact Center Process Monitor](#) on page 46
- [Database Maintenance](#) on page 46
- [High Availability](#) on page 47
- [Grace Period Reset](#) on page 47
- [Trace Control Utility](#) on page 47
- [Automated Log Archiver](#) on page 48

Avaya Contact Center Update Manager

Use the 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).

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.

Contact Center Process Monitor

Contact Center Process Monitor is a tool that you use to influence the CPU usage of Contact Center processes. The Process Monitor provides monitoring and control features to ensure that no process can over consume CPU cycles and compromise the operation of the Contact Center.

Each process is monitored according to parameters for CPU usage. Control over processes is exercised by changing the priorities when usage exceeds defined values.

You must change the Contact Center Process Control only if you have serious performance issues.

Database Maintenance

The Contact Center Manager Server, 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, Communication Control Toolkit, or Contact Center Multimedia databases:

- change the database port number
- migrate the database from Avaya NES Contact Center Release 6.0 to Avaya Aura® Contact Center Release 6.4 (Caché) format
- create a backup location on a network drive
- perform an immediate backup
- perform a scheduled backup
- restore the database

You can backup the Contact Center Manager 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 149.

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 82.

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 Media Server), all component logging is now on by default at an appropriate log level based on customer requirements review. A circular logging process occurs with a similar file name to configure a number of log files for each server. The user bounds the disk footprint of 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

For an upgrade, you reuse an existing server with a previous version of Contact Center software installed, and then upgrade the software to Contact Center Release 6.4 on the same server.

Upgrades from Avaya NES Contact Center (on Windows 2003 servers) to Avaya Aura® Contact Center Release 6.4 (on Windows 2008 servers) are not supported.

You can upgrade from earlier releases of Avaya Aura® Contact Center to Avaya Aura® Contact Center Release 6.4 by applying the appropriate upgrade Service Packs.

For a migration, you install a new Microsoft Windows 2008 server with a fresh version of Contact Center Release 6.4 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 6.4 on a new Windows 2008 server.
3. Restore the old Contact Center databases to the new Avaya Aura® Contact Center Release 6.4 server, converting the old databases where necessary.
4. Configure Avaya Aura® Contact Center Release 6.4.

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 6.4 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 Media Server:

- Migrate data from an existing Release 6.2 or 6.3 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 Media Server Release 6.4.
- Migrate data from an existing Release 6.2 or 6.3 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 Media Server Release 6.4.
- Migrate data from Avaya NES Contact Center 6.0 or 7.0 to one new Voice and Multimedia Contact Server without Avaya Media Server Release 6.4.
- Migrate a Release 6.4 Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Media Server to a new server. For example, to move Voice and Multimedia Contact Server without Avaya 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 6.2 or 6.3 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 6.4.

- Migrate data from an existing Release 6.2 or 6.3 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 6.4.
- Migrate data from Avaya NES Contact Center 6.0 or 7.0 to one new Release 6.4 Voice Contact Server.
- Migrate a Release 6.4 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 6.2 or 6.3 Contact Center Multimedia server to one new Avaya Aura® Contact Center Multimedia Contact Server Release 6.4.
- Migrate data from Avaya NES Contact Center 6.0 or 7.0 to one new Multimedia Contact Server Release 6.4.
- Migrate a Release 6.4 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 Media Server:

- Migrate data from an existing Release 6.2 or 6.3 single-server with Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, Contact Center Multimedia and Avaya Media Server to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Media Server Release 6.4.
- Migrate data from an existing Release 6.2 or 6.3 Contact Center Manager Server server, Contact Center Manager Administration server, Communication Control Toolkit server, Contact Center Multimedia server, and Avaya Media Server server to one new Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Media Server Release 6.4.
- Migrate a Release 6.4 Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Media Server to a new server. For example, to move Voice and Multimedia Contact Server with Avaya Media Server software from one server to a new larger and faster server.

The following contact center components can migrate to an Avaya Aura® Contact Center Multimedia Complement for Elite Server:

- Migrate a Release 6.4 Multimedia Complement for Elite Server to a new server. For example, to move Multimedia Complement for Elite Server software from one server to a new larger and faster server.

The following contact center components can migrate to an Avaya Aura® Contact Center No Switch Configured Multimedia Only Server:

- Migrate a Release 6.4 No Switch Configured Multimedia Only Server to a new server. For example, to move No Switch Configured Multimedia Only 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 Knowledge Worker Server:

- Migrate data from an existing Communication Control Toolkit Knowledge Worker server to a new Avaya Aura® Contact Center Knowledge Worker Server.
- Migrate data from an Avaya NES Contact Center 6.0 or 7.0 Communication Control Toolkit Knowledge Worker server to an Avaya Aura® Contact Center Knowledge Worker Server.
- Migrate a Release 6.4 Avaya Aura® Contact Center Knowledge Worker Server to a new server. For example, to move Knowledge Worker 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 6.4 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 Media Server migrations are supported:

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

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

Security framework deployments

The Contact Center security framework provides an identity management mechanism that uses integration with a directory services infrastructure (for example Active Directory) for authentication of CCMA users. This helps to reduce administrative costs, and eliminates the redundant user information associated with per-application authentication solutions.

Where Contact Center implements a security framework, the CCMA Internet Information Server (IIS) redirects new CCMA client requests for the CCMA log on page to a primary security server. The primary security server serves a log on page to the CCMA client and performs the authentication. Following a successful authentication, the primary security server redirects the original log on request to CCMA with an authentication header. CCMA logs on the CCMA client.

Contact Center supports three deployments of security framework, although two of these are for upgraded systems only:

- For new Contact Center installs, the primary security server is the 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. Contact Center supports only System Manager R6.2 or R6.3 as a primary security server.

Earlier releases of Contact Center supported using Unified Communications Management (UCM) as the primary security server. You can upgrade a Contact Center deployment that already uses this existing framework.

- Earlier releases of Contact Center supported a standalone AACC Security Framework server. You can upgrade a Contact Center deployment that uses an existing Security Framework server.

You can no longer install a standalone Security Framework server from the Contact Center DVD.

A core feature of security framework is Single Sign-On (SSO) , which 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 single sign-on for multiple applications in your network, you must configure all relevant applications to access the primary security server.

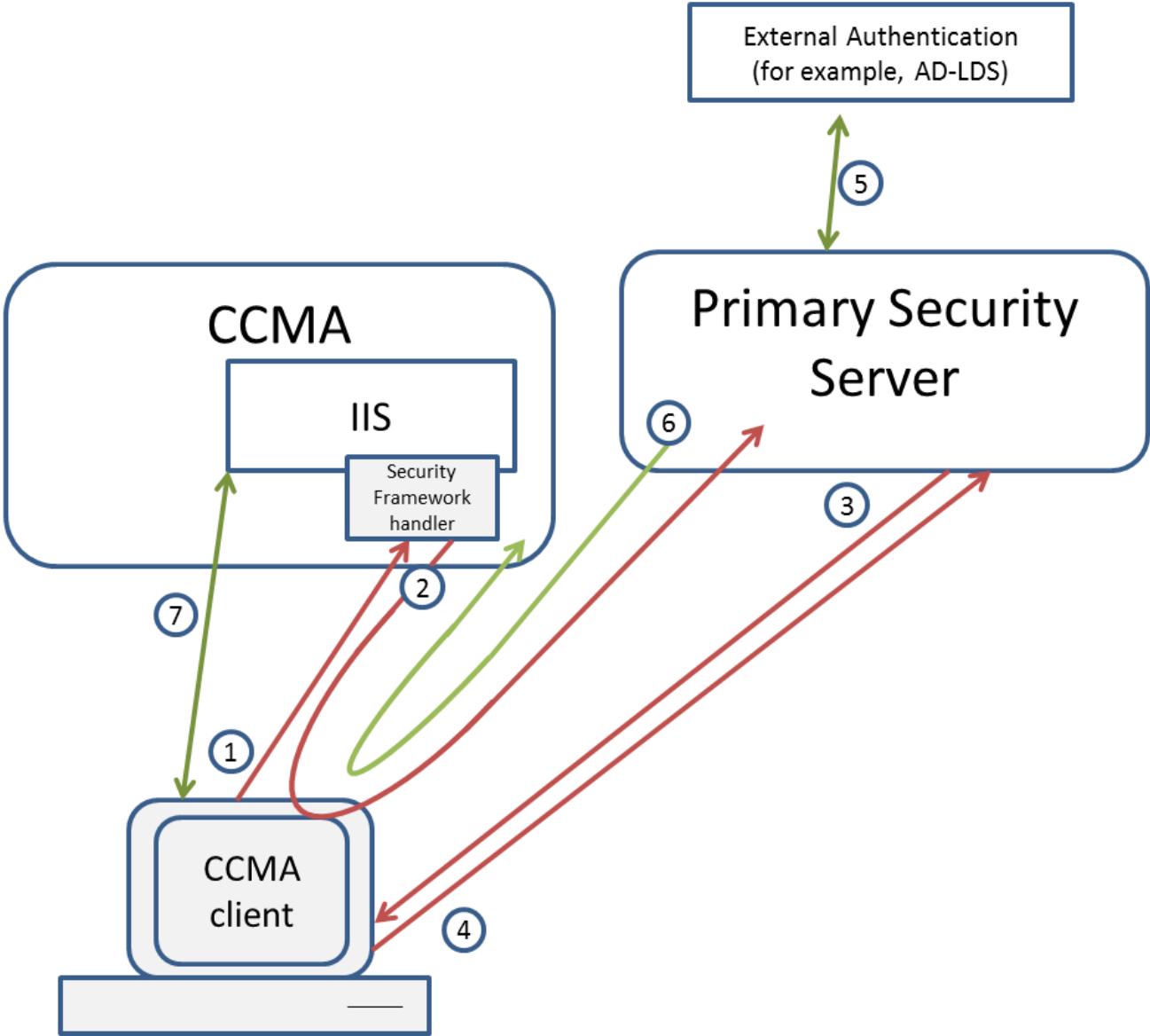


Figure 1: Contact Center security framework authentication sequence

1.	A CCMA client requests the log on page, but the request does not have an authentication header.
2.	The security framework handler redirects the client to the primary security server.
3.	The primary security server serves a log on page to the CCMA client.
4.	The CCMA client user provides their log on credentials.
5.	The primary security server sends the user credentials to External Authentication.
6.	If the user credentials are correct, the primary security server redirects the client to the CCMA IIS instance with the authentication header.

Table continues...

7.	CCMA logs on the user and all subsequent requests for this session use the authentication header.

Chapter 4: SIP-enabled Contact Centers

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

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

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

Avaya Aura® Unified Communications platform SIP-enabled contact center

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

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

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

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

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

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

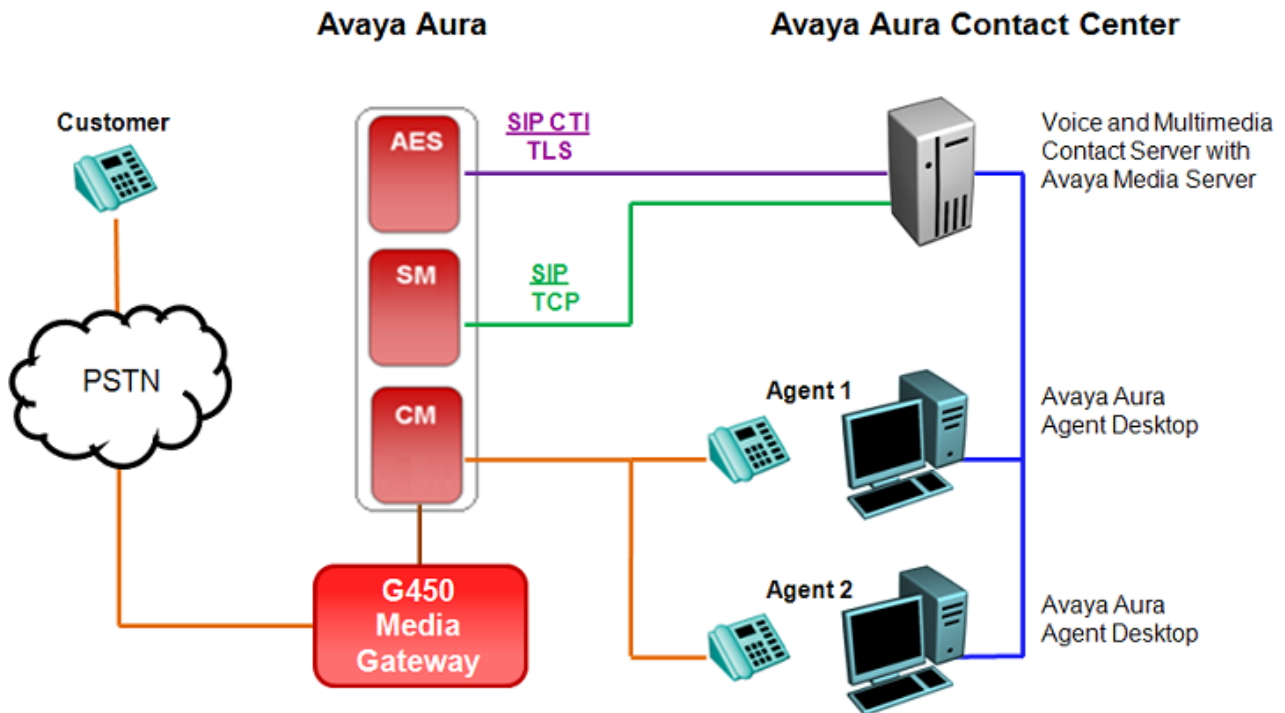


Figure 2: Typical SIP-enabled contact center using the Avaya Aura® Unified Communications platform

For more information about configuring an Avaya Aura® Unified Communications platform-based contact center, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).

Avaya Aura® Communication Manager

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

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

- Configure the Communication Manager stations for Avaya Aura® Contact Center agents.

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

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

Avaya Aura® SIP Enablement Services

Avaya Aura® SIP Enablement Services provides connectivity, integration, and a smooth migration path to SIP-enabled communications. You can use SIP Enablement Services to deploy SIP telephony alongside analog, digital, and IP telephones. SIP Enablement Services supports SIP trunking, SIP stations, presence, instant messaging, and other SIP-enabled applications.

You can redirect SIP calls to the Avaya Aura® Unified Communications platform to Contact Center for treatments, and routing to skillsets. To achieve this, you must configure the SIP Enablement Services server to trust the Contact Center Manager Server.

To determine which calls to redirect to Contact Center Manager Server for processing, in SIP Enablement Services, configure a routing entry and the contact details for Contact Center Manager Server .

Important:

Avaya Aura® Contact Center does not support Avaya Aura® SIP Enablement Services for new installations. Avaya Aura® Contact Center solutions already using SIP Enablement Services still support SIP Enablement Services.

Avaya Aura® Application Enablement Services

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

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

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

You can obtain a root certificate from your Certificate Authority. A root certificate is an unsigned public key that identifies the Root Certificate Authority (CA). Add the root certificate to the AES

server and then use the root certificate to generate a Certificate Signing Request (CSR). Send the CSR and the Common Name (CN) of the AES server to your CA. The CA verifies the identity of the request and issues a signed certificate (a private key) for the AES server.

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

Avaya Aura® Contact Center supplies a set of default certificates for use with AES. If you do not have access to or require a third-party Certificate Authority, you can install these Contact Center default certificates on the Application Enablement Services server to quickly establish a link between the two systems.

! Important:

AES 6.2 and later includes the default trust certificates. Using the default certificates, Avaya Aura® Contact Center automatically communicates with AES.

*** Note:**

The Contact Center default certificates for Application Enablement Services might not meet the security requirements of your organization. Avaya recommends that you use a third-party Certificate Authority or follow your organization's security policies to better secure the link between Avaya Aura® Contact Center and the Avaya Aura® Application Enablement Services server.

Avaya Aura® Session Manager

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

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

Avaya Aura® System Manager

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

SIP-enabled contact center call flow

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

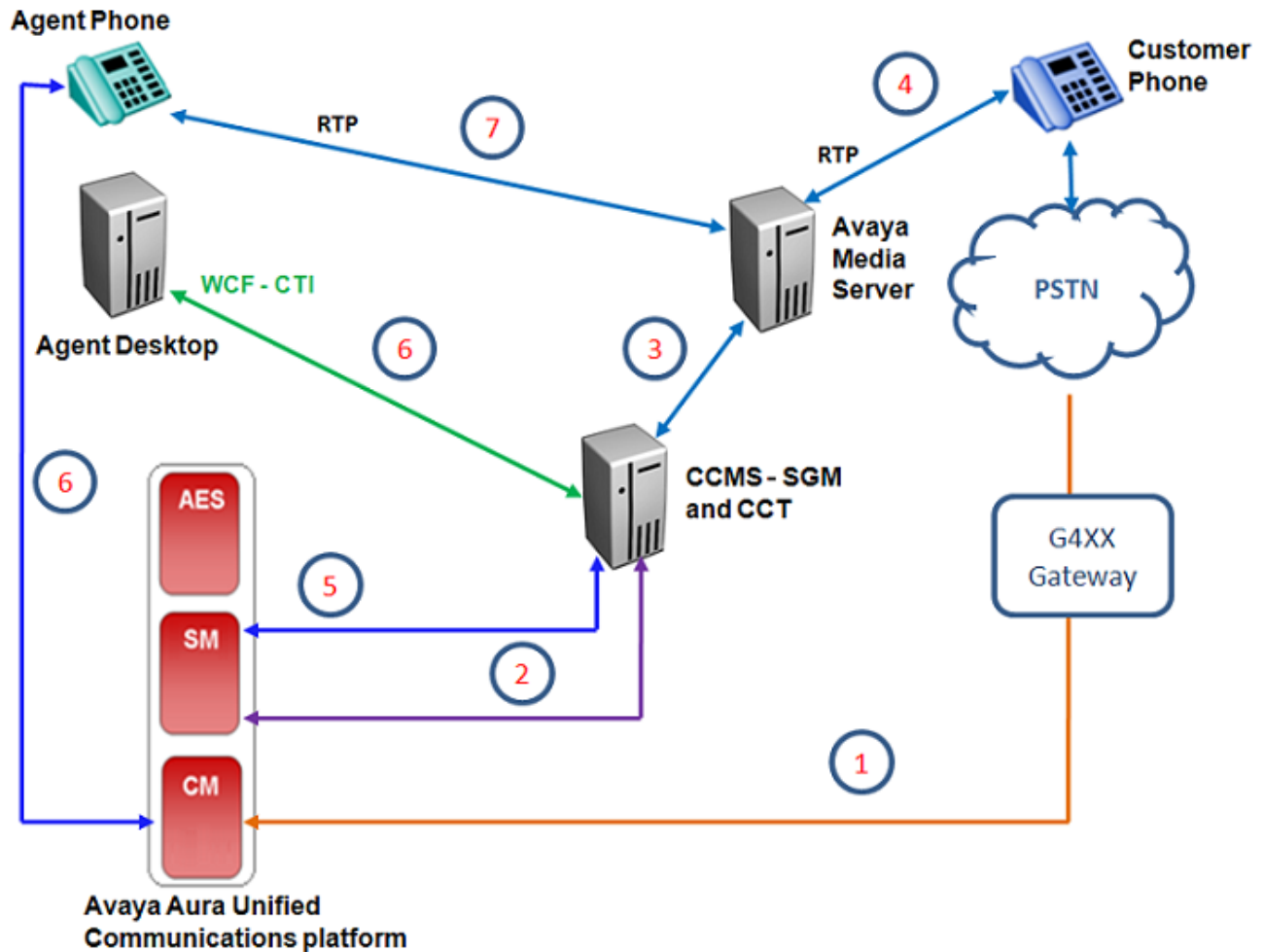


Figure 3: SIP-enabled contact center typical call flow example

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

1. A customer calls the contact center. Communication Manager examines the incoming number and routes the call to a signaling group destined for Session Manager.
2. Session Manager routes the call to Avaya Aura® Contact Center based on matching dial patterns, Linux regular expressions, and routing policies, entity links, and SIP entities. Session Manager then sends a SIP INVITE message to Contact Center.
3. When the SIP INVITE message arrives at the Contact Center Manager Server (CCMS), CCMS matches the message with one of the configured Route Point URIs. CCMS then anchors the customer call on an Avaya Media Server conference port.

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

Avaya Media Server establishes a conference between the agent and the customer and the customer and the agent can now communicate. You can delete the last sentence as it is not required.

SIP network components

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

SIP Proxy server

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

SIP Voice Proxy server

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

SIP CTI Proxy server

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

SIP Endpoint

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

SIP Entity

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

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

SIP User Agent (UA)

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

A SIP User Agent:

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

Examples of contact center SIP User Agents:

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

SIP BBUA

A SIP Back-to-Back User Agent (BBUA) is an entity that intercepts and modifies messaging between a UAS and a UAC. A SIP Back-to-Back User Agent provides intelligent call control for the local party. The Avaya Aura® Contact Center SIP Gateway Manager component functions as a BBUA intercepting the incoming customer calls. SIP Gateway Manager provides call treatments and assistance to customers.

SIP domain

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

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

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

Contact Center SIP domain

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

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

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

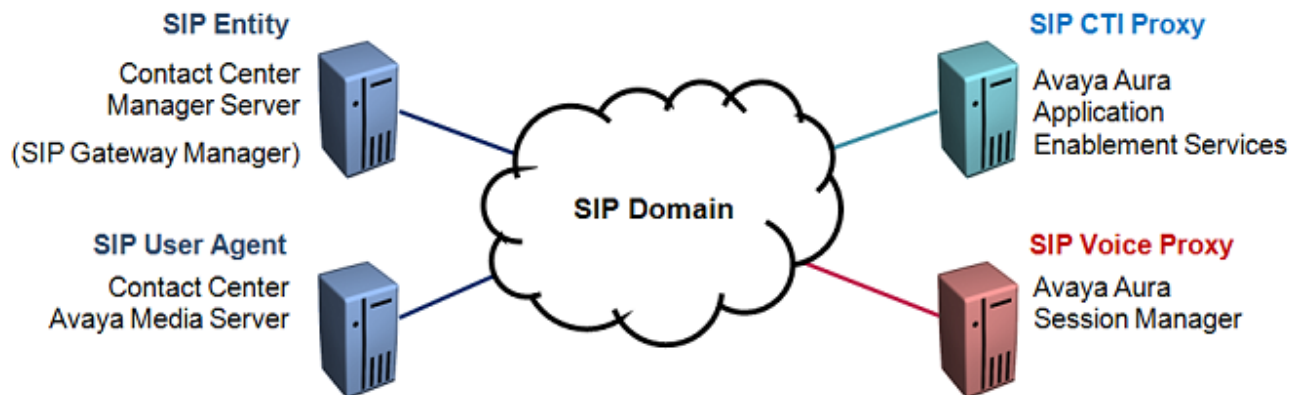


Figure 4: Example of a typical Contact Center SIP domain

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

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

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

Chapter 5: Avaya Communication Server 1000 AML-based contact center

In AML-based contact centers, Contact Center Manager Server (CCMS) controls Avaya Communication Server 1000 Controlled Directory Numbers (CDNs). The CCMS server communicates with the Avaya Communication Server 1000 Call Server using an Application Module Link (AML) protocol over an Embedded LAN (ELAN). Each CCMS requires a dedicated Avaya Communication Server 1000 Call Server to support contact center voice calls. Using a CCMS to control contact center calls ensures CCMS can support skill-based routing, call treatments, and reporting. In AML-based contact centers, TDM-based phones connect directly to the Call Server.

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

The following diagram shows a typical AML-based contact center.

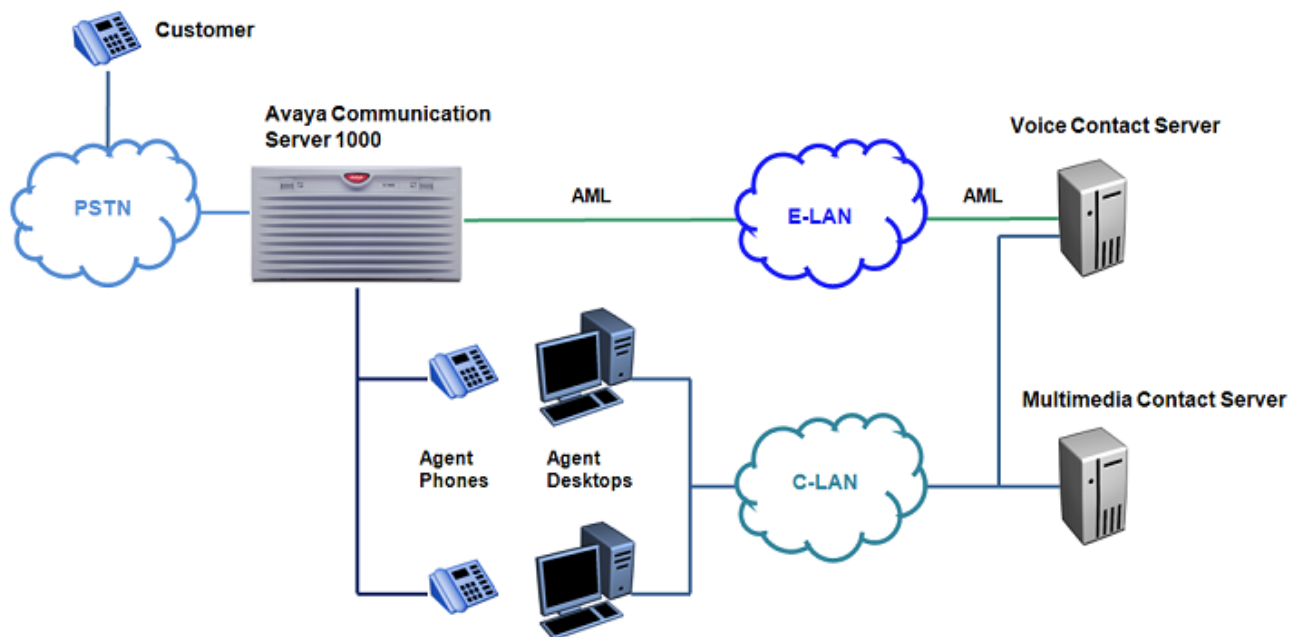


Figure 5: Example of a typical Avaya Communication Server 1000 AML-based contact center

Avaya Communication Server 1000 Switch

The private branch exchange (PBX) or switch provides a speech path for a voice contact between the source (usually a trunk) and the destination (a RAN trunk, voice port, or agent). Two connections to the switch interact with voice-processing systems: voice paths and signaling links.

Avaya Communication Server 1000 Release 5.0 to Release 7.0 supports the Avaya Networking Routing Service (NRS) application as a SIP Voice Proxy. Avaya Communication Server 1000 Release 7.5 and 7.6 do not support the NRS.

Avaya Communication Server 1000 Release 7.5 and 7.6 use Session Manager as the SIP Voice Proxy. For more information about configuring Session Manager to support Avaya Communication Server 1000, see *Avaya Aura® Contact Center Configuration – Avaya CS1000 Integration* (44400-512).

Avaya Communication Server 1000 supports AML-based and SIP-enabled contact centers. For more information about Avaya Communication Server 1000 in SIP-enabled contact centers, see *Avaya Aura® Contact Center Configuration – Avaya CS1000 Integration* (44400-512).

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 Avaya Aura® 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.

Important:

Avaya Aura® Contact Center Release 6.4 does not support SIP-enabled Avaya Communication Server 1000 for new installations. Existing Avaya Aura® Contact Center solutions using SIP-enabled Avaya Communication Server 1000 can be expanded or upgraded.

You must install the most recent service packs on the switch and make the switch operational. For information about which service pack to install on the switch, see the Avaya Web site (www.avaya.com/support).

Switch features

The Avaya Communication Server 1000 switch offers the following features:

- Meridian Link Services (MLS)
- Avaya CallPilot®
- Meridian Integrated Recorded Announcement (MIRAN)

Meridian Link Services

Meridian Link Services (MLS) is a process running on Contact Center Manager Server that provides Computer Telephony Integration (CTI) server access to the Meridian Link interface. Through MLS, the server can connect to Meridian Link applications over the Contact Center subnet.

External applications register with MLS to access application layer messages. MLS commands that result in call processing requests are sent over the ELAN subnet to the switch. Examples of external applications that can register with MLS include software that supports Computer Telephony Integration.

Supported switch platforms

Contact Center provides support for the Avaya Communication Server 1000 software releases and switching platforms for AML or standard Contact Center Manager Server.

Avaya CallPilot® communication

Avaya CallPilot® provides Voice/Fax Messaging as well as integrated Unified Messaging capabilities through the users' familiar desktop email environment or Web-based Unified Messaging and personal mailbox management with My Avaya CallPilot®. Avaya CallPilot® is an optional component to use with your Contact Center environment.

The Avaya CallPilot® voice channels connect to the switch by a DS30 cable. On the switch side, you configure this card as an SL1 phone TN (virtual agent).

Contact Center Manager Server also communicates with Avaya CallPilot® to instruct it to play prompts, play broadcast announcements, and collect digits that callers enter.

Communication with the Contact Center

The Contact Center Manager Server communicates with the switch and the voice-processing system.

Configure the speech paths necessary to connect calls to voice ports, agents, or RAN trunks, and to provide tone treatments (such as ringback and busy) to voice contacts. Contact Center Manager Server communicates with the switch over the Embedded Local Area Network (ELAN) subnet and the contact center subnet using the Application Module Link (AML) protocol. The switch and Contact Center interaction requires the following types of subnets for communication:

- ELAN subnet—An optional dedicated Ethernet TCP/IP LAN that connects the Contact Center Manager Server to the switch.

- Contact center subnet—The LAN to which your corporate services and resources connect. The Contact Center Manager Server and clients connect to the contact center subnet. Third-party applications that interact with the server also connect to this LAN.

Chapter 6: 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 login.

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.

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 7: 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
- Multimedia complement to an Avaya Aura® Call Center Elite voice-based call center
- No Switch Configured multimedia only

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
- AACC Multimedia Complement for Elite
- No Switch Configured Multimedia 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* (44400-610):

- 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 and the warm standby. 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 75
- [Contact routing and queuing](#) on page 75
- [Multicast communication](#) on page 75
- [Network routing](#) on page 76

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 *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (44400-510).

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.

For more information about installing and commissioning the Network Control Center, see *Avaya Aura® Contact Center Installation* (44400-311) and *Avaya Aura® Contact Center Commissioning* (44400-312).

Optional configuration tools

Two programming tools are available with Contact Center Manager Server:

- [Programming interfaces](#) on page 77
- [Web services](#) on page 78

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 8: 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. For more detailed information about Contact Center licensing, see [Licensing requirements](#) on page 492.

Installation options

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

- Voice and Multimedia Contact Server
- Voice Contact Server Only
- AACC Multimedia Complement for Elite
- No Switch Configured Multimedia Only
- Network Control Center Server Only
- Knowledge Worker 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 to configure Contact Center licensing. Contact Center License Manager supports the following license file types:

- **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.
- **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.

- **Avaya WebLM server on a virtual guest:** Contact Center License Manager supports the Virtualized Environment deployment of Avaya WebLM server. Install and commission a suitably licensed WebLM server on a virtual guest in your solution. Contact Center License Manager then obtains licenses from this WebLM server, and uses these licenses to control Avaya Aura® Contact Center licensed features. Deployments that use Avaya WebLM server on a virtual guest do not support the Avaya Aura® Contact Center High Availability feature.

For full details on the license file types and license deployment options, see [Licensing mechanisms](#) on page 259.

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



Caution:

Do not change the extension of the 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](#) on page 80
- [Configure license alarms](#) on page 80
- [Choose licensing types](#) on page 81
- [Manage standby license manager](#) on page 82
- [Update licensing grace period](#) on page 82

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 minute 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.

Choose licensing types

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

Essential licensing

Essential licensing supports entry-level, voice-only, single-site, single-server Contact Centers. All Essential licensing options are in a single license file managed by the co-resident License Manager. Avaya Aura® Contact Center supports upgrading from an entry-level voice-only Essential license to a full-featured multimedia Enterprise license.

Important:

Avaya Aura® Contact Center Release 6.4 does not support Essential licensing for new installations. Existing Avaya Aura® Contact Center solutions using Essential licensing can be expanded, upgraded, or migrated.

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 Media Server does not support the grace period.

Chapter 9: 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
- AACC Multimedia Complement for Elite
- No Switch Configured Multimedia 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 85
- [Components](#) on page 85

If you plan to report on data from an Avaya NES Contact Center Release 6.0 server, you must also install the following software:

- Sybase Open Client 12.5
- Update for Sybase ODBC driver

Default users

The installation adds default users to the Windows operating system when you install Contact Center Manager Administration. 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 an administrator account for the Contact Center Manager Administration server. The iceAdmin account is a MS Windows account.
- **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. The default password for the IUSR_SWC account is the same as the iceAdmin password.
- **webadmin**—An administration user that has access to all configuration components on Contact Center Manager Administration, including the component to create new users. You must use the webadmin account to configure other administrators. These new user accounts can then be used to manage the system rather than the webadmin account. The webadmin account is an application level account, it is not a MS Windows 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 Manager Administration – Client Administration* (44400-611):

- **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.
- **Active Directory Lightweight Directory Services (AD-LDS) Port Configuration**—Configure the ports for the AD-LDS or ADAM replication of the Contact Center Manager Administration data.
- **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

- Access and Partition Management (see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611))
- Configuration (see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611))
- Scripting (see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (44400-510))
- Multimedia (see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611))
- Real-Time Reporting (see *Avaya Aura® Contact Center Performance Management* (44400-710))
- Historical Reporting (see *Avaya Aura® Contact Center Performance Management* (44400-710))
- Report Creation Wizard (see *Avaya Aura® Contact Center Performance Management* (44400-710))
- Prompt Management (see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611))
- Emergency Help (see *Avaya Aura® Contact Center Performance Management* (44400-710))
- Audit Trail (see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611))
- Agent Desktop Displays (see Agent Desktop Displays online Help)
- Outbound (see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611))
- Call Recording and Quality Monitoring (see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611))
- CCMA database—The CCMA database is configured using the Contact Center Manager Administration application. The CCMA database stores reports, report schedules, and report statistics.

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](#) on page 87
- [Perform off-line configuration](#) on page 87
- [Manage users and skillsets for users](#) on page 88
- [Create script or flow applications](#) on page 88

- [Report real-time data](#) on page 88
- [Review real-time reports in Agent Desktop Display](#) on page 89
- [Report historical data](#) on page 90
- [Configure emergency support for agents](#) on page 91
- [Monitor configuration changes](#) on page 91
- [Create outbound campaigns](#) on page 91
- [Prompt Management](#) on page 91

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 Manager Administration – Client Administration* (44400-611).

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* (44400-610). 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 Manager Administration – Client Administration* (44400-611).

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 Manager Administration – Client Administration* (44400-611).

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 a your client computer to upload your Contact Center Manager applications.

For more information about creating applications in the Orchestration Designer, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (44400-510).

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 *Avaya Aura® Contact Center Performance Management* (44400-710). To understand the fields in the real-time reports, see *Avaya Aura® Contact Center Performance Management Data Dictionary* (44400-117).

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 Aura® 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.

If the client operating system is Windows Server 2008 Release 2, Windows XP, or Windows 2000, you must log on to the client as a user with Administrator privileges to install or upgrade Agent Desktop Displays.

Important:

If you install Windows Vista on the client, users cannot view online help. To view online help, you must download and install Windows update KB917607 on to each client. This update includes the `WinHlp32.exe` file, which is required to view WinHelp help files.

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 (created using Crystal Reports 2012) 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 *Avaya Aura® Contact Center Performance Management* (44400-710). To understand the fields in the historical reports, see *Avaya Aura® Contact Center Performance Management Data Dictionary* (44400-117).

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 Manager Administration – Client Administration* (44400-611).

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, 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 Manager Administration – Client Administration* (44400-611).

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* (44400-610). For information and procedures to create outbound campaigns in your Contact Center, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611).

Prompt Management

Using Prompt Management, Contact Center Manager Administration (CCMA) users can manage prompts on one or more Avaya Media Server (Avaya MS) servers. Prompt Management provides access control and partitioning.

You must configure CCMA as a trusted host in Avaya MS to configure the prompts. For more information on Prompt Management, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611).

Optional tools

Several optional components are installed on the Contact Center Manager Administration server. The following list describes the purpose of each optional component:

- [Data extraction](#) on page 92
- [AD-LDS replication](#) on page 92
- [Logon warning message](#) on page 93
- [Security Framework](#) on page 93

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.

AD-LDS replication

Active Directory Lightweight Directory Services (AD-LDS), formerly ADAM, is a Microsoft information storage framework and runs as a non-operating system service.

Active Directory Lightweight Directory Services (AD-LDS) supports data replication. AD-LDS replication allows the AD-LDS instance on one server to share data with an AD-LDS instance on another server, ensuring that the replicated data is the same across both servers. If the active CCMA fails, AD-LDS replication ensures the standby CCMA is configured with the most recent data.

Each Contact Center Manager Administration server can have only one Contact Center Manager Administration-specific AD-LDS instance.

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 2008.

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 the security framework, the warning message on the primary security server overrides the logon message.

Security framework

The Contact Center security framework provides an identity management mechanism that uses integration with a directory services infrastructure (for example Active Directory) for authentication of CCMA users. Contact Center can use the security service provided by System Manager. This helps to reduce administrative costs, and eliminates the redundant user information associated with per-application authentication solutions. Single sign-on is a core feature of the framework that minimizes the necessity for end users to provide credentials after they log on.

Chapter 10: 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
- AACC Multimedia Complement for Elite
- No Switch Configured Multimedia 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 94

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](#) on page 95
- [Configure access classes](#) on page 96
- [Reset passwords](#) on page 96
- [Monitor system configuration settings and performance](#) on page 96
- [Manage alarms and events](#) on page 97

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 login. 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 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.

To view client events, such as successful logon or logoff or failure to connect, use the PC Event Browser. To start PC Event Browser, click **Start > All Programs > Avaya > Contact Center > Server Utility > PC Event Browser**.

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 1: 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 11: Communication Control Toolkit

Communication Control Toolkit is a client/server application that helps you implement Computer-Telephony Integration (CTI) for installed and browser-based client integrations. For switches, the Communication Control Toolkit facilitates the integration of Contact Center, knowledge worker, and self-service solutions 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.

Installation options

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

- Voice and Multimedia Contact Server
- Voice Contact Server Only
- AACC Multimedia Complement for Elite
- No Switch Configured Multimedia Only
- Knowledge Worker Server Only

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

The following sections provide the information you need to install Communication Control Toolkit software:

- [Modes of operation](#) on page 99
- [Components](#) on page 100

Modes of operation

You can work with Communication Control Toolkit in two modes of operation:

- Contact Center
- Knowledge Worker

Contact Center

In a Contact Center environment, 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

Knowledge Worker

In a Knowledge Worker environment, skill-based routing is not required. You can use direct-connect with the TAPI Service Provider to connect directly to the Avaya Communication Server 1000 using the ELAN TCP/IP link. The proprietary protocol Application Module Link (AML) communicates between the Avaya Communication Server 1000 and the TAPI Service Provider.

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* (44400-610).

- 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 if you work in a Contact Center environment.

 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 101
- [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. Two terminal types indicate the types of physical communication endpoints:
 - Agent—An agent terminal can log on to an ACD queue and answer calls routed to that queue (if scripted). An Agent terminal can also make calls.
 - Knowledge Worker—A Knowledge Worker terminal cannot log on to an ACD queue or answer calls routed to a queue. A Knowledge Worker terminal can make and answer regular calls.
- 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.
- Assignments are not associative. If you assign one resource to a second, and assign the first resource to a third, the second and third resources are not assigned to each other. For example, if you assign an address to a terminal, and then assign that terminal to a user, the user does not inherit the address. You must also assign the address to the user.
- 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 2: 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.
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* (44400-610).

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 Knowledge Worker, 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 full Communication Control Toolkit API.

The Full 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 www.avaya.com.

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

Chapter 12: 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
- AACC Multimedia Complement for Elite
- No Switch Configured Multimedia 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](#) on page 106
- [Folder structure](#) on page 106
- [Components](#) on page 106

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. For more information about configuring these two folders, see *Avaya Aura® Contact Center Commissioning* (44400-312).

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* (44400-610).

- 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 Aura® 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 and the warm standby. 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 Web site 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.

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 with Contact Center Multimedia to provide Java Server Pages (JSP) script 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.

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* (44400-610).

This section contains the following topics:

- [Configure email settings](#) on page 110
- [Configure IM settings](#) on page 111

- [Configure Web communications settings](#) on page 112
- [Configure outbound settings](#) on page 113
- [Configure Social Network settings](#) on page 113
- [Social Media Analytics](#) on page 116
- [Configure Predictive Outbound settings](#) on page 116
- [Configure voice mail settings](#) on page 118
- [Configure scanned document settings](#) on page 118
- [Configure SMS text settings](#) on page 119
- [Configure faxed document settings](#) on page 120
- [Configure Agent Desktop settings](#) on page 121
- [Configure General settings](#) on page 122
- [Handle contacts](#) on page 123
- [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* (44400-610).

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* (44400-610).

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* (44400-610).

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 a test Web server to perform trials for the new customer Web site, 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* (44400-610).

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* (44400-610).

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 Manager Administration – Client Administration* (44400-611).

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 steeliest (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.

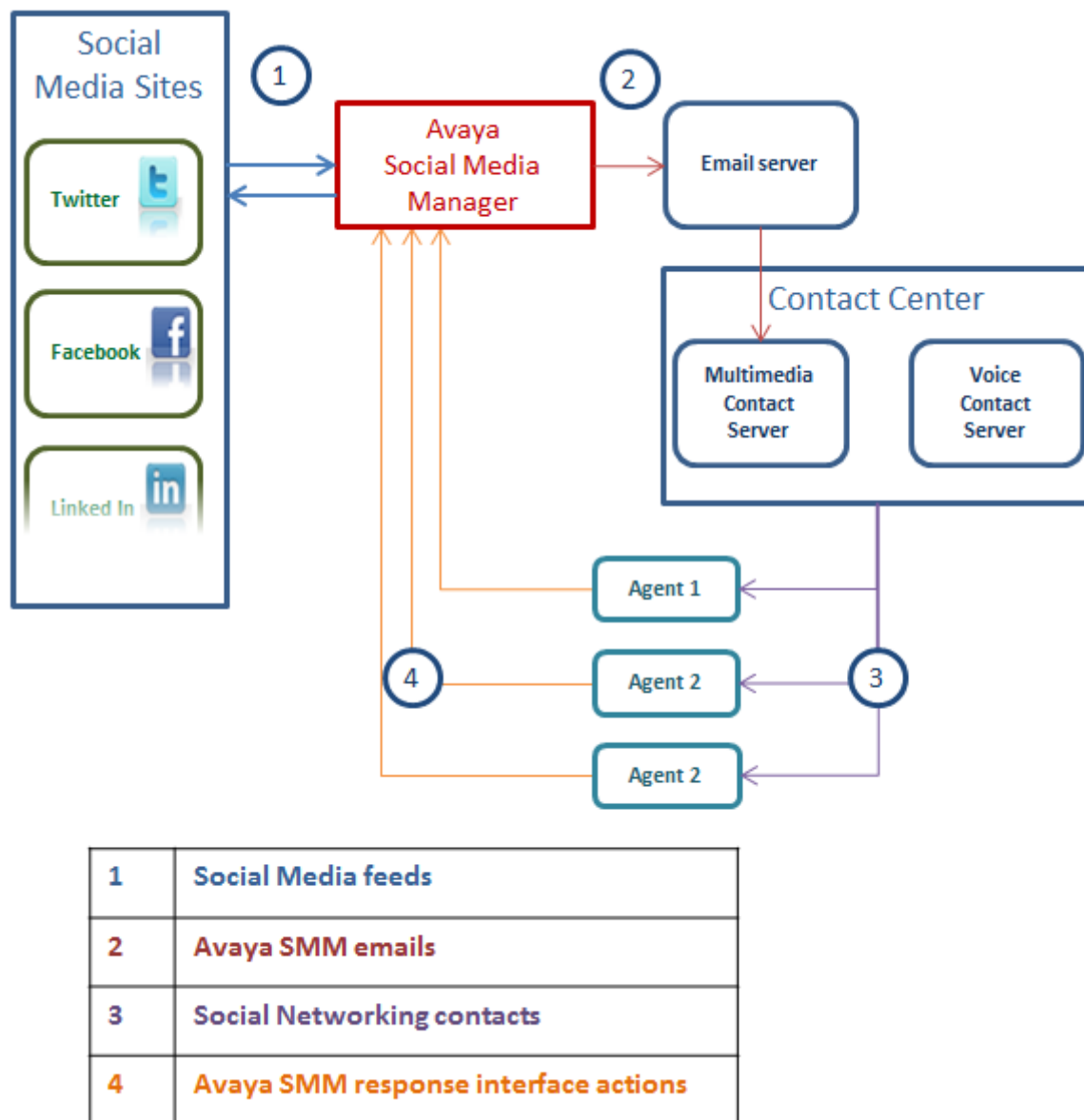


Figure 6: Example of the Social Network contact flow

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 Approval* 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 Predictive Outbound settings

Administrators create Outbound campaigns using the customer database, custom scripts, and predictive outbound settings that determine how the calls are presented to agents with predictive skillsets. Based on how the Administrator configures the campaign, calls can be dialed by the system or by the agent and presented to the agent automatically or with time for the agent to preview the contact.

Avaya installs hardware at customer sites to manage the administration tools (Call Processing Server), database (Portfolio server) and a switch (TSP-500) that connects to the Avaya Communication Server 1000 switch. The components of this hardware uses administration software for configuration components such as configuring agent scripts. Components integrate with Contact Center software such as Contact Center Manager Administration to configure Contact Center agents to handle predictive outbound contacts.

The Call Processing server calculates the number of calls answered (rather than ringing no answer, answering machine, and busy signal) and determines an average number of calls answered. For example, the Call Processing server can determine that one in three calls is answered by a live person. The Call Processing server also calculates the length of time for an agent to handle a single call based on agent state, status, wrap-up time, and number of calls answered. For example, it takes eight seconds for an agent to handle a call.

In Contact Center, agents are assigned a skillset for predictive outbound. The agent logs on to Agent Desktop and connects to Contact Center and the Predictive Outbound hardware.

When the agent with Predictive outbound skillset logs on to the phone, the dedicated phone line connection is formed between the agent telephone and the Call Processing server. Agents must use Agent Desktop for telephony functions. The Call Processing server sends voice contacts through the dedicated phone lines (for example, three voice contacts every eight seconds, anticipating that an agent handles the contact). The agents do not accept the contacts, but start participating when their phone line connects. They hear a beep in their headset to alert them to a contact. Agent scripts are provided by the Call Processing server so that agents can speak scripted text or know which tasks to perform for each contact, including transfer or conference.

In the Contact Center Multimedia Administrator, you can configure the following properties for predictive outbound functionality:

- Predictive outbound blending settings
 - Choose a threshold to monitor to determine whether an agent has spare cycles to handle an inbound skillset (email messages, voice, Web communications, instant messages) for a span of time that is not predictive outbound. If an agent is configured with a predictive outbound skillset, they can have only the predictive outbound skillset; agents cannot not have a predictive outbound skillset and an inbound skillset at the same time.
 - Skillset monitoring settings specify the interval (in seconds) that you want the blending service to check inbound skillsets with the blending template threshold to determine whether to re-assign predictive outbound agents. You can configure the number of agents to re-assign to the other skillset when the Level 2 threshold is exceeded.
 - Skillset reversal settings specify the interval (in seconds) that you want the blending service to check inbound skillsets to determine if agents previously assigned to the an inbound skillset can be returned to the predictive outbound skillset. You can configure the number of agents to return to the predictive outbound skillset when traffic falls below the Level 1 threshold.
- Configure the real-time data multicast settings for predictive outbound contacts to map a path for streams of data between the Contact Center Manager Server and the Contact Center Manager Administration server for reporting. You must configure the IP address and port number.
- Use the Administration tool on the Call Processing server to configure detailed agent scripts that provide the agent with information to present to the customer, and information about how to respond to customer statements. Each script is stored in a URL. Configure the URL location for the agent scripts for predictive outbound contacts.

For information about configuring the administration settings for Web communications contacts, see *Avaya Aura® Contact Center Predictive Outbound Fundamentals* (44400-106).

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* (44400-610).

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* (44400-610).

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* (44400-610).

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* (44400-610).

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* (44400-610).

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* (44400-610).

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* (44400-610).

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* (44400-610).

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 see matching contacts only in the skillsets that the agent is assigned to.
- 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* (44400-610).

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 and for the Predictive Outbound Support tool.
- **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* (44400-610).

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 predictive outbound contacts, depending on the applications your Contact Center is licensed to handle.

For more information about the Agent Desktop, see *Avaya Aura® Agent Desktop User Guide* (44400-114).

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 is 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.

 Note:

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.

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 *Avaya Aura® Agent Desktop User Guide* (44400-114).

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 *Avaya Aura® Agent Desktop User Guide* (44400-114).

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 adds 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.

HA replication

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 primary Contact Center Multimedia server fails. All multimedia services are disabled on the Standby server until it is required to run as the primary server. For more information about the redundancy feature for Contact Center, see [High Availability fundamentals](#) on page 149.

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* (44400-610).

Chapter 13: Avaya Media Server

Avaya Media Server is a software based media processing platform for the Contact Center. All media processing is performed in software on the host CPUs. The Avaya Aura® Contact Center DVD contains a custom version of Avaya Media Server. This Contact Center custom version of Avaya Media Server contains an additional component that provides the conference and Agent Greeting services in SIP-enabled Contact Centers.

The 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 Media Server requires licenses for the conference feature. Agent Greeting licensing is required to configure this optional feature.

The Avaya Aura® Contact Center version of Avaya 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 Media Server Release 7.6 on Linux.

Avaya Media Server is supported on the Windows Server 2008 Release 2, 64-bit, Service Pack 1 operating system when installed coresident with Avaya Aura® Contact Center. Standalone Avaya Media Server is not supported on the Windows Server 2008 operating system.

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

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

Avaya Media Server media files and media management

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

the custom media files using the Avaya Media Server Element Manager. You update and configure the default media files directly in the locale specific folders on the Avaya Media Server.

Content Store

The Avaya Media Server Content Store provides a persistent storage capability for configuration data and media files. You use the Avaya Media Server Element Manager Web administration utility to configure and manage the contents of the Content Store. If you have more than one Avaya Media Server, you can designate one server to be the primary Avaya Media Server. You can then configure the other Avaya Media Servers to replicate (copy) the configuration data and media files from the Content Store on the primary Avaya Media Server. This configures all of the Avaya 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 Media Server fails the remaining Avaya Media Servers are configured correctly and can continue processing media and contact center calls.

Custom media

Avaya Media Server stores (customer generated) custom media files in a media Content Store. Typically, a customer records their own announcements and stores the WAV media file recordings in the Avaya 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 Media Server cluster-based solution, you configure your custom media files only on the primary Avaya Media Server Content Store. The custom media files are automatically replicated to all other Avaya Media Servers in the cluster.

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

Custom media organization

In Avaya Media Server Element Manager (EM), you organize custom media 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 must create one locale-specific content group for treatments such as RAN.

Avaya 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

Table continues...

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

You can create one or more additional content groups for music. Typically you store different types of music media in different content groups. 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 Media Server locale-specific content group. To use scripted music in OD flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the Avaya Media Server content groups containing the music files. The OD flow applications or scripts reference these routes to access the treatment files and scripted music on the Avaya Media Server.

The following example shows the structure of a content namespace for a contact center based in Canada, which uses English recorded announcements, and has three optional music types; folk, jazz, and rock. The SIP domain for the contact center is ocs-nmclab.com. The locale configured on the CCMS server is en_ca.

The media content namespace structure is as follows:

ocs-nmclab.com <= media content namespace, matches SIP domain name

- en_ca <= locale-specific media content group (announcements)
- folk <= media content group (folk music)
- jazz <= media content group (jazz music)
- rock <= media content group (rock music)

Default media files

Contact Center Avaya 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 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_xx.wav) where xx is the country portion of the locale (for example, ringback_us.wav, ringback_ru.wav)

The default media files are stored in the Operating System file structure (not in the Avaya Media Server content namespace). The canned media files are stored in Linear 16-bit PCM recording format.

If you choose to create your own recordings, you must replace the existing default media files with files of the exact same name. For example, if you choose to record your own media files for single digit numerals, then you must save the files as one.wav and two.wav to match the existing default media file names. Then you replace the existing default media files with the media files of your own recordings. You must then delete the existing Avaya Media Server transcoded output files. For example, if you are using PCMA transcoding, delete the one.wav and two.wav media files from the locale-specific PCMA folder. This forces Avaya Media Server to pick up your new Linear 16-bit PCM recording and generate a new transcoded output file of your recording.

Default media files are not stored in the Avaya Media Server Content Store, and are therefore not replicated to other Avaya Media Servers. If you update the canned or default media files on one Avaya Media Server, you must copy the updated default media files to all other Avaya Media Servers.

The Asian 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

All audio media files must have a .wav file name extension, for example hatchi.wav, jiu.wav, and seven.wav.

Default media organization

Each Avaya Media Server installation includes a number of default (canned) media files. These default media files are stored in a country and locale specific folder on the Avaya Media Server.

On a Windows operating system, the default location for the default media files is:

```
D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\Announcements
\contactcenter\default\xx\yy\116
```

Where xx is the country portion of the locale and yy is the language portion of the locale.

On a Linux operating system server, the default location for the default media files is:

```
/opt/avaya/ma/MAS/platdata/Announcements/contactcenter/default/xx/yy/116
```

Where xx is the country portion of the locale and yy is the language portion of the locale.

For example, the Linux operating system Avaya Media Server directory locations for Canadian English and French are:

```
/opt/avaya/ma/MAS/platdata/Announcements/contactcenter/default/ca/en/l16
```

```
/opt/avaya/ma/MAS/platdata/Announcements/contactcenter/default/ca/fr/l16
```

Media file formats

Avaya Media Server provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbts/sec. Create your announcement and music media files with this encoding before copying them onto the Avaya Media Server server.

Network configurations

You can configure Avaya 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 Media Server network configurations:

- Standalone Avaya Media Server, for lower capacity contact centers.
- Standard Avaya Media Server cluster, for higher capacity contact centers, and for providing load sharing with content replication.
- Standalone Avaya Media Server High Availability pair, for call protection in a Contact Center HA environment.
- Multiple Avaya Media Server High Availability pairs, for call protection with higher capacity and content replication in a Contact Center HA environment.
- Standard Avaya 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 Media Server

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

In Contact Center Manager Administration, you configure the Avaya Media Server as a media server and assign it to handle conference media services. When you configure a Media Server in Contact Center Manager Administration, Contact Center License Manager pushes license keys to that Avaya Media Server. When Avaya Aura® Contact Center uses WebLM licensing, Avaya Media Server does not require a license file or any specific licensing configuration. Do not configure WebLM licensing on Avaya Media Server.

Avaya Media Server cluster

An Avaya Media Server cluster is a collection of Avaya Media Server nodes that work closely together. Avaya Media Server clusters offer improved redundancy, improved performance and load balancing. An Avaya 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 Media Server servers in the same cluster.

An Avaya Media Server cluster has:

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

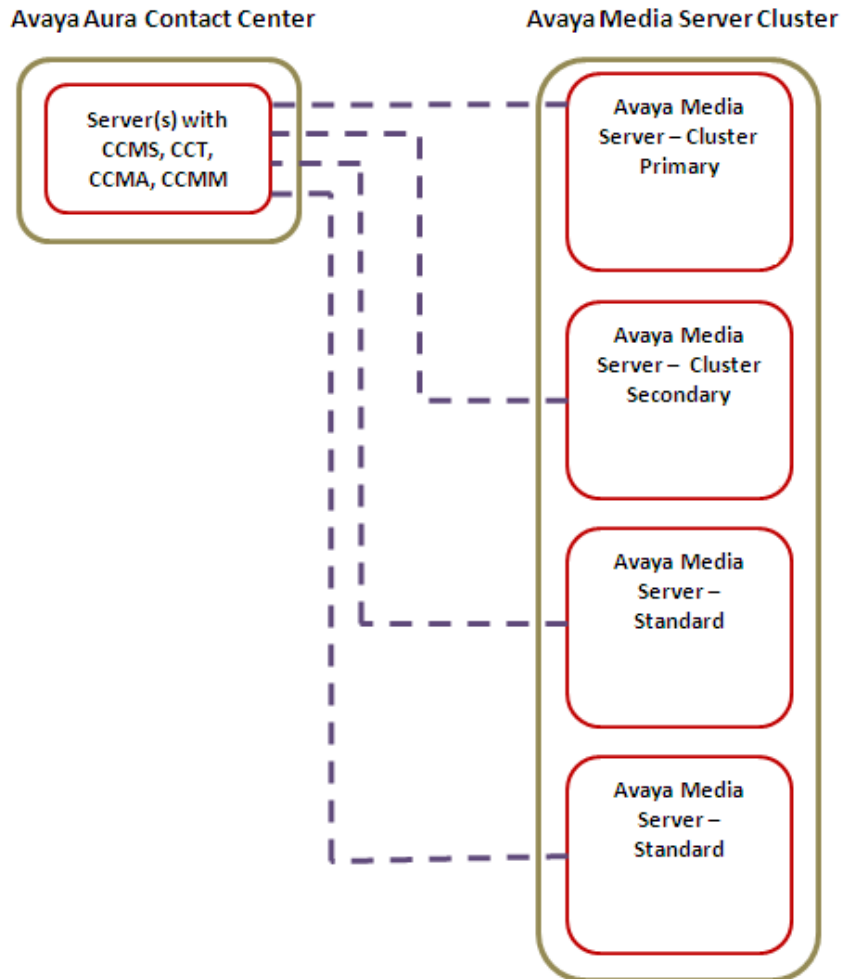


Figure 7: Avaya Media Server cluster

In this deployment, you configure the Avaya 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 Media Servers in the cluster deployment.

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

Licensing

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

Avaya Media Server Cluster Operating Systems

The servers in an Avaya Media Server cluster must all have the same operating system. All the servers in an Avaya Media Server cluster must use the Windows Server 2008 Release 2 64-bit

operating system, or all the servers must use the Red Hat Enterprise Linux 64-bit operating system. Avaya Media Server is supported only when Red Hat Linux is installed with English Language selected. Avaya Media Server does not support clusters with mixed operating systems. You cannot install other applications on the Avaya Media Server.

Avaya Media Server improved cluster redundancy

Each Avaya Media Server supports up to 1000 concurrent agents. When using an Avaya Media Server cluster, in Contact Center Manager Administration, you must configure each Avaya 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 Media Servers.

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

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

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

In an Avaya Media Server cluster, if both the primary and secondary server fail then the Avaya Media Server cluster does not play custom media such as announcements and music. Only default (canned) media such as ringback is available.

Avaya Media Server cluster configuration

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

In an Avaya Media Server cluster-based solution, you use Element Manager to configure your custom media files in the Content Store of the primary Avaya Media Server. The Content Store contents, including custom media files, are automatically replicated to all other Avaya Media Servers in the cluster.

Avaya Media Server stores default (canned) media files in a country and locale specific folder on every Avaya Media Server. Examples of default media files include digit recordings (one.wav, two.wav, three.wav, and so on). Default media files are not stored in the Avaya Media Server Content Store, and are therefore not replicated automatically to other Avaya Media Servers. If you update the canned or default media files on one Avaya Media Server, you must copy the updated default media files to all Avaya Media Servers in the cluster.

Configure the following Avaya Media Server resources and settings only on the primary Avaya 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 and music types (stored in a Content Namespace in the Content Store)
- Streamed music source (Really Simple Syndication or SHOUTCast)
- Media Processing and Security

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

- Cluster Configuration.
- Default “canned” media files. If you update the canned or default media files on one Avaya Media Server, you must copy the updated default media files to all Avaya Media Servers in the cluster.

Avaya Media Server High Availability pair

The Avaya 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 Media Server servers. The High Availability feature uses two Avaya 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 Media Server as the primary server and the other as the backup server. Both servers communicate with each other using a heart beat mechanism. Interruptions in the heartbeat from the primary server trigger a switchover to the backup server. Because both the primary and backup servers are identical in functionality and configuration, the switchover is seamless.

! Important:

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

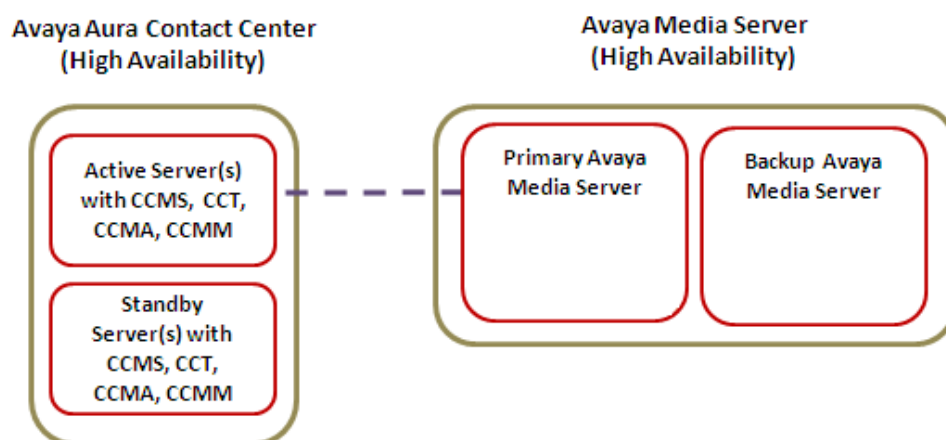


Figure 8: Avaya Media Server High Availability pair

In Contact Center Manager Administration (CCMA), you configure the Avaya 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.

Avaya Media Server supports Agent Greeting in a High Availability deployment. However, during a switchover Avaya Media Server supports only greeting playback; it does not support agent—recorded greetings. Existing calls into the Agent Greeting application are lost in the event of a switchover, but the recording application continues to work for new calls after the switchover.

Licensing

In Contact Center Manager Administration (CCMA), add the Avaya 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 Media Server fails, the other Avaya Media Server takes over media processing.

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

Each Avaya Media Server in the HA pair requires one VALUE_CCTR_AMS_INSTANCE license.

Avaya Media Server High Availability configuration

Avaya Media Server supports custom (customer generated) media files and default (canned) media files. You update and configure the custom media files using the Avaya Media Server Element Manager. You update and configure the default media files directly in the locale specific folders on the Avaya Media Server.

In Avaya Media Server High Availability-based solutions, you configure your custom media files only on the primary Avaya Media Server. The custom media files are stored in the Content Store and they are automatically replicated to the backup Avaya Media Server.

If you update the canned or default media files on one Avaya Media Server, you must copy the updated default media files to all Avaya Media Servers.

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

- Licensing
- 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 and music types (stored in a Content Namespace in the Content Store)
- Streamed music source (Really Simple Syndication or SHOUTCast)
- Media Processing and Security

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

- High Availability configuration
- Default “canned” media files. If you update the canned or default media files on one Avaya Media Server, you must copy the updated default media files to all Avaya Media Servers

Multiple Avaya Media Server High Availability pairs

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

! Important:

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

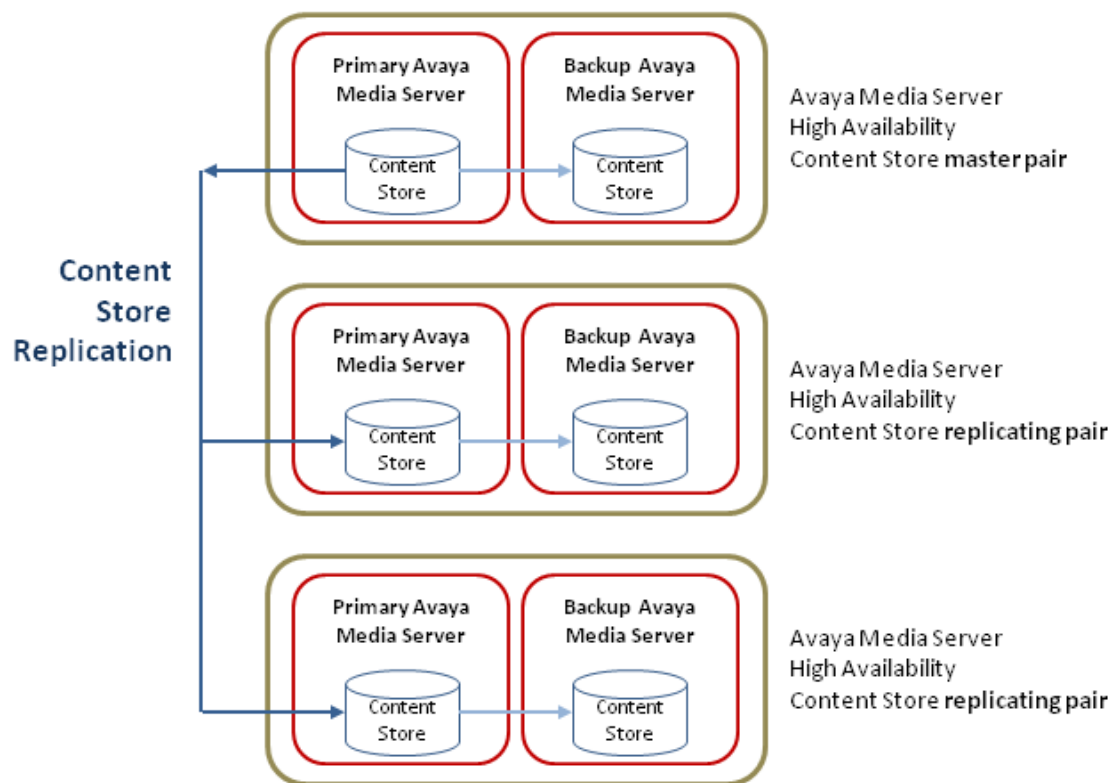


Figure 9: Content Store replication between multiple Avaya Media Servers with High Availability

In this deployment, you configure Content Store replication across the Avaya Media Server Primary servers. This allows you to perform custom media configuration on a single primary server only, and

the media configuration automatically replicates to the other Avaya Media Server servers in the network configuration.

In Contact Center Manager Administration, you configure each Avaya 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 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 Media Server fails, the other Avaya 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 Media Servers configured as Media Servers in CCMA. Contact Center License Manager pushes license keys to both Avaya Media Servers of each High Availability pair. When Avaya Aura® Contact Center uses WebLM licensing, Avaya Media Server does not require a license file or any specific licensing configuration. Do not configure WebLM licensing on Avaya Media Server.

Each Avaya Media Server HA pair requires two VALUE_CCTR_AMS_INSTANCE licenses.

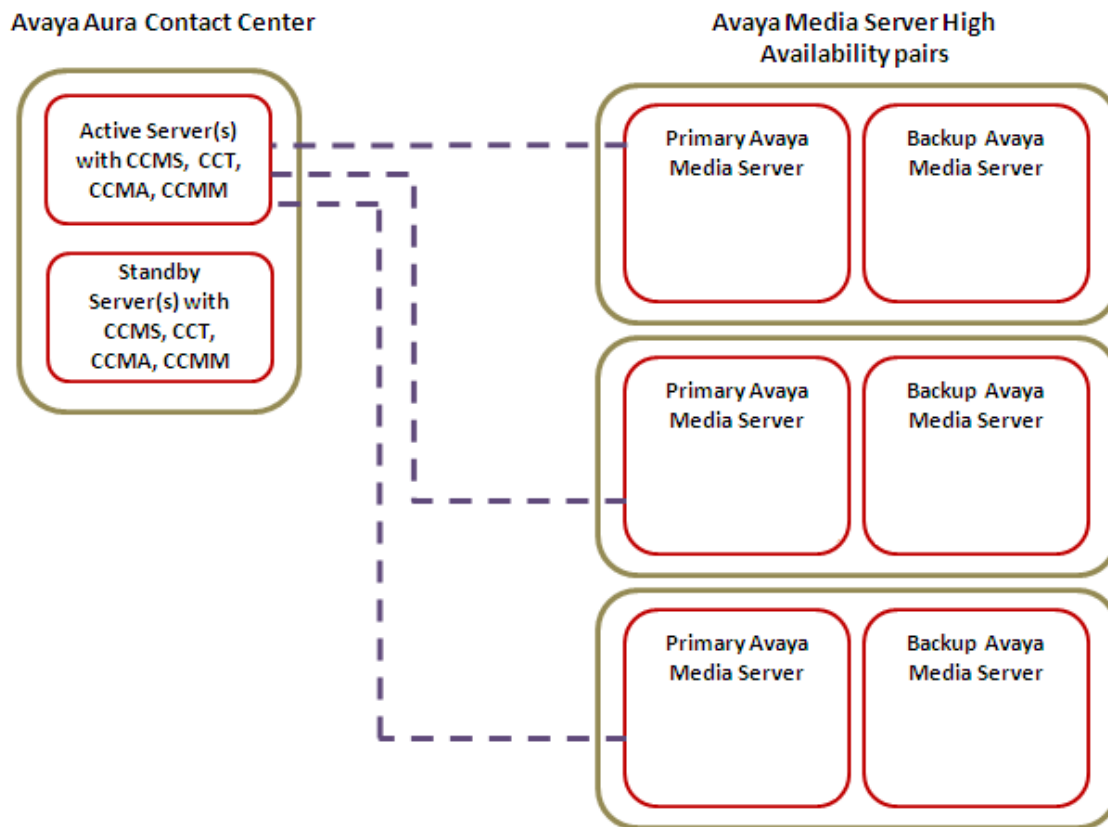


Figure 10: Avaya Media Servers with High Availability and WebLM licensing

Multiple High Availability pair configuration

Avaya Media Server supports custom (customer generated) media files and default (canned) media files. You update and configure the custom media files using the Avaya Media Server Element Manager. You update and configure the default media files directly in the locale specific folders on the Avaya Media Server.

Configure the following Avaya Media Server resources and settings on the primary server of the Avaya 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 and music types (stored in a Content Namespace in the Content Store)

Configure the following Avaya Media Server resources and settings on each primary Avaya 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 Media Server resources and settings on every Avaya Media Server in the cluster:

- High Availability configuration.
- Default “canned” media files. If you update the canned or default media files on one Avaya Media Server, you must copy the updated default media files to all Avaya Media Servers.

Avaya Media Server Remote Geographic Node deployment

Where the contact center deploys High Availability with a Remote Geographic Node, implement a single Avaya Media Server server, an Avaya Media Server cluster, or an Avaya Media Server HA pair at the remote site.

A Remote Geographic Node site supports the following Avaya Media Server deployments:

- A single primary Avaya Media Server. The single primary Avaya Media Server replicates data from the primary Avaya Media Server at the campus site.
- An Avaya Media Server cluster. The primary Avaya Media Server of the cluster replicates data from the primary Avaya Media Server at the campus site. The other Avaya Media Servers in the remote cluster replicate data from the primary Avaya Media Server of the remote cluster.
- An Avaya Media Server High Availability pair. The primary Avaya Media Server of the HA pair replicates data from the primary Avaya Media Server at the campus site. The backup Avaya Media Server at the remote site replicates data from the primary Avaya Media Server at the remote cluster.

Configure one remote Avaya Media Server primary server to replicate from the primary Avaya Media Server at the campus site. Then configure all other Avaya Media Servers at the remote site to replicate from the primary Avaya Media Server at the remote site.

The Avaya 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 Media Server servers in the remote site cluster.

Avaya Aura® Contact Center supports the deployment of Avaya Media Server High Availability pairs at a Remote Geographic Node site. You can also deploy Avaya 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 Media Server Zoning

Avaya Media Server (Avaya MS) Zoning allows contact center administrators to target a specific Avaya MS instance or prioritized list of instances when anchoring incoming contact center calls. The administrator chooses the preferred Avaya MS instance on which to anchor the contact center call using a new scripting command in Avaya Aura® Orchestration Designer (OD). The preferred Avaya 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 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 MS instance from the available pool.

The existing AACC call handling model, prior to Avaya MS Zoning, saw incoming customer calls anchored on an available Avaya 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 MS instance is a round-robin algorithm, which means you cannot reliably predict the specific Avaya MS instance to be used for any given call. In this case, Avaya 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 MS selection process, administrators can optimize WAN bandwidth utilization by distributing Avaya 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 four sites in any Avaya MS Zoning solution. This includes a main data center and three additional sites (this can include a combination of a Remote Geographic Site and two standard remote sites).

The following diagrams show the differences between solutions with and without Avaya MS Zoning.

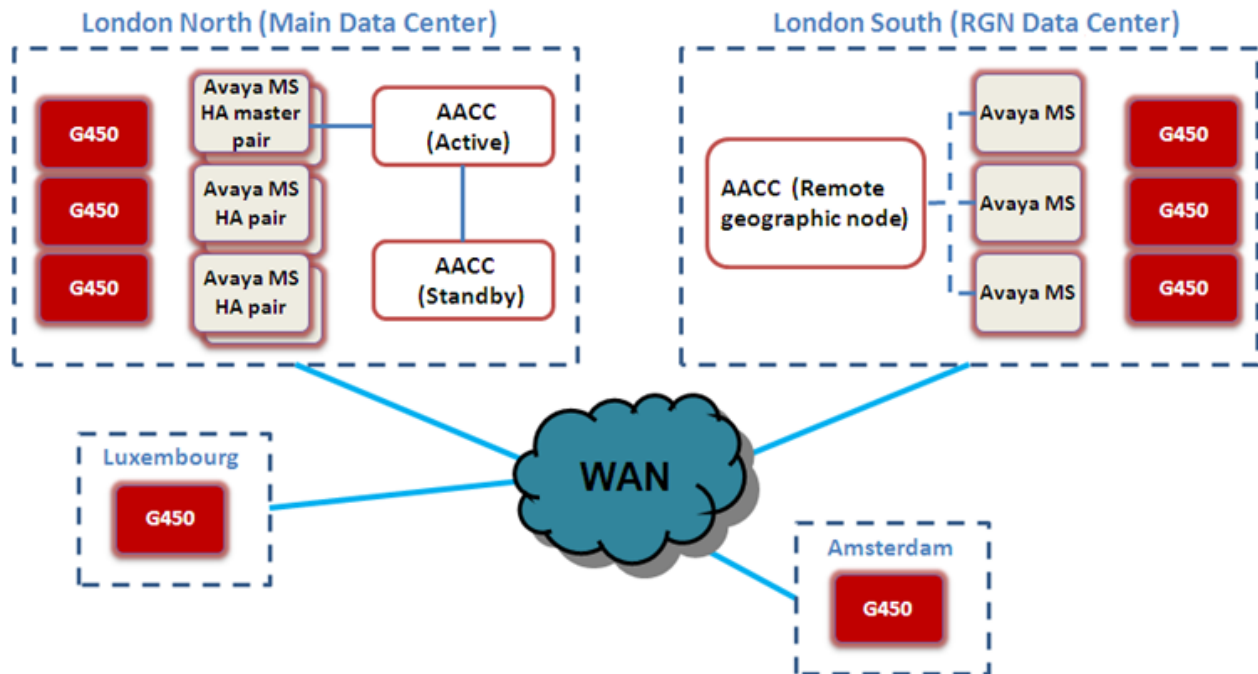


Figure 11: AACC solution without Avaya MS Zoning

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 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 MS instances at the RGN site are single Avaya MS servers – Avaya MS High Availability pairs at RGN sites were previously not supported in Avaya Aura® Contact Center solutions.

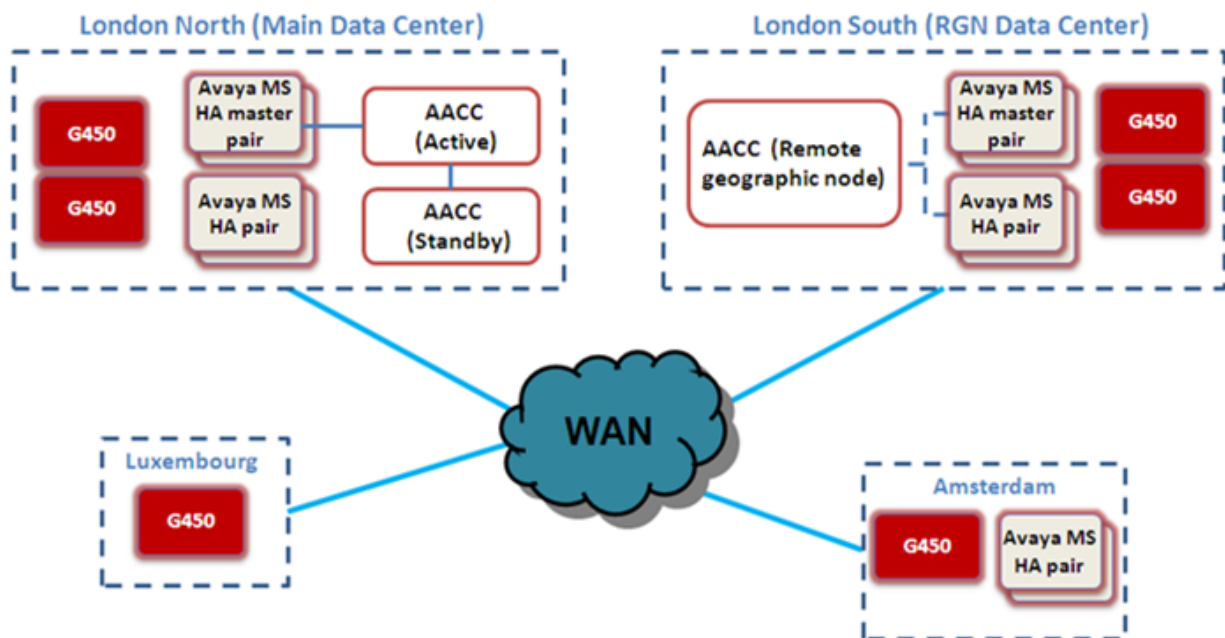


Figure 12: AACC solution with Avaya MS Zoning

The diagram above also describes a Mission Critical HA solution with a Remote Geographic Node site. In this example, an Avaya MS High Availability pair is co-located with a call ingress point at the Amsterdam location. The Luxembourg site still contains no Avaya 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 MS instances are deployed. In this example, calls arriving from Luxembourg can be anchored on the Avaya 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 MS High Availability pairs located at the RGN site with G450 Media Gateways. With Avaya MS Zoning, it is now possible for the Main Data Center to use the Avaya MS servers and gateways located at the RGN site. It is also possible for the non-HA AACC server to use Avaya MS High Availability pairs at the RGN site.

You enable the Avaya MS Zoning feature on the CCMA Global Settings page. You must have a license that supports Avaya MS Zoning — you cannot enable Avaya 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 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 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 MS instance and the agent for each customer call. An agent in close proximity to the Avaya 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 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 MS Zoning.

For more information on how to configure Avaya MS Zoning, see *Avaya Aura® Contact Center Commissioning* (44400-312).

WAN requirements

The following is a list of Wide Area Network (WAN) requirements for Avaya 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 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 14: 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. Avaya Aura® 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
- Warm standby High Availability

The level of Avaya Aura® 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. Avaya Aura® Contact Center also supports Geographic Disaster Recovery and data resiliency.

Campus High Availability

In a campus High Availability environment the standby and active servers are in the same location.

In a campus solution 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 shutdown 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 is assigned a static IP address. After the Active server in each replication pair is determined, 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 that active application using the Managed IP address. The Standby server assumes this same Managed IP address, if it takes over processing and becomes the active application. The Active server stops hosting the Managed IP when it stops being the Active server. When the Standby server starts-up to take over call processing, it attaches the Managed IP address to its network interface.

If your High Availability enabled active Contact Center Manager Server has two network interfaces and is configured to support an embedded LAN (ELAN), then the Contact Center Manager Server

supports two Managed IP addresses; one Managed IP and name for the CLAN and one Managed IP and name for the ELAN. Contact Center Manager Server 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, 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. The network subnet IP address range is controlled by the subnet mask.

Managed name

A Managed name can also be configured that maps to the Managed IP address. This Managed name can be configured on a Domain Name System (DNS) or in the hosts file on the servers that are connecting to the High Availability servers.

You use the Managed IP address or Managed name when configuring remote IP addresses or server names, do not use the physical name or IP address.

Campus switchover

In a campus environment, a switchover from the active to the standby server using the managed IP address appears as a server restart to external applications.

You can invoke a switchover manually, or have the switchover triggered automatically when communication is lost or if a service fails. For switchover to occur, the standby server must shadow the active server and switchover must be enabled on both servers.

The main advantages of Campus High Availability are:

- Automatic switchover
- Faster switchover time
- Minimal switchover steps
- Third-party applications connect to the Managed IP address

Campus High Availability caters to Contact Center application or server failures and offers resiliency for local network failures.

Email switchover notification

You can enable automatic email switchover notifications, to alert the Contact Center administrator. When enabled, the specified email address receives an automatic email which provides switchover information to the recipient. This switchover information includes:

- Switchover description — the switchover is manual, is automatic due to a critical service failure, or automatic due to network communication failure.
- Depending on the type of switchover, additional information is provided in the email. In the case of automatic switchovers due to critical service or network failures, information such as event ID's and switchover times are included in the email.
- In the case of automatic switchovers due to service or network failures, the administrator receives two emails. The first email informs the administrator that a switchover is imminent, and the second email arrives after successful completion of the switchover.

Contact Center application geographic redundancy

The Avaya Aura® Contact Center High Availability feature supports geographic redundancy and resiliency. In geographic Wide Area Network (WAN) solutions the standby server on the remote geographic site is called a Remote Geographic Node (RGN) server. Avaya Aura® Contact Center geographic High Availability supports data resiliency and Disaster Recovery.

The Active server and the Standby server are in the same campus location. The Standby server shadows the Active server. If the Active server fails the local Standby server takes over contact processing on the local campus site.

The Remote Geographic Node (RGN) server on the remote site shadows the Active server on the campus site. The RGN shadows data from the Managed IP on the campus site. This means that following an Avaya Aura® Contact Center outage on the campus site, the RGN does not need to change the network address from which it is shadowing data.

The RGN server must have the same Contact Center applications installed as the Active server. For example, if the Active server has a Voice and Multimedia Contact Server installed then the RGN must have a Voice and Multimedia Contact Server installed.

If the Active server fails, the local Standby server assumes the shared Managed IP address and starts processing contacts. The Remote Geographic Node (RGN) server monitors the campus Managed IP address so it continues shadowing. The RGN server shadows the Active CCMS and CCT server, maintaining a near real-time local copy of the CCMS, CCT, and Administration databases. Therefore, the RGN server is configured with the most recent data and it can take over if the campus site fails.

Contact Center Manager Administration (CCMA) uses Microsoft Active Directory Lightweight Directory Services (AD-LDS) technology to store data. CCMA uses AD-LDS replication to support geographic redundancy and resiliency. Install a standby CCMA instance on a Remote Geographic Node server. This standby CCMA on the RGN replicates the Active CCMA. Therefore, the CCMA on the RGN server is configured with the most recent data and it can take over from the campus site if necessary.

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 switchover. The Remote Geographic Node servers use the backup Domain Controller to authenticate users.

Geographic High Availability solution

The following diagram shows an example of a geographic High Availability solution. The Standby Voice Contact Server shadows the Active Voice Contact Server. CCMA on the Standby server replicates CCMA on the Active 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. CCMA on the Remote Geographic

Node replicates the CCMA instance on the Active server. The Remote Geographic Node Multimedia Contact Server shadows the Active Multimedia Contact Server on the campus site.

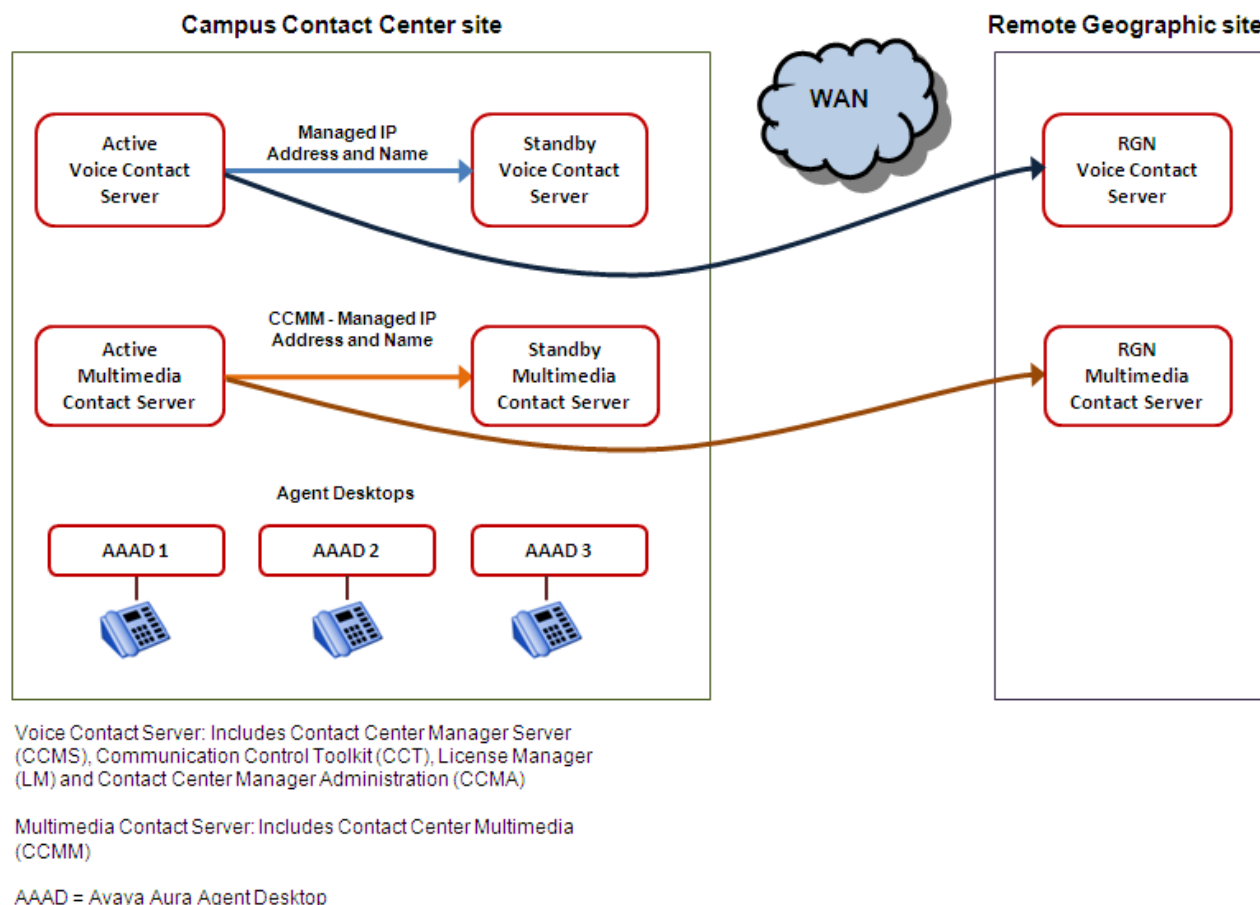


Figure 13: Example of a typical Geographic High Availability solution

The main advantages of Geographic High Availability are:

- Support for database shadowing over WAN.
- Added redundancy in event of primary or campus site failure.

Geographic High Availability caters for full site failures. 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 and Standby Contact Center servers, and Contact Center Remote Geographic Node(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(s) for data resiliency and Disaster Recovery.

- Avaya Communication Server 1000 AML-based solution, with a campus Active Contact Center server, and Contact Center Remote Geographic Node(s) for data resiliency and Disaster Recovery.

Warm standby High Availability solutions or solutions that use the Avaya Aura® Solution for Midsize Enterprise platform do not support geographic High Availability.

Database Shadowing

Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Multimedia (CCMM) each store Contact Center information in a Caché database. 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 is constantly retrieving 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's database.

The Standby application server shadows the Active application server, maintaining a near real-time local copy of the CCMS, CCT, CCMM, and Administration databases. Therefore, the Standby Server is configured with the most recent data and it can take over from the Active Server if necessary.

Trusted IP address

The active and standby servers use the Trusted IP address to verify network connectivity. If the active server cannot communicate with the standby server it attempts to communicate with the Trusted IP address.

If the active server cannot connect to the Trusted IP address on startup then no Contact Center services start on that 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.

You must use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Contact Center Manager Server

In a campus solution, one CCMS actively processes scripts and contacts. This is called the active CCMS. Another CCMS in the same Contact Center solution runs in standby mode. This standby CCMS monitors and shadows the active CCMS, it tracks the state of active calls but does not process calls. The standby CCMS monitors the active CCMS, forming a resilient or replicating pair. If the active CCMS fails, the standby CCMS recognizes the failure and start processing contacts.

Contact Center Manager Server employs an automated or manual switchover between the Active and the Standby server. A CCMS service failure, hardware, network, or database failure can initiate a switchover.

In a combined campus and geographic enterprise solution, a third CCMS is installed on the remote geographic site. The server on the remote site is called a Remote Geographic Node. If the campus site fails this CCMS Remote Geographic Node can take over contact processing or it can be used for disaster recovery.

You can also choose to perform a manual switchover. For more information about performing a manual switchover for maintenance, see *Avaya Aura® Contact Center Server Administration* (44400-610).

Contact Center Manager Administration and AD-LDS

Contact Center Manager Administration uses Microsoft Active Directory Lightweight Directory Services (AD-LDS) technology to store user information, access classes, partitions, private and graphical real-time reports, and real-time report filters. AD-LDS runs as a non-operating system service.

Active Directory Lightweight Directory Services (AD-LDS) supports data replication. AD-LDS replication allows the AD-LDS instance on one server to share data with an AD-LDS instance on another server, ensuring that the replicated data is the same across both servers. AD-LDS replication ensures that when data is added, deleted or modified on either the primary or standby CCMA, that the result is replicated to the other server. If the primary server fails, AD-LDS replication ensures the standby server is configured with the most recent data.

In a campus solution the Contact Center Administrator launches Contact Center Manager Administration using the managed name of the server. If an active Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), or Contact Center Manager Administration (CCMA) application or server fails, the Contact Center Manager Administration client Web browser continues to use the managed name and the Contact Center Administrator continues working without interruption.

A High Availability CCMA replication solution contains a primary CCMA and a standby CCMA. The standby server replicates the primary server AD-LDS contents.

AD-LDS replication is a real time operation and can be used in conjunction with CCMA backup and restore. Not all data is replicated with AD-LDS, some manual synchronization is required for all user

created reports and wallboards after switchover. If you add or modify user-created reports on the primary server you must backup and restore them on to the standby server, to keep the two CCMA's synchronized.

The primary server and the standby replication server must both be in the same Windows workgroup or domain for AD-LDS replication to work. AD-LDS replication uses a common windows account, used by both servers, to copy or replicate data from the primary CCMA AD-LDS to the standby CCMA AD-LDS.

The primary CCMA is always the primary CCMA. If the primary CCMA fails, the standby CCMA is still a standby CCMA, they do not switch roles. To restore CCMA solution resiliency, you must repair and reinstate the primary server, or install a new primary server using the same details as the previous primary CCMA. After a primary CCMA failure or shutdown, AD-LDS replication ensures that data stored in AD-LDS is available on the standby server. Data not stored in AD-LDS must be manually restored to the standby CCMA using the CCMA Backup and Restore utility.

In a combined campus and geographic enterprise solution, a third CCMA is installed on the remote geographic site. The server on the remote site is called a Remote Geographic Node. If the campus site fails this CCMA Remote Geographic Node can take over administration of the remote site or it can be used for disaster recovery.

For more information about performing switchovers for continuity in the Contact Center or for maintenance, see *Avaya Aura® Contact Center Server Administration* (44400-610).

Active Directory - Lightweight Directory Services data store

Contact Center Manager Administration makes use of Active Directory - Lightweight Directory Services (AD-LDS) and other data files to store application data. The following data is stored in AD-LDS (AD-LDS data):

- User information and details
- Access classes
- Partitions
- Private and graphical real-time reports
- Real-time report filters
- Historical report filters
- Servers configured
- Real Time Display templates

The following data is not stored in AD-LDS (non-AD-LDS data):

- Scheduling data for Contact Center Management assignments
- Scheduling data for historical reports
- Historical report output files
- User-created historical reports imported into Contact Center Manager Administration
- Real-time report exported files
- Emergency Help exported files

- Report Creation Wizard user-created formulas (stored in the file `RCW.mdb`)
- Report Creation Wizard user-created report definitions
- Audit Trail events
- Private user-created reports
- Public user-created reports
- RCW user-created reports
- Custom Report Groups index file

Data backup and restore

You must regularly back up the primary Contact Center Manager Administration (CCMA) server for the following reasons:

- To avoid loss of data in the event of a server failure: schedule backups to back up your CCMA data at least once a day (or more frequently, based on your Contact Center requirements). Schedule backups during periods of low activity.
- To keep data synchronized between CCMA and CCMS: you must back up and restore CCMA data and your Contact Center Manager Server data at the same time to ensure your contact center functions correctly. If the Contact Center Manager Server files change infrequently, you can back up only the CCMA data.
- To keep non AD-LDS data synchronized between the primary CCMA and standby CCMA. For example, if you add or modify user-created reports, you must backup and restore the user-created reports to the standby server.

Use the Contact Center Manager Administration Backup and Restore utility to backup and restore the CCMA (AD-LDS and non-AD-LDS) data. Each CCMA backup contains both AD-LDS and non-AD-LDS data. During a data restore, the CCMA Backup and Restore utility handles AD-LDS and non-AD-LDS data differently. To prevent accidentally overwriting replicating AD-LDS data, the CCMA Backup and Restore utility enforces the following rules:

- A primary CCMA backup can be fully restored to a primary server. Both AD-LDS and non-AD-LDS is restored.
- A primary CCMA backup can be partially restored to a standby server. Only non-AD-LDS is restored.
- A standby CCMA backup can be fully restored to a standby server. Both AD-LDS and non-AD-LDS is restored.
- A standby CCMA backup can be partially restored to a primary server. Only non-AD-LDS is restored.

In a Voice Contact Server environment, when you perform a backup of the Contact Center Manager Server, you must ensure that you back up the entire server and the associated databases, including CCMA. This ensures that the data between the two applications is always synchronized. Furthermore, you must store both backups in the same secure location.

If you install a replicating server, you must still perform regular backups. Unlike Active Directory Lightweight Directory Services (AD-LDS) replication, backups provide snapshots of your CCMA data files at moments in time. Backing up data, and not relying on AD-LDS replication as the only method of backing up CCMA data, is important for the following two reasons:

- Not all CCMA data is stored in AD-LDS, and therefore is not replicated.

- You cannot use AD-LDS replication to roll back data to a specific time.

In addition to backing up files, you must record your Real-Time Reporting configuration settings and your Emergency Help configuration settings whenever these settings change. During the restoration process, you must manually re-configure these settings.

In High Availability solutions, you must backup the primary CCMA at least once a day and store the backup in secure network location. Do not store the primary CCMA backup on the primary server. If the primary CCMA is offline and if you are using the standby CCMA, then regularly backup the standby server, because this contains the most recent data. Do not store the standby CCMA backup on the standby server. Always store the CCMA backups in a secure network location.

Recovery after the Primary CCMA software fails

In a High Availability solution, the Contact Center Administrator launches Contact Center Manager Administration using the managed name of the CCMS and CCMA server. If the primary CCMA instance fails or is shut down, the Contact Center Administrator continues accessing CCMA by pointing Internet Explorer at the managed name of the remaining standby CCMA server.

If the primary CCMA instance fails or is shutdown, AD-LDS replication ensures the remaining CCMA server contains the most recent AD-LDS data such as agent and partition data. You must restore the most recent primary CCMA data backup onto the standby CCMA server. The standby CCMA is then configured with the most recent (AD-LDS and non-AD-LDS) data.

At this point the primary CCMA is offline and the Contact Center Administrator is using the fully configured standby CCMA. CCMA is no longer replicating and it is therefore no longer resilient.

To reinstate Contact Center Manager Administration High Availability resiliency:

- Restart the primary CCMA server.
- Ensure all CCMA services are running. Because AD-LDS data replication is bidirectional, the restarted primary CCMA replicates the AD-LDS data from the standby CCMA.
- On the standby CCMA, backup the CCMA data.
- Restore the standby CCMA backup to the primary CCMA.

The primary CCMA is then configured with the most recent (AD-LDS and non-AD-LDS) data. CCMA High Availability resiliency is restored and the Contact Center Administrator can once again use the primary CCMA.

Recovery after the Standby CCMA software fails

In a High Availability solution, if the standby CCMA instance fails or is shut down, the Contact Center Administrator continues accessing CCMA by pointing Internet Explorer at the managed name of the primary CCMA server. While the standby CCMA is offline, CCMA is no longer replicating and it is therefore no longer resilient.

To reinstate Contact Center Manager Administration High Availability resiliency:

- Restart the standby CCMA.
- Restore the most recent primary CCMA backup to the standby CCMA.

Recovery after the Primary CCMA server fails

In a High Availability solution, if the primary CCMA server fails the Contact Center Administrator continues accessing CCMA by pointing Internet Explorer at the managed name of the remaining

CCMA server. While the primary CCMA server is offline, CCMA is no longer replicating and it is therefore no longer resilient.

To reinstate Contact Center Manager Administration High Availability resiliency:

- Rebuild the primary CCMA server. The new primary CCMA server must have the exact same name as the previous primary CCMA server.
- Reinstall the Operating System and Internet Information Services (IIS). The new primary CCMA server must have the exact same disk partitions, workgroup or domain, OS patches and details as the standby CCMA server.
- Restore the most recent primary CCMA backup to the new primary CCMA server.
- Restart the primary CCMA server. Because AD-LDS data replication is bidirectional the restarted primary CCMA replicates the AD-LDS data from the standby CCMA. The primary CCMA server is updated with the most recent AD-LDS contact center data.
- On the standby CCMA server, backup the CCMA data.
- Restore this backup CCMA data to the primary CCMA server.

The primary CCMA server is then configured with the most recent (AD-LDS and non-AD-LDS) data. CCMA High Availability resiliency is restored and the Contact Center Administrator can once again use the primary CCMA.

For more information about installing CCMA, see *Avaya Aura® Contact Center Installation* (44400-311). For more information about commissioning CCMA, see *Avaya Aura® Contact Center Commissioning* (44400-312).

Recovery after the Standby CCMA server fails

In a High Availability solution, if the standby CCMA server fails the Contact Center Administrator continues accessing CCMA by pointing Internet Explorer at the managed name of the primary CCMA server. While the standby CCMA server is offline, CCMA is no longer replicating and it is therefore no longer resilient.

To reinstate Contact Center Manager Administration High Availability resiliency:

- Rebuild the standby CCMA server. The new standby CCMA server must have the exact same name as the previous standby CCMA server.
- Reinstall the Operating System and Internet Information Services (IIS). The new standby CCMA server must have the exact same disk partitions, workgroup or domain, OS patches and details as the primary CCMA server.
- On the primary CCMA server, remove the obsolete standby CCMA server replication entries from the active CCMA database.
- When reinstalling CCMA software on the new standby CCMA server, run the AD-LDS replication utility.
- On the primary CCMA server, backup the CCMA data.
- Restore this backup CCMA data to the standby CCMA server.

The standby CCMA server is then configured with the most recent (AD-LDS and non-AD-LDS) data. CCMA High Availability resiliency is restored.

For more information about installing CCMA, see *Avaya Aura® Contact Center Installation* (44400-311).

For more information about commissioning CCMA, see *Avaya Aura® Contact Center Commissioning* (44400-312).

For more information about removing obsolete CCMA replication entries, see *Avaya Aura® Contact Center Upgrade and Patches* (44400-410).

For more information about performing switchovers for continuity in the Contact Center, see *Avaya Aura® Contact Center Server Administration* (44400-610).

Communication Control Toolkit

One CCT actively processes contacts. This CCT is called the active CCT. Another CCT in the same Contact Center solution runs in standby mode. This standby CCT monitors and shadows the active CCT, it tracks the state of active calls but does not process calls. The standby CCT monitors the active CCT, forming a resilient or replicating pair. If the active CCT fails, the standby CCT recognizes the failure and start processing contacts.

A CCT service failure, hardware, network, or database failure can initiate a switchover.

Communication Control Toolkit (CCT) server employs an automated or manual switchover between the active and the primary server.

In a combined campus and geographic enterprise solution, a third CCT is installed on the remote geographic site. The server on the remote site is called a Remote Geographic Node. If the campus site fails this CCT Remote Geographic Node can take over contact processing or it can be used for disaster recovery.

For more information about performing switchovers for continuity in the Contact Center or for maintenance, see *Avaya Aura® Contact Center Server Administration* (44400-610).

Contact Center Multimedia

Avaya Aura® Contact Center supports High Availability (HA) resiliency using a pair of Contact Center Multimedia (CCMM) servers.

One CCMM actively processes multimedia contacts. This CCMM is called the active CCMM. Another CCMM in the same Contact Center solution runs in standby mode. This standby CCMM shadows the active CCMM, but does not process contacts. The standby CCMM monitors the active CCMM, forming a resilient or replicating pair. If the active CCMM fails, the standby CCMM recognizes the failure and starts processing contacts. Contact Center Multimedia employs an automated or manual switchover between the primary and secondary server.

In a campus solution, a Contact Center Multimedia hardware, network, or database failure can initiate a High Availability switchover.

If a critical CCMM service fails, the service is automatically restarted by the Windows Service Monitor.

In a combined campus and geographic enterprise solution, a third CCMM is installed on the remote geographic site. The server on the remote site is called a Remote Geographic Node. If the campus site fails this CCMM Remote Geographic Node can take over contact processing or it can be used for disaster recovery.

For more information about configuring CCMM active and standby servers, see *Avaya Aura® Contact Center Server Administration* (44400-610).

For more information about performing switchovers for continuity in the Contact Center or for maintenance, see *Avaya Aura® Contact Center Server Administration* (44400-610).

Avaya Media Server

The Avaya Media Server High Availability feature ensures uninterrupted availability of media processing and reduces loss of processing data when an Avaya Media Server fails. The High Availability feature uses two Media Servers operating in a standby deployment. 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 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 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 Media Server supports High Availability only on a Linux operating system.

Avaya Media Server High Availability pair

In a High Availability deployment, configure a redundant pair of Avaya Media Server servers. Configure a High Availability primary Avaya Media Server and a High Availability backup Avaya Media Server on two separate servers. In Contact Center Manager Administration, you configure the Avaya 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 installed as a High Availability pair, Avaya Media Server uses the Avaya Media Server License Server feature. You install the

same license file on the primary server and the secondary Avaya Media Server replicates this license automatically.

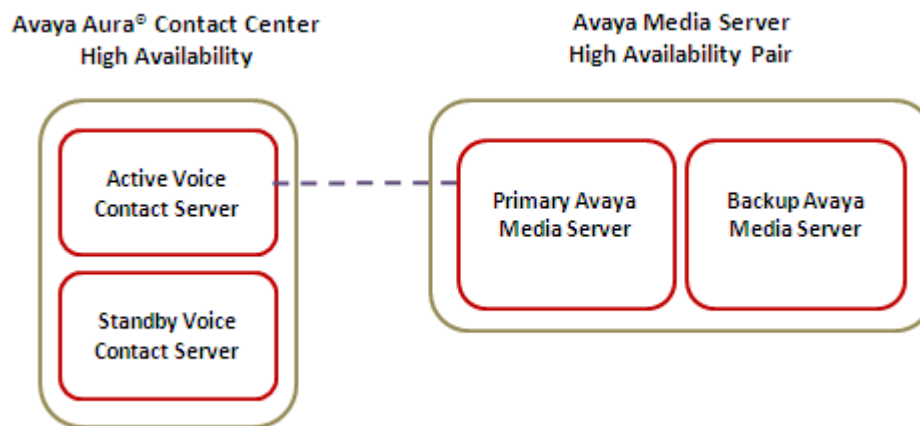


Figure 14: Single Avaya Media Server with High Availability

Avaya Media Server server High Availability pairs

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

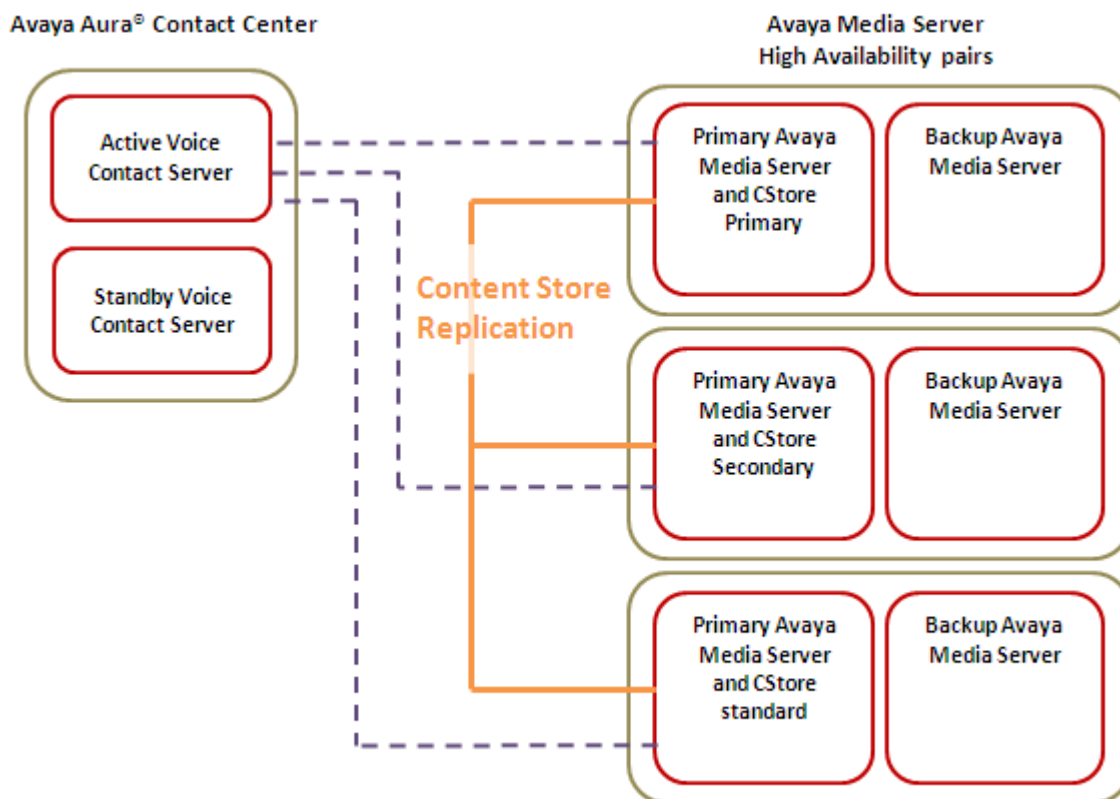


Figure 15: Multiple Avaya Media Servers with High Availability

In this deployment, you configure Content Store (CStore) replication across the Avaya 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 Media Server servers in the network configuration.

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

In a High Availability deployment, when using more than one Avaya Media Server redundant pair, you license each redundant pair separately.

Avaya Media Server Remote Geographic Node deployment

Where the contact center deploys High Availability with a Remote Geographic Node, implement an Avaya Media Server cluster or HA pair at the remote site. The Avaya Media Server servers at the remote site obtain licenses from the Avaya Aura® Contact Center servers at that remote site.

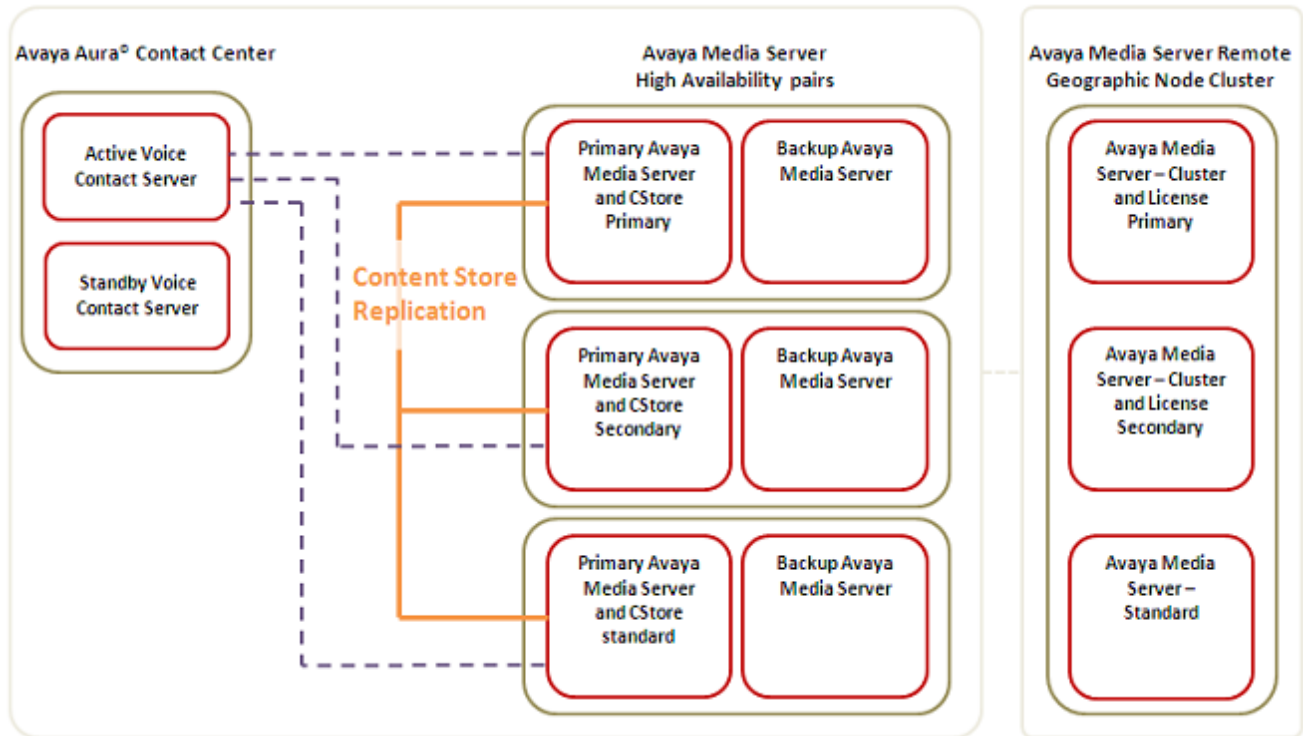


Figure 16: Multiple Avaya Media Servers in a Remote Geographic node configuration

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 Media Server servers in the remote site cluster.

*** Note:**

Avaya Aura® Contact Center 6.4 supports the deployment of Avaya Media Server High Availability pairs at a Remote Geographic Node site. You can also deploy Avaya 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 standby server and network configuration

You can use managed IP addresses for campus redundancy. With a managed IP address, both the active and standby servers have the same IP address, thus other applications that require calls to the IP address or server name (such as Contact Center Manager Administration need the Contact Center Manager Server name), no requirements are required to reconfigure the Contact Center system.

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).

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 balance. The process of grouping NICs is called teaming. 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 Contact Center High Availability feature supports Remote Geographic Nodes. Remote Geographic Nodes are similar to the standby servers but they are used only to shadow data from the active server—they have no other responsibility. 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 Nodes can be used for disaster recovery if the entire campus site fails.

The Active server refers to the other standby server on the remote geographic site as the Remote Geographic Node server. The Active server, Standby server and Remote Geographic Node server are part of the same Avaya Aura® Contact Center but they are typically in different geographic locations and subnets.

In a combined campus and geographic solution, one server is the Active server and one is the Remote Geographic Node server. The active server actively processes scripts, contacts and records statistics. The Remote Geographic Node server shadows the active server database. The Remote Geographic Node server copies all configuration changes made on the active server and monitors the active server status.

The Remote Geographic Node server must match the active 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 active server and it must be patched to the same level. The active and Remote Geographic Node servers must have the same patch level and the same operating system updates.

The Remote Geographic Node server does not automatically take over if the active (campus) system fails. You must start the Remote Geographic Node server manually. For more information on manually switching over to a Remote Geographic Node server, see [How to manually switch over to the Remote Geographic Node of a Mission Critical solution](#) on page 182 or [How to manually switch over to the Remote Geographic Node in an AML CS1000-based solution](#) on page 204.

Geographic standby server and network configuration

In a Geographic High Availability environment where the servers need not be physically close, configure High Availability to perform a full site-by-site switchover.

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).

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 balance. The process of grouping NICs is called teaming. 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 is a licensed feature. It is enabled when you purchase a standby server license.

For campus High Availability, 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 High Availability license, and does not use the grace period mechanism.

For geographic High Availability, 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 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 re-instate the active server.

Hot patching

Microsoft Windows Server 2008 does not support the patching of running applications. You must stop a Windows Server 2008 application to patch it. Avaya Aura® Contact Center is supported on the Microsoft Windows Server 2008 operating system. The Avaya Aura® 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 Avaya Aura® Contact Center patches might not support Hot Patching and these patches might require a maintenance window. Read the patch Readme file to determine if a patch supports Hot Patching.

Avaya Aura® Contact Center Service Packs (for example, Service Pack 8) do not support Hot patching. To install a Service Pack, you must schedule a maintenance cycle and restart the contact center. Avaya Aura® Contact Center Service Packs that deliver dot releases, for example a Service Pack that upgrades from Release 6.2 to Release 6.3, do not support Hot patching. For more information, read the Service Pack Readme file.

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 *Avaya Aura® Contact Center Upgrade and Patches* (44400-410).

More information

- For information on Mission Critical High Availability see [Mission Critical High Availability](#) on page 168.
- For information on Hot-standby High Availability, see [Hot-standby High Availability](#) on page 197.
- For information on Warm standby High Availability, see [Warm standby High Availability](#) on page 206.
- More information and procedures to install the active and standby servers and configuring the databases on each server are in *Avaya Aura® Contact Center Installation* (44400-311), *Avaya Aura® Contact Center Commissioning* (44400-312) and *Avaya Aura® Contact Center Server Administration* (44400-610).

Chapter 15: Mission Critical High Availability

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

The level of Avaya Aura® 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. This is achieved by deploying your Contact Center solution with a resilient Avaya Aura® Unified Communications platform configured for High Availability. Avaya Aura® Contact Center also supports Geographic Disaster Recovery and data resiliency in certain configurations. Avaya Aura® Contact Center supports the following Mission Critical High Availability solutions:

- [Mission Critical HA with Avaya Aura platform resiliency](#) on page 168
- [Mission Critical HA with Midsize Enterprise](#) on page 170
- [Mission Critical HA without Avaya Aura platform resiliency](#) on page 171
- [Mission Critical HA with Avaya Aura Unified Communications Virtualized Environment](#) on page 173

Mission Critical HA with Avaya Aura® platform resiliency

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

- Two Voice Contact Servers that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), License Manager, and Contact Center Manager Administration (CCMA) configured as a High Availability pair.
- Two Multimedia Contact Servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA on a Voice and Multimedia Contact Server. You can use two Voice and Multimedia Contact Servers configured as a High Availability pair instead of two Voice Contact Servers and two Multimedia Contact Servers.
- Two or more Avaya Media Server Linux-based servers, configured as a High Availability pair. Avaya Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.

- Two Avaya Aura® Session Manager (SM) instances.
- Two Avaya Aura® Application Enablement Services (AES) servers with Avaya Aura® System Platform-based High Availability.
- Two Avaya Aura® Communication Manager (CM) servers configured as a High Availability Duplex pair.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

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

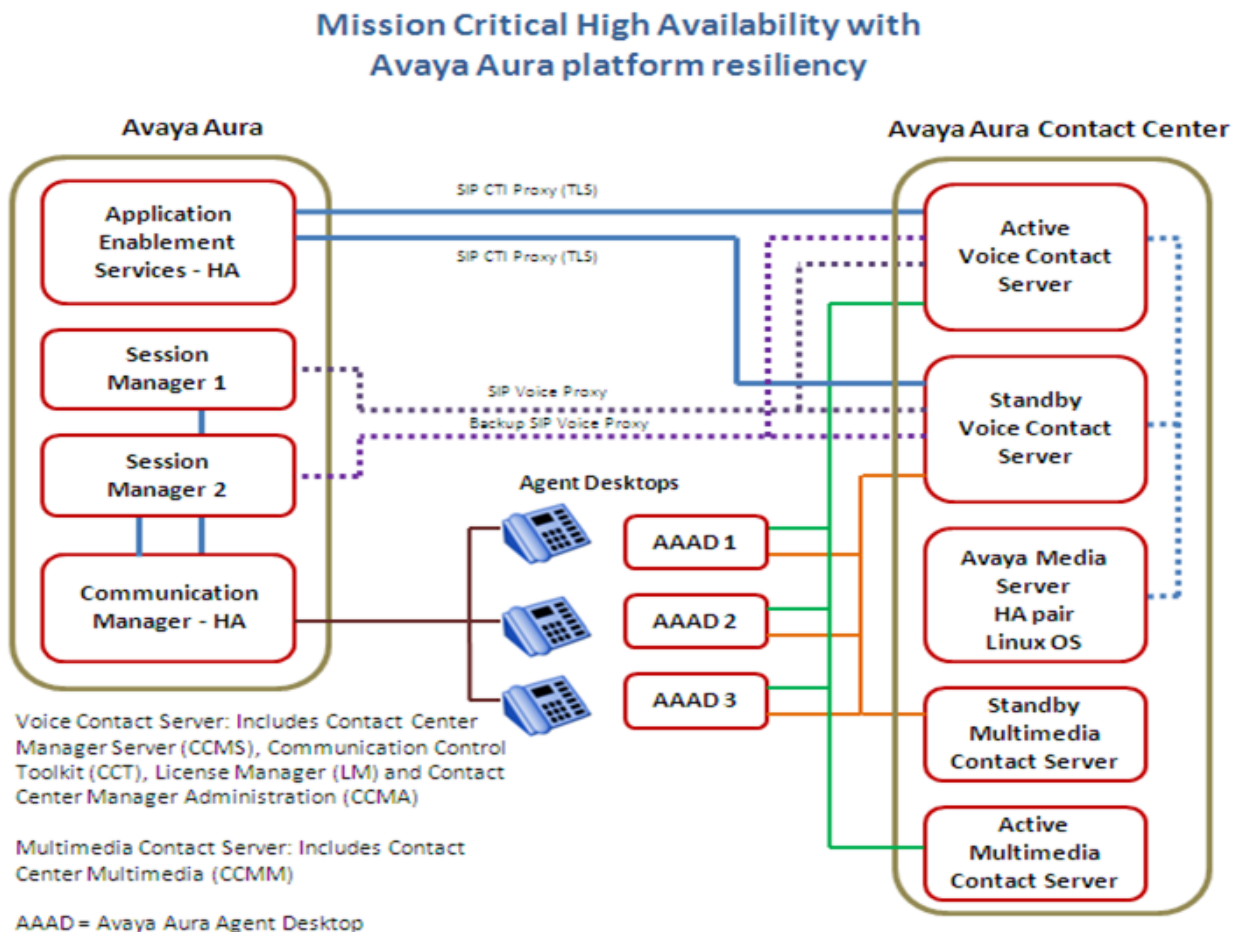


Figure 17: Example of a typical Mission Critical High Availability solution with a resilient Avaya Aura® platform

Mission Critical HA with Midsize Enterprise

Avaya Aura® Contact Center supports the Avaya Aura® Solution for Midsize Enterprise (ME) Release 6.2 Fast Reboot High Availability (FRHA) feature. To achieve Mission Critical High Availability using Midsize Enterprise you must have a SIP-enabled Contact Center with the following:

- Two Voice Contact Servers that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), License Manager, and Contact Center Manager Administration (CCMA) configured as a High Availability pair.
- Two Multimedia Contact Servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA on a Voice and Multimedia Contact Server. You can use two Voice and Multimedia Contact Servers configured as a High Availability pair instead of two Voice Contact Servers and two Multimedia Contact Servers.
- Two or more Avaya Media Server Linux-based servers, configured as a High Availability pair. Avaya Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.
- Two Midsize Enterprise Release 6.2 servers, configured for High Availability.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

The following diagram shows a typical Mission Critical High Availability solution with Avaya Aura® Solution for Midsize Enterprise Release 6.2.

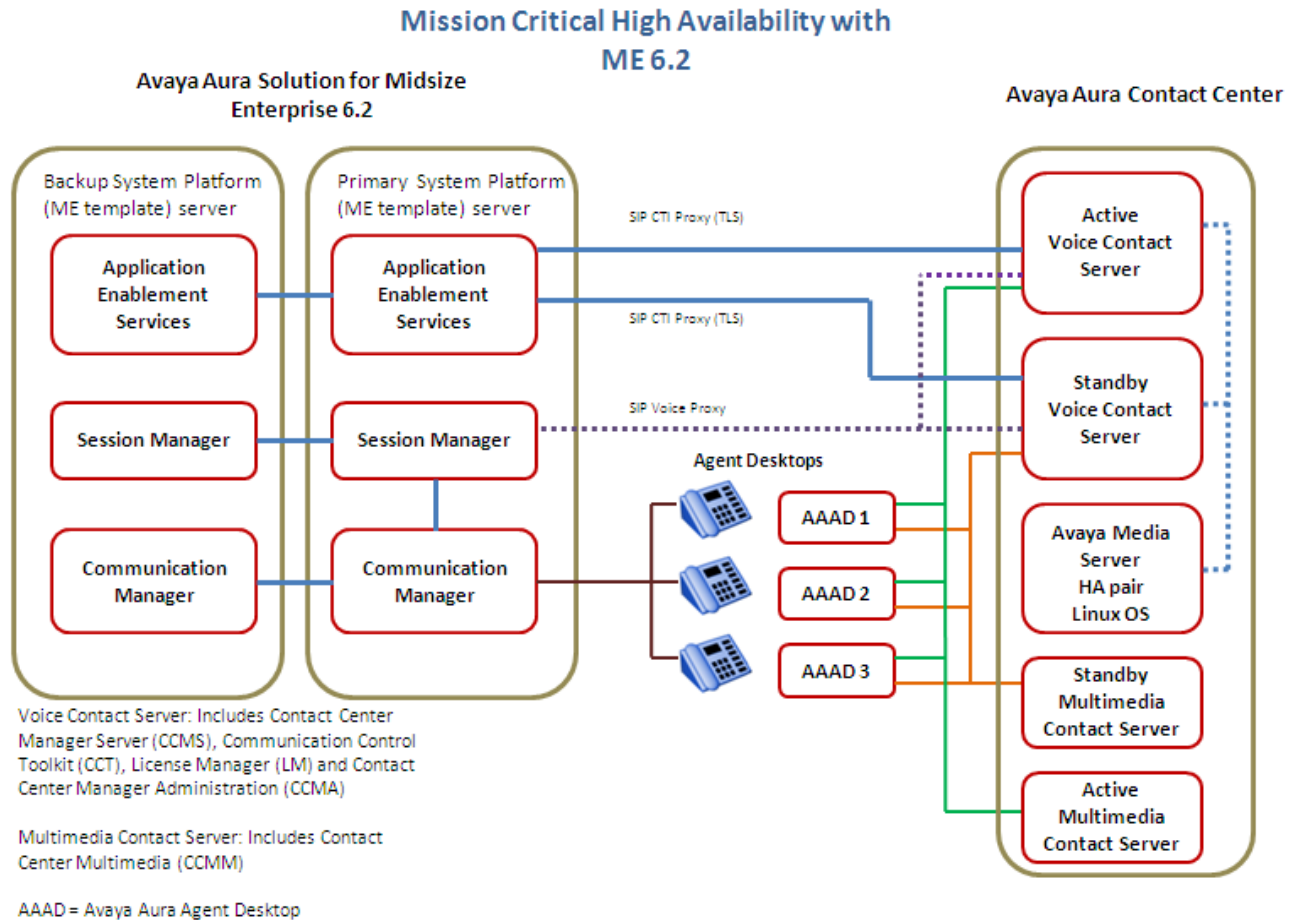


Figure 18: Example of a typical Mission Critical High Availability solution with ME

Mission Critical HA without Avaya Aura® platform resiliency

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

- Two Voice Contact Servers that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), License Manager, and Contact Center Manager Administration (CCMA) configured as a High Availability pair.
- Two Multimedia Contact Servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA on a Voice and Multimedia Contact Server. You can use two Voice and Multimedia Contact Servers configured as a High Availability pair instead of two Voice Contact Servers and two Multimedia Contact Servers.

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

*** Note:**

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

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

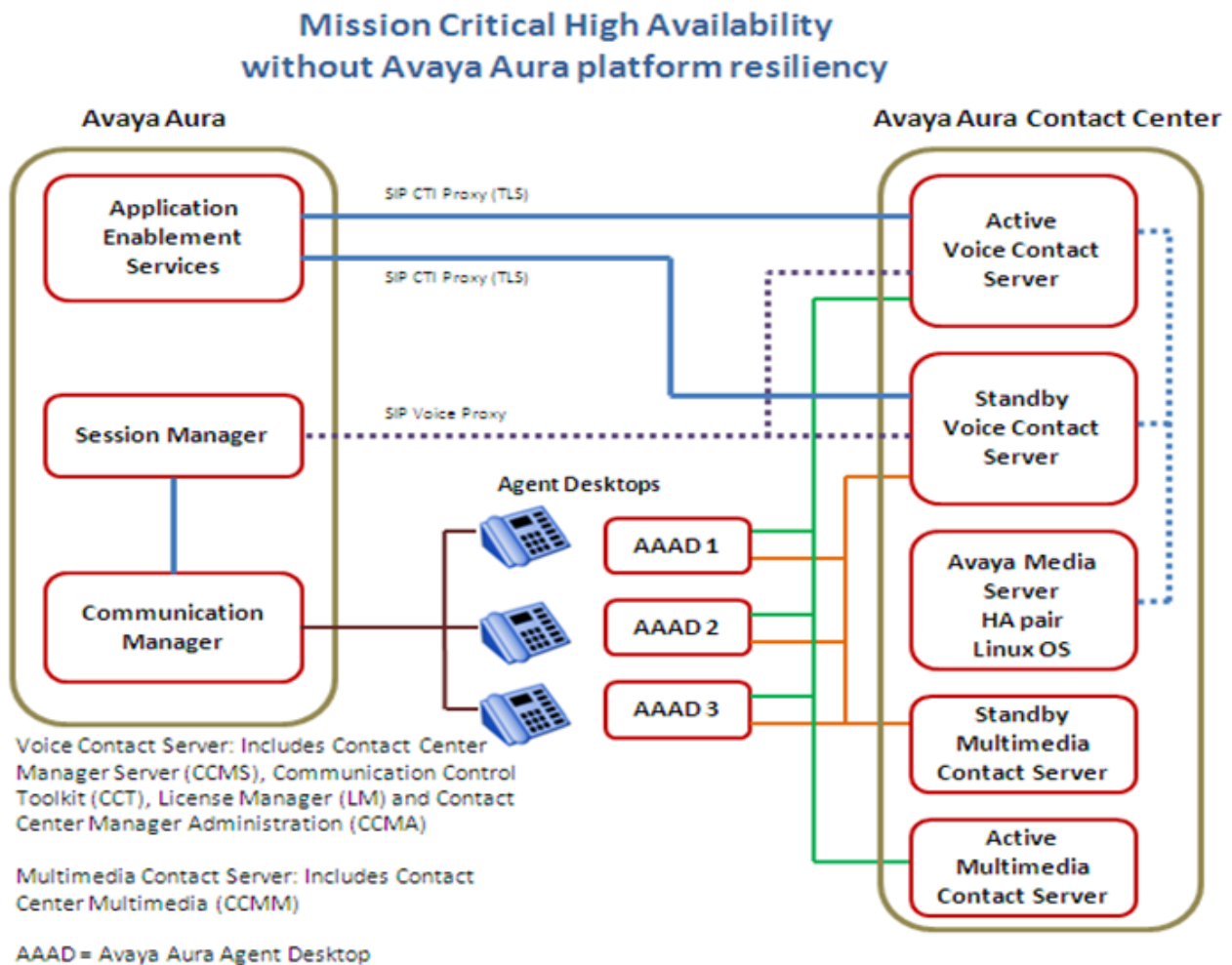


Figure 19: Example of a typical Mission Critical High Availability solution without a resilient Avaya Aura® platform

Mission Critical HA with Avaya Aura® Unified Communications Virtualized Environment

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

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

- Two Voice Contact Servers that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), License Manager, and Contact Center Manager Administration (CCMA) configured as a High Availability pair.
- Two Multimedia Contact Servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA on a Voice and Multimedia Contact Server. You can use two Voice and Multimedia Contact Servers configured as a High Availability pair instead of two Voice Contact Servers and two Multimedia Contact Servers.
- Two or more Avaya Media Server Linux-based servers, configured as a High Availability pair. Avaya Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.
- One Avaya Aura® Unified Communications Virtualized Environment (VE) voice platform. This solution type does not provide voice platform resiliency.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

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

- Two Voice Contact Servers that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), License Manager, and Contact Center Manager Administration (CCMA) configured as a High Availability pair.
- Two Multimedia Contact Servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA on a Voice and Multimedia Contact Server. You can use two Voice and Multimedia Contact Servers configured as a High Availability pair instead of two Voice Contact Servers and two Multimedia Contact Servers.
- Two or more Avaya Media Server Linux-based servers, configured as a High Availability pair. Avaya Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.
- Two Avaya Aura® Unified Communications Virtualized Environment (VE) voice platforms.

 Note:

This solution type provides Contact Center Mission Critical High Availability resiliency, but with limited Avaya Aura® Unified Communications Virtualized Environment voice platform resiliency. This solution uses a single Avaya Aura® Application Enablement Services instance. This Application Enablement Services instance is a single point of failure in the Contact Center solution.

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

Mission Critical High Availability overview

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

All of the Avaya Aura® Contact Center components (CCMS, CCMA, CCT, LM, CCMM, and Avaya Media Server) must be in the same network subnet IP address range. All of the Avaya Aura® Unified Communications components (CM, SM, and AES) must be in the same campus network location as the Avaya Aura® Contact Center components.

All Avaya Aura® Contact Center components (CCMS, CCMA, CCT, and CCMM) 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. The active and standby Avaya Aura® Contact Center servers must be in the same subnet IP address range for campus High Availability resiliency to work. All Avaya Aura® Agent Desktop clients must be registered in this domain, or in domains with a two-way trust relationship with this Contact Center server domain.

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

Contact Center Administrators use the active server in daily operation. Configuration changes made to the active system during normal operation are automatically copied to the standby applications, therefore the standby applications are configured and ready to take over processing from the active system. Statistical data is also automatically copied to the standby applications. Data is replicated to the standby applications in near real time.

Switchover

In a Mission Critical High Availability campus solution, a monitored CCMS or CCT service failure, hardware, network, or database failure can initiate a switchover but only in the following situations:

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

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an Active server, a switchover occurs. If the Contact Center Administrator

uses System Control and Monitor Utility (SCMU) to stop a monitored service on an Active server, a switchover does not occur.

Agent experience during a switchover

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

*** Note:**

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

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

Administrator experience during a switchover

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

If an active Contact Center Manager Server, Communication Control Toolkit, or Contact Center Manager Administration application or server fails, the Contact Center Manager Administration client Web browser continues to use the managed name and the Contact Center Administrator continues working by refreshing the Web browser.

Supervisor experience during a switchover

Agent states such as logged in state and ready state are maintained when the active Avaya Aura® Contact Center server fails, and this is reflected in the Real Time Displays (RTDs) being observed. Not all real-time values such as time in state are maintained however, and the supervisor notices that some RTD items are reset. The supervisor must inform IT staff, who receive an automatic email/SNMP switchover notification in parallel, and can then proceed with the Customer's normal follow-up procedure for dealing with a server switchover.

The RTDs must be configured to use multicast as opposed to unicast in order eliminate the need to manually restart the RTD after an Avaya Aura® Contact Center server switchover.

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

*** Note:**

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

Mission Critical solution

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

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

If a network communication failure occurs, the Active and Standby servers use a Trusted IP address to diagnose network connectivity faults. Use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

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

If SMMC on the Standby server cannot communicate with the Active Server, but can communicate with the Trusted IP address, SMMC enables call processing on the Standby server. If SMMC on the Standby server cannot communicate with the Active Server or with the Trusted IP address, the Standby server shuts down.

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

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

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

The following table shows the Mission Critical Active and Standby server configurations and outcomes.

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

Rebooting High Availability servers

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

Changing Mission Critical Standby servers

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

- Use SMMC to shutdown the HA system on the Active and Standby servers.
- Configure the new Standby server.
- Configure the Active server to use the new Standby server.
- Reboot the Active and Standby servers.
- Use SMMC to start the HA system on the Active and Standby servers.
- Use SMMC to enable Switchover on the Active server.

Mission Critical High Availability configuration utilities

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

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

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

High Availability Utility (Mission Critical High Availability version)

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

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

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

SMMC system tray

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

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

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

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

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

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

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

Table continues...

High Availability status	SMMC icon
The Geographic Standby server HA system is shadowing and synchronized with the Active server.	

High Availability Utility and SMMC system tray

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

How to reinstate High Availability resiliency after a switchover

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

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

- On the currently active running server (previous standby server), run the Database Maintenance utility and back up all database applications to a network share. You do not need to stop the active server to back up the applications.
- On the currently stopped server (previous active server), ensure that High Availability shadowing is still stopped.

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

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

Run Server Configuration to update the local server information to identify the real local IP addresses. Ensure that the License Manager IP address and license type are correct.

- On the Active server, start High Availability and enable switchovers.
- On the Standby server, start High Availability, enable switchovers, and start shadowing.
- If your HA solution supports multimedia contacts, on the primary Contact Center Multimedia server, restart the CCMM Multimedia Contact Manager service.

For more information about these High Availability related procedures, see *Avaya Aura® Contact Center Server Administration* (44400-610).

How to reinstate High Availability resiliency after a total network outage

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

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

- Ensure the Active and Standby servers can communicate with each other and the Trusted IP address.
- Configure the Active server to be the High Availability Active server.
- Start High Availability on the Active server.
- Backup the Active server databases and restore them on to the Standby server.
- Configure the Standby server to be the High Availability Standby server.
- On the Standby server, use Server Configuration to verify that the Standby server details are correct.
- Start High Availability on the Standby server.
- Enable switchovers on the Active server.

For more information about these High Availability related procedures, see *Avaya Aura® Contact Center Server Administration* (44400-610).

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

If the High Availability campus site fails or is shutdown, you can manually start your Remote Geographic Node solution. During normal operation the Remote Geographic Node (RGN) shadows the campus site database. The RGN is configured to use local voice platform and multimedia resources. The RGN is configured with the same agent and skillset information as the campus site. If the campus site fails or is shutdown, you must start the RGN Contact Center and Avaya Aura® Agent Desktop applications.

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

1. On the Remote Geographic Node (RGN), use the System Management and Monitoring Component (SMMC) system tray to stop the High Availability system. This ensures that the Remote Geographic Node server is not shadowing data from the campus site.

2. On the RGN server, using the High Availability configuration utility, select “Temporarily set as non-HA”.
3. Restore the most recent campus primary CCMA database (mdb) files to the RGN CCMA.
4. On the RGN server, use the SMMC system tray to start Contact Center services.
5. On the RGN server, use the System Control and Monitor Utility (SCMU) to verify that all core Contact Center services started.
6. Log on to the RGN CCMA and confirm that the CCMS, CCT, and CCMM servers have been updated with the RGN server name and IP addresses.
7. On the Avaya Media Server primary node of the RGN site, on the Element Manager Cluster Configuration - Replication Settings page, clear the 'Master Cluster Primary Node Address' option. This stops the RGN site from attempting to replicate content from the primary Avaya Media Server data center on the campus site.
8. Log on to the RGN CCMA. From the CCMA Launchpad, select Configuration, and then Media Servers. Enable the “Master Content Store” option for the local RGN Avaya Media Server or the local RGN Avaya Media Server HA pair.
9. Launch Agent Desktop clients using the RGN Voice and Multimedia Contact Server host name.
10. If your Contact Center solution uses an external Web Communications server, configure the Web Communications server to update the files with the RGN server name.

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

When upgrading a HA-enabled server to Avaya Aura® Contact Center Release 6.4, you must use the HA configuration utility to configure and apply the server mode details again. This reduces the number of steps if you need to switch over from a campus solution to a Remote Geographic Node.

For more detailed information about this outline procedure, see the High Availability chapter in *Avaya Aura® Contact Center Server Administration* (44400-610).

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

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

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

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

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

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

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

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

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

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

When upgrading a HA-enabled server to Avaya Aura® Contact Center Release 6.4, you must use the HA configuration utility to configure and apply the server mode details again. This reduces the number of steps if you need to switch over from a Remote Geographic Node to a campus solution.

For more detailed information about this outline procedure, see the High Availability chapter in *Avaya Aura® Contact Center Server Administration* (44400-610).

Switchover Handling Script

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

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

If the Active CCMS server is shutdown or fails, a switchover occurs, and the Standby CCMS server starts processing calls. The Standby CCMS server is now the Active CCMS server. New calls that arrive after the switchover are presented to the Master script on the currently Active CCMS server and call processing continues as normal.

Calls that were in treatment on the Avaya Media Server during the switchover cannot be returned to their original Active CCMS because it is no longer available, so these calls are routed to the Switchover Handling Script on the currently Active CCMS.

The Switchover Handling Script expedites the calls that were in treatment at the time of the active server failure. This means that calls are queued as quickly as possible to an appropriate skillset for that contact type. This can be a default skillset, or a skillset defined by the Contact Center Administrator.

Calls in treatment during a switchover might contain data, depending on their position in the script on the Active server before the switchover occurred. Avaya recommends that you modify the default

Switchover Handling Script to check each call for useful data. If the call does not have useful data, queue the call to the appropriate default skillset.

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

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

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

 Note:

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

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

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

- SEND INFO
- SEND REQUEST
- GET RESPONSE

The Switchover Handling Script does not support the following commands:

- EXECUTE SCRIPT
- GIVE BUSY
- GIVE MUSIC
- GIVE OVERFLOW
- GIVE RAN
- GIVE RINGBACK

- GIVE SILENCE
- GIVE IVR
- GIVE Controlled Broadcast

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

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

Other applications cannot start the Switchover Handling Script, and the Switchover Handling Script cannot start other applications. For more information about scripts and applications, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (44400-510).

Avaya Aura® platform campus resiliency

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

Avaya Aura® platform campus resiliency supports the following:

- Communication Manager survivability. For more information, see [Communication Manager survivability overview](#) on page 189
- Session Manager redundancy. For more information, see [Session Manager redundancy overview](#) on page 189
- Either Application Enablement Services Fast Reboot High Availability (FRHA) or Machine Preserving High Availability (MPHA). For more information, see [Application Enablement Services Fast Reboot High Availability \(FRHA\) overview](#) on page 190 and [Application Enablement Services Machine Preserving High Availability \(MPHA\) overview](#) on page 191
- Avaya Aura® Solution for Midsize Enterprise Fast Reboot High Availability (FRHA). For more information, see [Avaya Aura® Solution for Midsize Enterprise Solution for Midsize Enterprise 6.2 Fast Reboot High Availability \(FRHA\) overview](#) on page 193

High Availability campus site

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

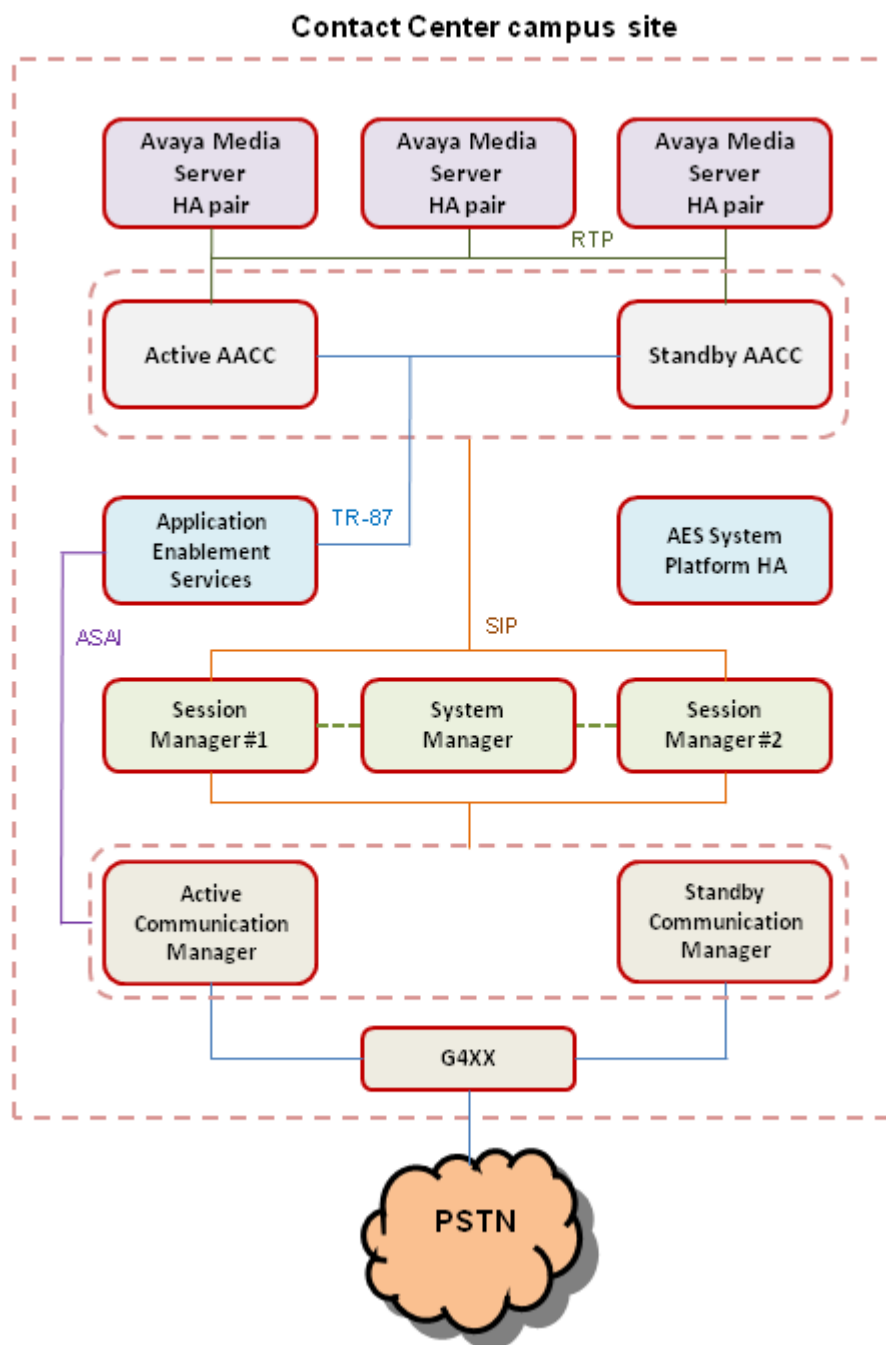


Figure 20: Example of a campus voice-enabled site with platform resiliency

Communication Manager survivability overview

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

Example of Communication Manager campus survivability:

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

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

Contact Center experience if a Communication Manager fails

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

Session Manager redundancy overview

Avaya Aura® Session Manager Releases 6.1 and 6.2 use the active-active approach where two instances are simultaneously active; any request routes to either instance, and a failure of one of the Session Manager instances does not interrupt new calls. Active-active redundancy requires that the Session Manager instances be interconnected over an IP network with sufficient bandwidth and low enough latency to synchronize runtime data.

Example of Session Manager redundancy:

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

Add SM-2 as the backup Session Manager server.

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

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

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

Contact Center experience if a Session Manager fails

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

Application Enablement Services Fast Reboot High Availability (FRHA) overview

Application Enablement Services (AES) supports the System Platform Fast Reboot High Availability (FRHA) mode. FRHA is the default High Availability protection mode for Application Enablement Services 6.1 and 6.2. Once initialized, the High Availability software on the active node propagates this configuration to virtual machines on the standby node. FRHA continuously captures and propagates disk data from the active node to the standby node to allow for recovery from any future switchover or failover events. As implied by the name of this High Availability mode, any planned, preemptive, or unplanned failover event causes the standby node to become the new active node, and its virtual machines boot up to continue providing solution services in your network.

System Platform High Availability Failover is a licensed feature, and, if required, you must purchase it when ordering Application Enablement Services (AES) Releases 6.1 or 6.2.

AES Fast Reboot High Availability switchover or failover

An active node switchover or failover can be triggered by many different issues, both planned and unplanned. An administrator can perform a planned switchover when the active and standby nodes become synchronized and therefore contain the same data. The administrator performs this action typically to complete maintenance on the active server, causing it to become the new standby node during the maintenance action.

An automatic preemptive failover, initiated by the system, is typically triggered by ongoing detection of an intermittent hardware failure or transient shortages of node resources (for example, insufficient disk or memory space). Similar to a planned switchover, a preemptive switchover requires full disk data synchronization across the active and standby servers.

An unplanned failover is typically caused by a loss of power, a sudden and severe hardware failure, or a sudden loss of connectivity.

Regardless of the High Availability event type, the failover cause is available on the High Availability page of the System Platform web console.

AES 6.2 Fast Reboot High Availability requirements

AES 6.2 Fast Reboot High Availability failover requires the following:

- Two System Platform supported servers with exactly the same hardware configuration.
- Both servers must be in close proximity (within 100 meters) so that they can be connected with an Ethernet crossover cable.
- The same version of System Platform must be installed on the active and standby nodes, and both servers must be patched to the same level.
- Install the AES solution template on the active node.
- Do not install a template on the standby node.

You must perform all System Platform, High Availability, and AES template configuration using the System Platform web console of the primary server.

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

Contact Center experience during the AES switchover or failover

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

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

Note:

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

Application Enablement Services Machine Preserving High Availability overview

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

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

- a hardware failure

- a network failure
- a server reboot or server shutdown

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

Important Considerations

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

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

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

MPHA does not protect against AES software failures.

Important:

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

MPHA failover requirements

Machine Preserving High Availability failover requires the following:

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

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

Contact Center experience during the MPHA failover

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

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

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

*** Note:**

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

Avaya Aura® Solution for Midsize Enterprise 6.2 Fast Reboot High Availability (FRHA) overview

Midsize Enterprise (ME) supports the System Platform Fast Reboot High Availability (FRHA) mode. FRHA is the default High Availability protection mode for Midsize Enterprise 6.2. Once initialized, the High Availability software on the active node propagates this configuration to virtual machines on the standby node. FRHA continuously captures and propagates disk data from the active node to the standby node to allow for recovery from any future switchover or failover events. As implied by the name of this High Availability mode, any planned, preemptive, or unplanned failover event causes the standby node to become the new active node, and its virtual machines boot up to continue providing solution services in your network.

ME 6.2 does not support resiliency in geographic Wide Area Network (WAN) solutions.

ME 6.2 High Availability switchover or failover

An active node switchover or failover can be triggered by many different issues, both planned and unplanned. An administrator can perform a planned switchover when the active and standby nodes become synchronized and therefore contain the same data. The administrator performs this action typically to complete maintenance on the active server, causing it to become the new standby node during the maintenance action.

An automatic preemptive failover, initiated by the system, is typically triggered by ongoing detection of an intermittent hardware failure or transient shortages of node resources (for example, insufficient disk or memory space). Similar to a planned switchover, a preemptive switchover requires full disk data synchronization across the active and standby servers.

An unplanned failover is typically caused by a loss of power, a sudden and severe hardware failure, or a sudden loss of connectivity.

Regardless of the High Availability event type, the failover cause is available on the High Availability page of the System Platform web console.

ME 6.2 High Availability failover requirements

ME 6.2 Fast Reboot High Availability failover requires the following:

- Two System Platform supported servers with exactly the same hardware configuration.
- Both servers must be in close proximity (within 100 meters) so that they can be connected with an Ethernet crossover cable.
- The same version of System Platform must be installed on the active and standby nodes, and both servers must be patched to the same level.
- Install the Avaya Aura® Solution for Midsize Enterprise solution template on the active node.
- Do not install a template on the standby node.

You must perform all System Platform, High Availability, and Midsize Enterprise template configuration using the System Platform web console of the primary server.

For more information on ME 6.2 and the FRHA feature, see *Implementing Avaya Aura® Solution for Midsize Enterprise*.

Contact Center experience during the ME 6.2 failover

There is a brief pause in operations associated with a node switchover or failover event, in addition to the time it takes for all virtual machines to boot on the new active server. In total, it can take up to ten minutes for a switchover or failover on the ME to complete.

During this period, Avaya Aura® Agent Desktop client software displays a message box advising agents to use their desk phones to answer voice calls. However, established calls and calls that are incoming around the time of the failure are lost. Calls cannot be processed during this Fast Reboot High Availability failover period. Agents can continue processing email messages using Agent Desktop software. When the ME failover to the standby node is complete Contact Center Manager Server regains call control and Agent Desktop client software displays another message box advising agents to use Agent Desktop to handle voice calls.

Avaya Aura® platform geographic resiliency

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

Avaya Aura® platform geographic resiliency supports the following:

- [Communication Manager Survivable Core \(ESS\)](#) on page 195
- [Session Manager geographical redundancy overview](#) on page 196
- [Application Enablement Services geographical redundancy overview](#) on page 196

Campus site and remote geographic site

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

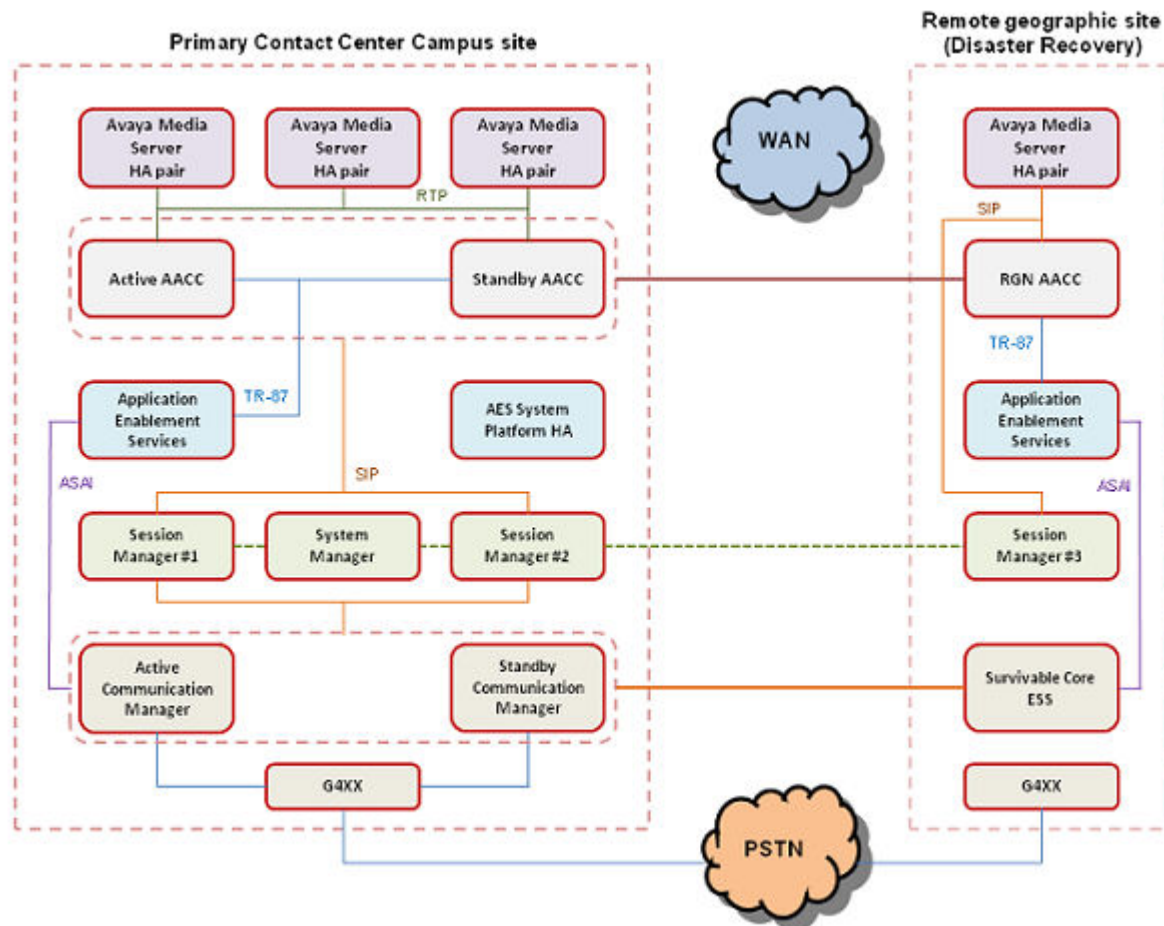


Figure 21: Example of a campus site with a disaster recovery remote geographic site

Communication Manager Survivable Core (ESS)

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

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

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

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

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

Session Manager geographical redundancy overview

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

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

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

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

Application Enablement Services geographical redundancy overview

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

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

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

Important:

Avaya Aura® Contact Center does not support the native AES geographic redundancy feature, with an AES MPHA configuration on the remote site replicating from an AES MPHA configuration on the campus site.

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

Chapter 16: Hot-standby High Availability

To achieve hot-standby High Availability you must have an AML-based Contact Center with the following:

- Two Voice Contact Servers that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT) and Contact Center Manager Administration (CCMA) configured as a High Availability pair.
- Two Multimedia Contact Servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA on a Voice and Multimedia Contact Server. You can use two Voice and Multimedia Contact Servers configured as a High Availability pair instead of two Voice Contact Servers and two Multimedia Contact Servers.
- Avaya Communication Server 1000 High Availability PBX, Release 7.0 or later.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

All of the Avaya Aura® Contact Center components (CCMS, CCMA, CCT, LM, and CCMM) must be in the same network subnet IP address range. The Avaya Communication Server 1000 PBX must be in the same campus network location as the Avaya Aura® Contact Center components.

All Avaya Aura® Contact Center servers (CCMS, CCMA, CCT, and CCMM) 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 Aura® Agent Desktop clients must be registered in this domain, or in domains with a two-way trust relationship with this Contact Center server domain.

The following diagram shows a typical hot-standby High Availability solution.

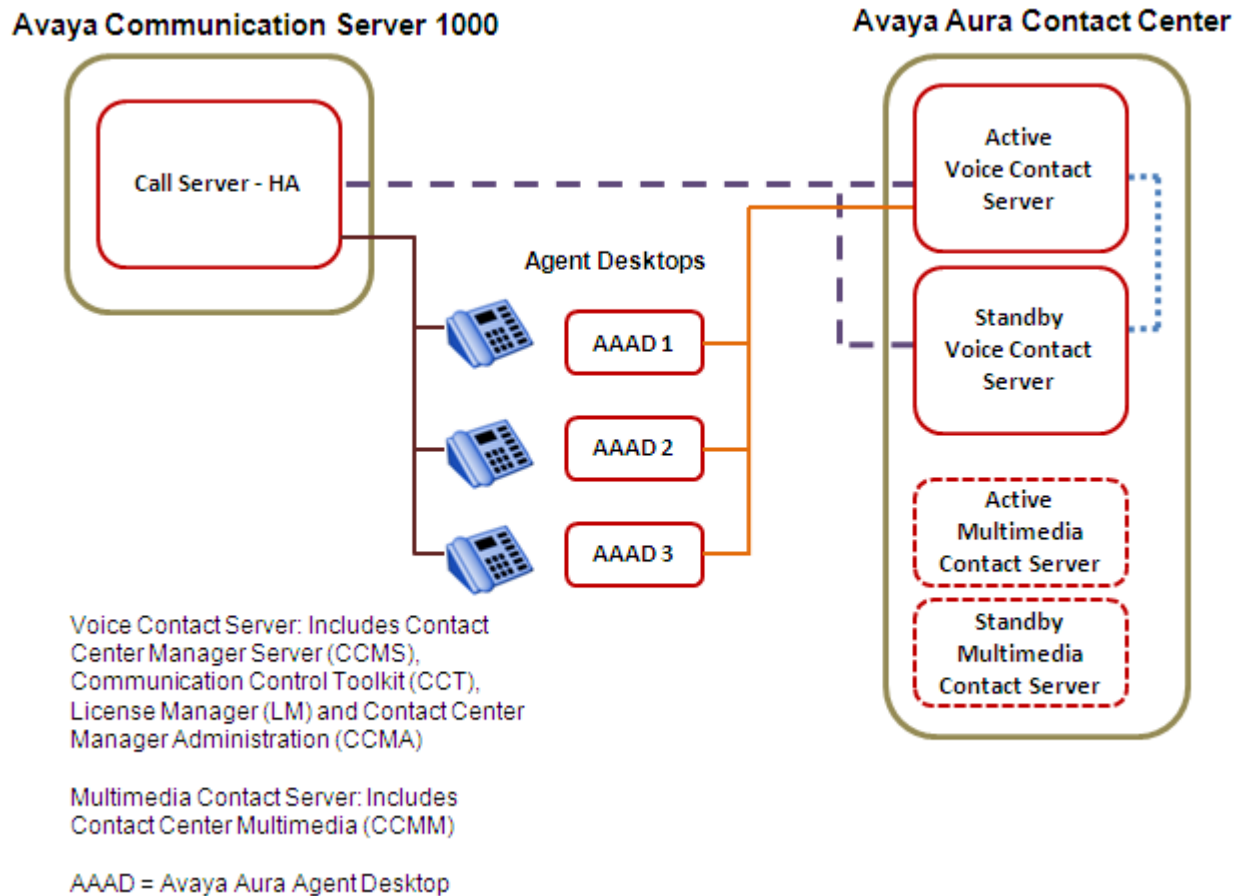


Figure 22: Example of a typical hot-standby High Availability solution

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).

One set of Avaya Aura® Contact Center applications (a CCMS, a CCT, and an optional CCMM) actively processes scripts and contacts. This set of applications is called the active set. Another set of Contact Center applications in the same Contact Center system, runs in hot-standby mode. This standby set of Contact Center applications monitors and shadows the active applications in the system and does not process calls. The standby CCMS monitors the active CCMS. The standby CCT monitors the active CCT. The standby CCMM monitors the active CCMM. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts.

Contact Center Administrators use the active server in daily operation. Configuration changes made to the active system during normal operation are automatically copied to the standby applications, therefore the standby applications are configured and ready to take over processing from the active system. Statistical data is also automatically copied to the standby applications. Data is replicated to the standby applications in real time.

Switchover

In a High Availability campus solution, a monitored CCMS or CCT service failure, hardware, network, or database failure can initiate a switchover but only in the following situations:

- The active and standby servers are in running state.
- The active server is running. All the critical CCMS and CCT services are monitored and running.
- The active server has Switchover enabled.
- The shadowing latency is less than the latency threshold.
- A database restore is not running on the Standby server.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database.
- The standby server can communicate with (ping) the Trusted IP address.

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

The Shadowing Latency threshold is used to validate how much time the Standby server needs to catch up with the Active server shadowed database contents. The default value of the Shadowing Latency threshold is 120 seconds. You can review the Shadow Latency information on the Open High Availability utility - System panel. The Shadow Latency must be greater than or equal to zero, but less than the latency threshold. The latency threshold is calculated as 120 seconds plus the Switchover timeout value as configured on the Server Mode panel of the High Availability utility.

To reinstate High Availability resiliency after a switchover, it is sometimes necessary to restore a database backup onto the new (post-switchover) standby server. The following table shows when a database restore is required to reinstate High Availability resiliency after a switchover:

Cause of switchover	Database restore required
Active server critical service outage	No
Manual switchover	No
Active server ELAN network outage	No
Active server CLAN (contact center subnet) network outage	Yes
Complete network outage	Yes
Active server crash	Yes
Active server reboot	Yes

After a switchover, you can review the System Control panel of the High Availability utility on the (post-switchover) standby server to confirm if a database restore is necessary. In the High Availability utility — *System Control* panel, in the *Information* box, look for a notice about restoring the database(s).

Agent experience during a switchover

If any Avaya Aura® Contact Center application or server fails, the hot-standby High Availability solution maintains the logon state of voice Avaya Aura® Agent Desktop agents. Calls in progress between a customer and an agent are not affected. The logon state of multimedia-enabled agents is not preserved when a switchover to a standby application occurs. For a CS 1000-based, voice-only Contact Center system with 5000 active agents, it takes approximately 30 seconds for the standby Contact Center Manager Server to begin processing new incoming calls in the script. If your contact center uses Open Queue for multimedia contacts, or CallPilot, the time delay for the standby Contact Center Manager Server to process new incoming calls in the script is a few minutes. During this short period, calls are given default ACD by the CS 1000. No established calls are lost. No calls that are incoming around the time of the failure are lost. No calls that are in treatment at the time of the failure are lost. There is no call loss. The reporting subsystem in Contact Center Manager Server (CCMS) recovers shortly after the script is operational, and the server starts to record events and statistics in the database as normal.

Like Contact Center Manager Server, the Communication Control Toolkit (CCT) server exhibits a zero-touch stateful recovery with hot-standby performance. If a phone call is on-hold and a switchover occurs, the Agent might have to take the call off hold using their phone. If pop-ups are used at the time of a CCT server outage, then the pop-ups resume seamlessly in less than 30 seconds.

In a hot-standby High Availability solution Avaya Aura® Agent Desktop clients are registered with the managed IP address of the active CCT server. In multimedia-enabled solutions Agent Desktop clients are registered with the managed IP address of the active Contact Center Multimedia server. During a switchover, multimedia enabled-agents might notice a short delay in receiving new contacts.

Note:

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

Administrator experience during a switchover

In a hot-standby High Availability campus solution the Contact Center Administrator launches Contact Center Manager Administration using the managed name of the server.

If an active Contact Center Manager Server, Communication Control Toolkit, or Contact Center Manager Administration application or server fails, the Contact Center Manager Administration client Web browser continues to use the managed name and the Contact Center Administrator continues working by refreshing the Web browser.

*** Note:**

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

High Availability Utility

Configure hot-standby and warm standby High Availability resiliency for CCMS, CCT and CCMM using the High Availability Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

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

The High Availability utility on an Active Server has the following dialogs under the Tasks tab:

- CC Applications
 - Start or stop the system
 - Enable or disable CC applications
 - Enable or disable switchover on the CC applications
 - Display system information

- CC Configuration
 - Monitor application service status
 - Define which application services are stopped or started
 - Configure how often a service restarts before switching over to the standby server
- System Control
 - Initiate a manual switchover for the Active Server
 - Initiate Standby Server shadowing

Use the hot-standby and warm standby High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which is the standby server. This utility is also used to start database shadowing and High Availability functionality. This version of the High Availability Utility does not use the System Management and Monitoring Component (SMMC) system tray.

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

How to reinstate High Availability resiliency after a switchover

In a Hot-standby or Warm standby campus solution, if the Active server fails or if a manual switchover is triggered, the Standby server starts processing contacts. The initially active server is now stopped, and the High Availability - Enable Switchover option is disabled. The Standby server becomes the Active server and it continues to process contacts. The High Availability SMTP feature sends an email to the Contact Center Administrator informing them about the switchover. The Active server has no corresponding Standby server at this point, and the solution is no longer resilient.

After a switchover, the High Availability Utility displays a message on the System Control panel if a database restore is required to reinstate High Availability resiliency:

- After a manual switchover, a database restore to the new Standby server is not required.
- After a switchover caused by a critical service problem, a database restore to the new Standby server is not required.
- After a switchover caused by a contact center subnet (CLAN) network outage, the High Availability Utility displays a message to inform the user to restore the Active server database to the new Standby server.
- After a switchover caused by an ELAN subnet network outage, a database restore to the new Standby server is not required.
- After a switchover caused by an Active server crash, the High Availability Utility displays a message to inform the user to restore the Active server database to the new Standby server.

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

1. If the High Availability Utility — System Control panel displays a message stating that a database restore to the new Standby server is required, perform these sub steps. Otherwise, skip to step 2.
 - a. On the currently active running server (previous standby server), run the Database Maintenance utility and back up all database applications to a network share. You do not need to stop the active server to back up the applications.
 - b. On the currently stopped server (previous active server), stop High Availability shadowing.
 - c. Use the Database Maintenance utility to restore the Contact Center databases from the network share.
2. In the High Availability configuration utility, configure this stopped server to be the Standby High Availability server.
3. Run Server Configuration to update the local server information to identify the real local IP addresses. Ensure that the License Manager IP address and license type are correct.
4. On the Active server, start High Availability and enable switchovers.
5. On the Standby server, start High Availability, enable switchovers, and start shadowing.
6. If your HA solution supports multimedia contacts, on the primary Contact Center Multimedia server, restart the CCMM Multimedia Contact Manager service.

For more information about these High Availability related procedures, see *Avaya Aura® Contact Center Server Administration* (44400-610).

How to reinstate High Availability resiliency after a total network outage

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

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

- Ensure the Active and Standby servers can communicate with each other and the Trusted IP address.
- Configure the Active server to be the High Availability Active server.
- Start High Availability on the Active server.

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

For more information about these High Availability related procedures, see *Avaya Aura® Contact Center Server Administration* (44400-610).

How to manually switch over to the Remote Geographic Node in an AML CS1000-based solution

If the CS1000 AML-based Hot standby High Availability campus site fails or is shutdown, you can manually commission and start the Remote Geographic Node solution. During normal operation the Remote Geographic Node (RGN) shadows the campus site database. The RGN is therefore configured with the same information as the campus site. The RGN is correctly configured with the same agent and skillset information as the campus site.

If the campus site fails or is shutdown, you commission the RGN servers by ensuring the server configuration details point to local telephony and multimedia resources at the RGN location.

In the following example the geographic site has a Remote Geographic Node Voice Contact Server and a Remote Geographic Node Multimedia Contact Server.

Before commissioning the Remote Geographic Node server:

- Completely disable the Active and Standby servers on the campus site.
- Activate the Avaya Communication Server 1000 (CS1000) Survivable Media Gateway on the geographic site.

Remote Geographic Node CCMS, CCMA, and CCT configuration

Perform the following steps on the Remote Geographic Node (RGN) Voice Contact Server:

- Use the HA utility to verify that shadowing has stopped. Stop shadowing if it has not.
- Use the HA utility to select, while in RGN server mode, the **Temporarily set as non-HA** check box, and click **OK**.
- Restore the most recent campus primary CCMA database to the RGN CCMA.
- Use the System Control and Monitor Utility (SCMU) to start all services.
- Log on to the RGN CCMA Web administration, and confirm that the CCMS, CCT, and CCMM servers have updated to the RGN server name and IP address.
- Launch Agent Desktop.

- If your Contact Center solution uses an external Web Communications server, configure the Web Communications server to update the files with the RGN server name.

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

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

In the following example the campus site has a Remote Geographic Node Voice Contact Server that includes CCMS, CCMA, LM and CCT, a Voice Contact Server, and a standalone Avaya Media Server.

- Stop all contact center services on the RGN servers.
- On the RGN servers, backup all the application databases and the ADMIN database.
- On the RGN servers, using the High Availability utility, clear the **Temporarily set as non-HA** check box. This sets the RGN servers back to RGN mode.
- Restore the RGN database backups on the campus active servers.
- On the active CCMA server, restore the most recent CCMA database (mdb) files from the RGN CCMA using selective restore.
- On the active servers, using the High Availability utility, under **Tasks > CC Applications**, click **Start** to start HA. This starts the AACC services.
- Use the System Control and Monitor Utility (SCMU) to confirm that all services started.
- Log on to CCMA. CCMA displays the RGN Information message, which prompts you to confirm changing the CCMS, CCT, and CCMM server names to the original campus values.
- On the RGN Information message, click **Yes**.
- After Active server is up, take the database backup from the active server, and restore this backup to both the Standby server and the RGN server.
- On the Standby and RGN servers, using the High Availability utility, start shadowing.

Chapter 17: Warm standby High Availability

Avaya Aura® Contact Center supports the following warm standby High Availability (HA) solutions.

Contact Center Multimedia in standalone configuration:

- Two No Switch Configured — Voice and Multimedia Contact Server with Avaya Media Server servers that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), Contact Center Manager Administration (CCMA) and Contact Center Multimedia (CCMM) configured as a High Availability pair.
- Redundant Ethernet switches.
- This configuration is supported only for Campus High Availability.

Important:

Avaya Media Server High Availability is not supported on the Windows operating system. Avaya Media Server High Availability is supported only on the Linux operating system. If you plan to implement High Availability for the No Switch Configured Multimedia Only solution, you must uninstall Avaya Media Server from both the primary and the backup Multimedia Only servers. For more information about removing Avaya Media Server, see *Avaya Aura® Contact Center Installation* (44400-311).

Avaya Aura® Call Center Elite voice and Avaya Aura® Contact Center multimedia complement configuration:

- Two AACC Multimedia Complement for Elite servers that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), Contact Center Manager Administration (CCMA) and Contact Center Multimedia (CCMM) configured as a High Availability pair.
- Avaya Aura® Call Center Elite.
- Redundant Ethernet switches.
- This configuration is supported only for Campus High Availability.

All of the Avaya Aura® Contact Center components (CCMS, CCMA, CCT, LM, CCMM) must be in the same network subnet IP address range. All of the contact center components must be in the same network subnet or campus network location.

The following diagram shows a typical warm standby High Availability solution.

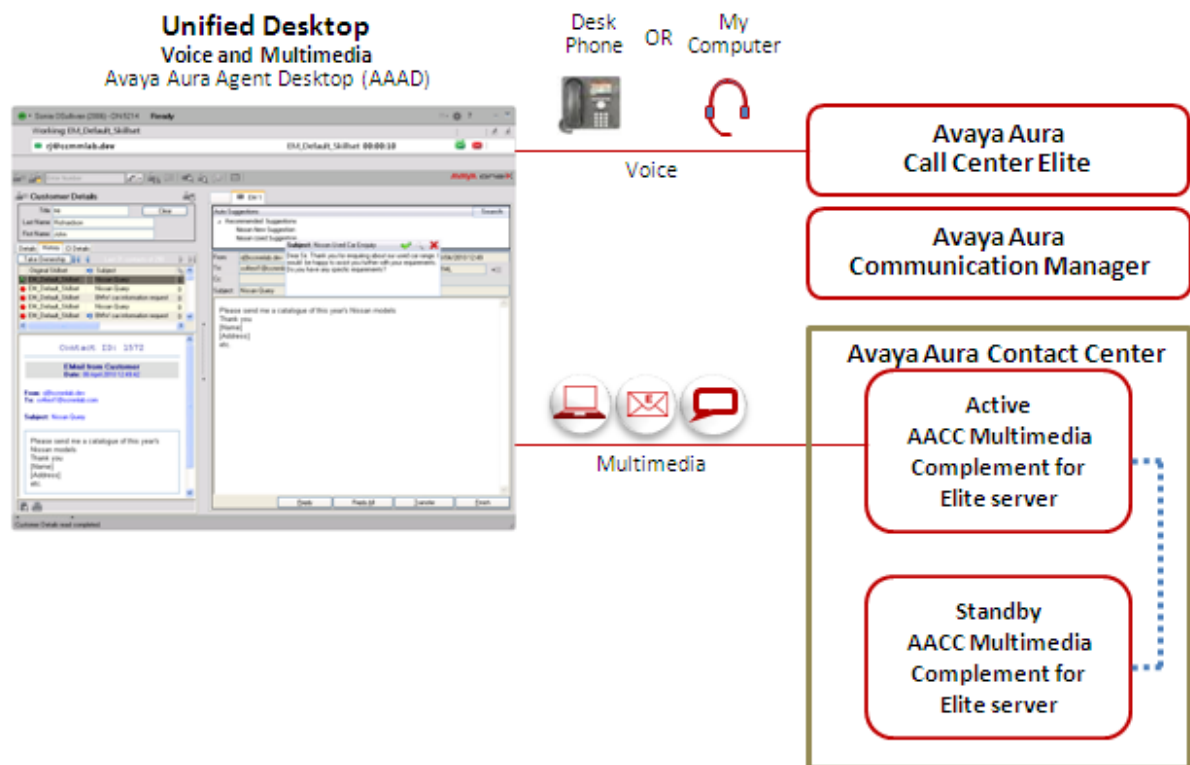


Figure 23: Example of a typical warm standby High Availability solution

Avaya Aura® Contact Center supports warm standby High Availability (HA) resiliency for Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Multimedia (CCMM).

One set of Avaya Aura® Contact Center applications (a CCMS, a CCT, and an optional CCMM) actively processes scripts and contacts. This set of applications is called the active set. Another set of Contact Center applications in the same Contact Center system, runs in standby mode. This standby set of Contact Center applications monitors and shadows the active applications in the system and does not process calls. The standby CCMS monitors the active CCMS. The standby CCT monitors the active CCT. The standby CCMM monitors the active CCMM. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts.

Contact Center Administrators use the active server in daily operation. Configuration changes made to the active system during normal operation are automatically copied to the standby applications, therefore the standby applications are configured and ready to take over processing from the active system. Statistical data is also automatically copied to the standby applications. Data is replicated to the standby applications in real time.

Switchover

In a High Availability campus solution, a monitored CCMS or CCT service failure, hardware, network, or database failure can initiate a switchover but only in the following situations:

- The active and standby servers are in running state.
- The active server is running. All the critical CCMS and CCT services are monitored and running.
- The active server has Switchover enabled.
- The shadowing latency is less than the latency threshold.
- A database restore is not running on the Standby server.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database.
- The standby server can communicate with (ping) the Trusted IP address.

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

The Shadowing Latency threshold is used to validate how much time the Standby server needs to catch up with the Active server shadowed database contents. The default value of the Shadowing Latency threshold is 120 seconds. You can review the Shadow Latency information on the Open High Availability utility - System panel. The Shadow Latency must be greater than or equal to zero, but less than the latency threshold. The latency threshold is calculated as 120 seconds plus the Switchover timeout value as configured on the Server Mode panel of the High Availability utility.

To reinstate High Availability resiliency after a switchover, it is sometimes necessary to restore a database backup onto the new (post-switchover) standby server. The following table shows when a database restore is required to reinstate High Availability resiliency after a switchover:

Cause of switchover	Database restore required
Active server critical service outage	No
Manual switchover	No
Active server ELAN network outage	No
Active server CLAN (contact center subnet) network outage	Yes
Complete network outage	Yes
Active server crash	Yes
Active server reboot	Yes

After a switchover, you can review the System Control panel of the High Availability utility on the (post-switchover) standby server to confirm if a database restore is necessary. In the High Availability utility — *System Control* panel, in the *Information* box, look for a notice about restoring the database(s).

Agent experience during a switchover

In a warm-standby High Availability solution Agent Desktop clients are registered with the managed IP address of the High Availability server pair.

In the event of a switchover, once the standby server has transitioned to the active mode and taken over the Managed IP, Agent Desktop clients automatically reconnect to the newly active server.

*** Note:**

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

Administrator experience during a switchover

In a warm-standby High Availability campus solution, the Contact Center Administrator launches Contact Center Manager Administration using the managed name of the server.

If an active Contact Center Manager Server, Communication Control Toolkit, or Contact Center Manager Administration application or server fails, the Contact Center Manager Administration client Web browser continues to use the managed name and the Contact Center Administrator continues working by refreshing the Web browser.

*** Note:**

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

High Availability Utility

Configure hot-standby and warm standby High Availability resiliency for CCMS, CCT and CCMM using the High Availability Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

- Server Mode
 - Configure the IP address for the Active and Standby servers
 - Configure the IP address for Trusted servers
 - Configure the IP address for the Remote Geographic Node
 - Identify if the server is Active or Standby

- Enable Automatic Switchover
- Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs.
- Notifications
 - Configure an email server for email notifications
 - Configure where and how often to send email notifications
 - Configure the email character set
- System
 - Display information on the system status
 - Verify that shadowing is running

The High Availability utility on an Active Server has the following dialogs under the Tasks tab:

- CC Applications
 - Start or stop the system
 - Enable or disable CC applications
 - Enable or disable switchover on the CC applications
 - Display system information
- CC Configuration
 - Monitor application service status
 - Define which application services are stopped or started
 - Configure how often a service restarts before switching over to the standby server
- System Control
 - Initiate a manual switchover for the Active Server
 - Initiate Standby Server shadowing

Use the hot-standby and warm standby High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which is the standby server. This utility is also used to start database shadowing and High Availability functionality. This version of the High Availability Utility does not use the System Management and Monitoring Component (SMMC) system tray.

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

How to reinstate High Availability resiliency after a switchover

In a Hot-standby or Warm standby campus solution, if the Active server fails or if a manual switchover is triggered, the Standby server starts processing contacts. The initially active server is now stopped, and the High Availability - Enable Switchover option is disabled. The Standby server becomes the Active server and it continues to process contacts. The High Availability SMTP feature sends an email to the Contact Center Administrator informing them about the switchover. The Active server has no corresponding Standby server at this point, and the solution is no longer resilient.

After a switchover, the High Availability Utility displays a message on the System Control panel if a database restore is required to reinstate High Availability resiliency:

- After a manual switchover, a database restore to the new Standby server is not required.
- After a switchover caused by a critical service problem, a database restore to the new Standby server is not required.
- After a switchover caused by a contact center subnet (CLAN) network outage, the High Availability Utility displays a message to inform the user to restore the Active server database to the new Standby server.
- After a switchover caused by an ELAN subnet network outage, a database restore to the new Standby server is not required.
- After a switchover caused by an Active server crash, the High Availability Utility displays a message to inform the user to restore the Active server database to the new Standby server.

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

1. If the High Availability Utility — System Control panel displays a message stating that a database restore to the new Standby server is required, perform these sub steps. Otherwise, skip to step 2.
 - a. On the currently active running server (previous standby server), run the Database Maintenance utility and back up all database applications to a network share. You do not need to stop the active server to back up the applications.
 - b. On the currently stopped server (previous active server), stop High Availability shadowing.
 - c. Use the Database Maintenance utility to restore the Contact Center databases from the network share.
2. In the High Availability configuration utility, configure this stopped server to be the Standby High Availability server.
3. Run Server Configuration to update the local server information to identify the real local IP addresses. Ensure that the License Manager IP address and license type are correct.
4. On the Active server, start High Availability and enable switchovers.
5. On the Standby server, start High Availability, enable switchovers, and start shadowing.

6. If your HA solution supports multimedia contacts, on the primary Contact Center Multimedia server, restart the CCMM Multimedia Contact Manager service.

For more information about these High Availability related procedures, see *Avaya Aura® Contact Center Server Administration* (44400-610).

How to reinstate High Availability resiliency after a total network outage

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

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

- Ensure the Active and Standby servers can communicate with each other and the Trusted IP address.
- Configure the Active server to be the High Availability Active server.
- Start High Availability on the Active server.
- Backup the Active server databases and restore them on to the Standby server.
- Configure the Standby server to be the High Availability Standby server.
- On the Standby server, use Server Configuration to verify that the Standby server details are correct.
- Start High Availability on the Standby server.
- Enable switchovers on the Active server.

For more information about these High Availability related procedures, see *Avaya Aura® Contact Center Server Administration* (44400-610).

Chapter 18: 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 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

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	CS 1000 SIP-enabled Contact Center	Avaya Aura SIP-enabled Contact Center
Landing Pads	Yes	Yes	Yes
UUI SIP header	No	Yes	Yes
P-Intrinsic SIP header	No	Yes	Yes
SIP INFO message using Context Creation	No	Yes	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	CS 1000 SIP-enabled Contact Center	Avaya Aura SIP-enabled Contact Center
Landing Pads	OI Open Queue and OI Universal Networking.	OI Open Queue and OI Universal Networking.	OI Open Queue and OI Universal Networking.

Table continues...

Solution type	CS 1000 AML-based Contact Center	CS 1000 SIP-enabled Contact Center	Avaya Aura SIP-enabled Contact Center
Front-end Avaya Aura® Experience Portal	N/A	No additional licenses required.	No additional licenses required.
Back-end Avaya Aura® Experience Portal	N/A	No additional licenses required.	No additional licenses required.
SIP INFO message using Context Creation	N/A	No additional licenses required.	No additional licenses required.

! Important:

Avaya Aura® Contact Center Release 6.4 does not support SIP-enabled Avaya Communication Server 1000 for new installations. Existing Avaya Aura® Contact Center solutions using SIP-enabled Avaya Communication Server 1000 can be expanded or upgraded.

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	CS 1000 SIP-enabled 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 Intrinsic.	Maximum Call Attached Data is 4096 bytes. Maximum 5 ASCII key-value pairs of Contact Intrinsic.	Maximum Call Attached Data is 4096 bytes. Maximum 5 ASCII key-value pairs of Contact Intrinsic.
UI SIP header using ASAI	N/A	96 bytes maximum.	96 bytes maximum.
P-Intrinsic SIP header	N/A	Depends on your solution. ^{Note 1}	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.	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-Intrinsic SIP header information: The amount of P-Intrinsic 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-Intrinsic.			

Table continues...

Transfer method	CS 1000 AML-based Contact Center	CS 1000 SIP-enabled Contact Center	Avaya Aura SIP-enabled Contact Center
- If your solution has an Avaya Aura® Communication Manager in the incoming call path, the Refer-To header for blind transfers is limited to 1500 bytes overall. - If your solution has an Avaya Aura® Communication Manager in the call path, for improved P-Intrinsics support, Avaya recommends Communication Manager Release 6.0.1 SP8 or later.			

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 and Avaya Communication Server 1000.

Avaya Aura® Contact Center supports User-to-User Information (UII) 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 Ininsics 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 (UII) 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, whereas 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 and Avaya Voice 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 Aura® 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 Aura® 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 Voice Portal or Avaya Aura® Experience Portal MPP server. Universal Call Identifier can be passed to Voice Portal or Avaya Aura® Experience Portal through an application's SIP headers. Voice Portal and 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
- SIP-enabled Avaya Communication Server 1000 solutions
- 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.

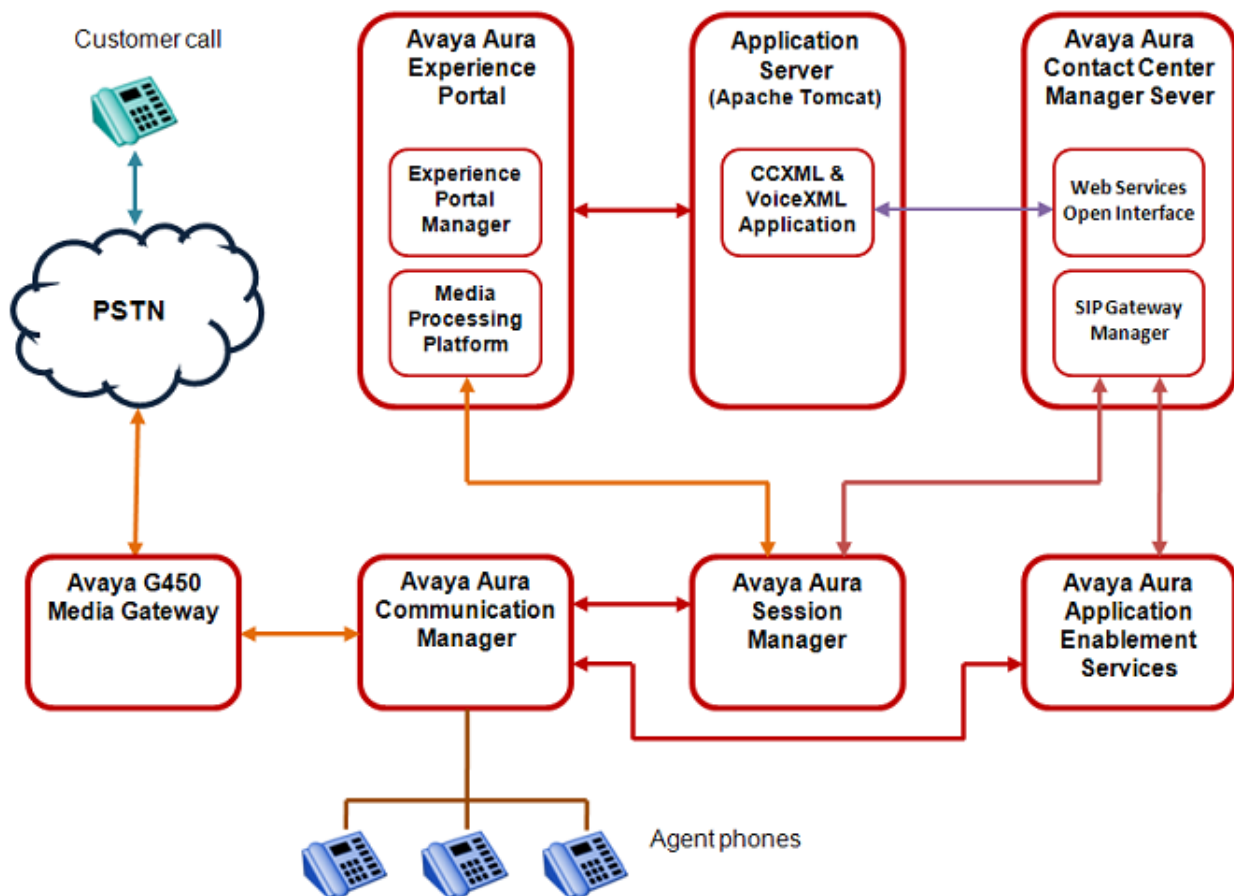


Figure 24: Example of front-end Avaya Aura® Experience Portal using Contact Center Web Service Open Interfaces

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 Intrinsic.
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. 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.
13. The call is offered to a Contact Center agent. In a SIP-enabled contact center, the agent can access customer details and Contact Intrinsic before answering the call.
14. The Contact Center agent answers the customer call.
15. The XML application terminates the call when it finishes execution or when the caller hangs up.

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 customers 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.

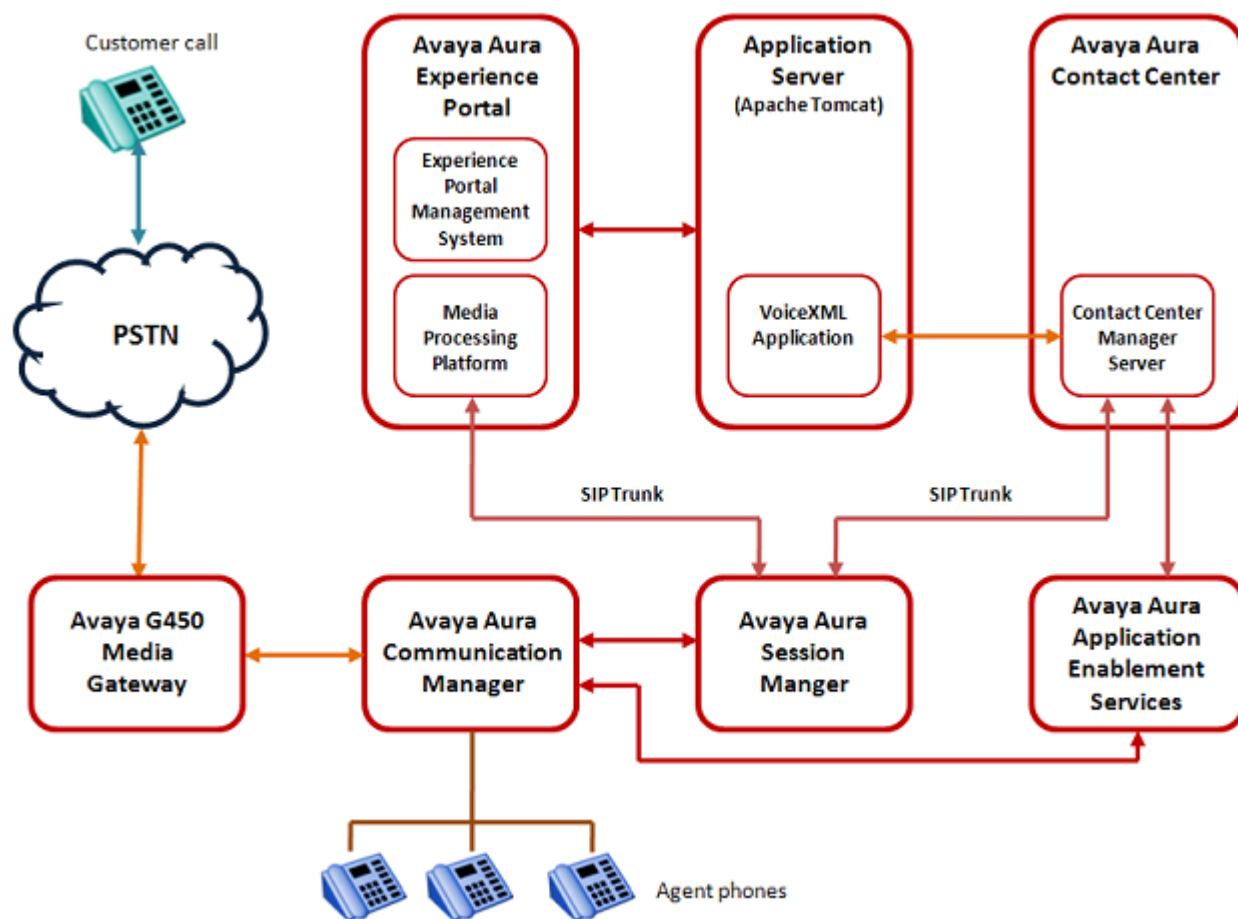


Figure 25: Example of front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

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 UI data generated Contact Intrinsic.
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 Intrinsic 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 hangs up.

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 (UII and P-Intrinsic) 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.

Avaya Aura Contact Center solution and back-end Avaya Aura Experience Portal

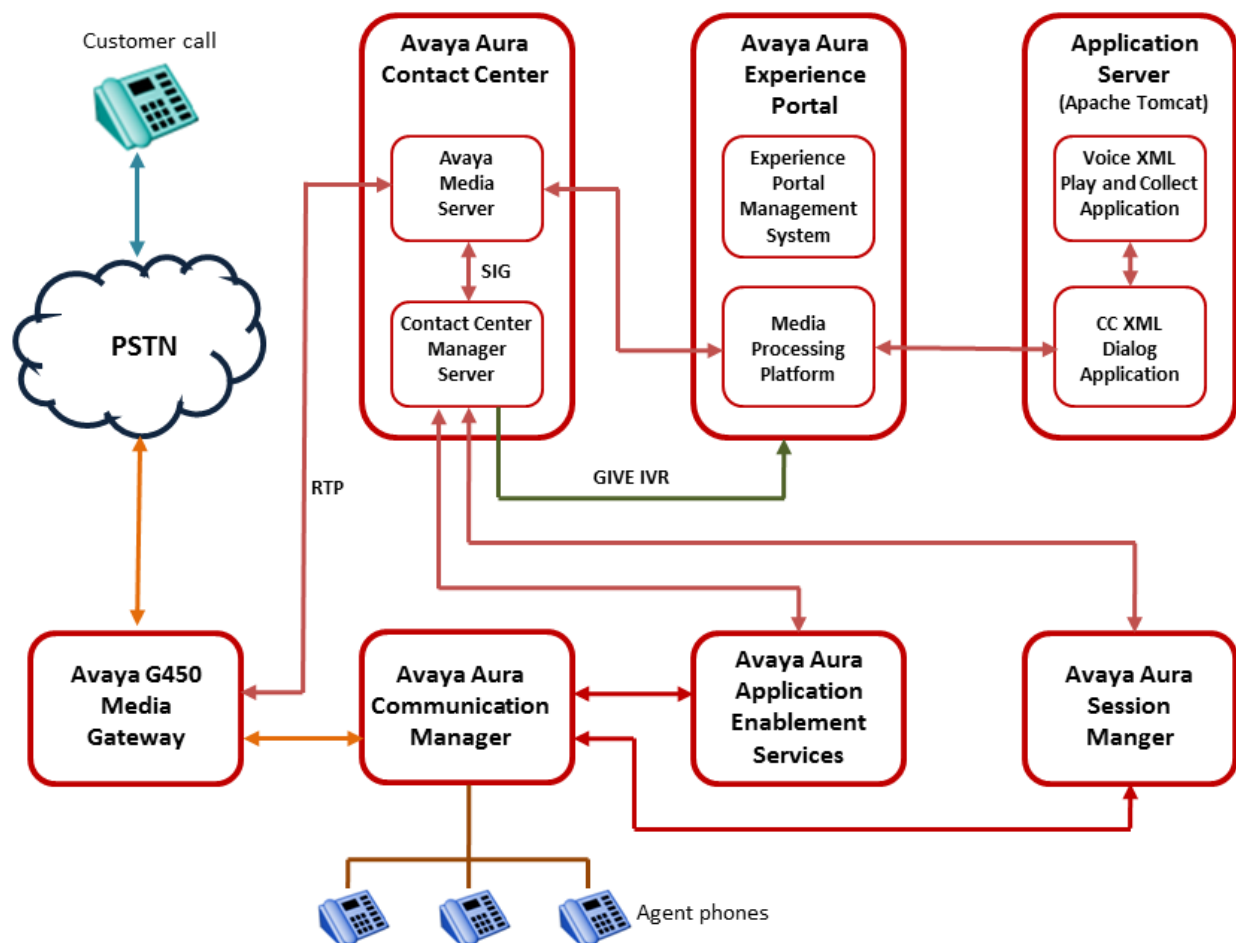


Figure 26: Example of back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

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 UII 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 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 (UI) 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, whereas 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 Intrinsic. The Orchestration Designer script can then access and use the Contact Intrinsic for the call, and Contact Center can pass them on to Avaya Aura® 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.

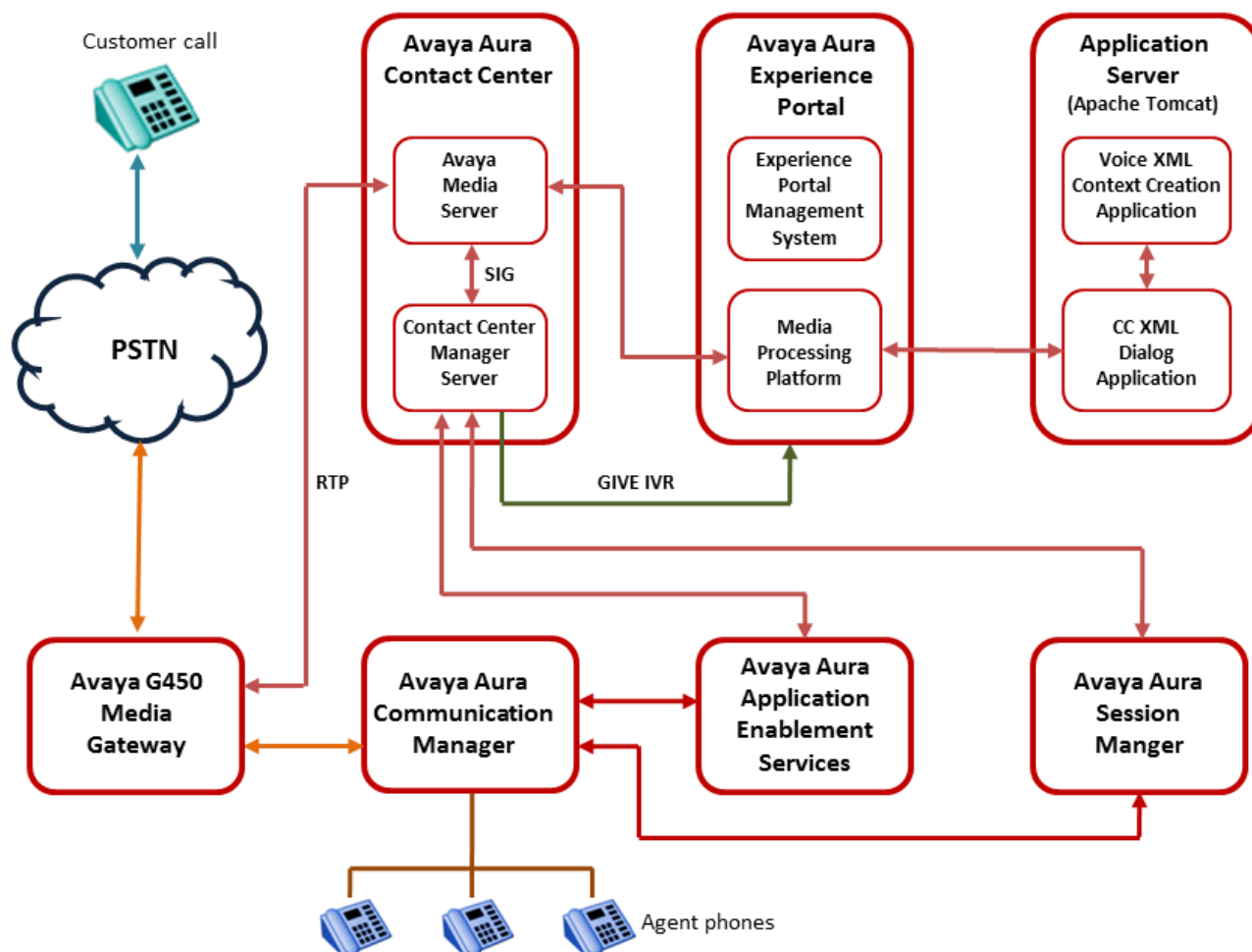


Figure 27: Example of back-end Avaya Aura® Experience Portal using the Context Creation sample application

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 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 Intrinsic.
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 Voice Portal and 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 front-end self-service and Avaya Aura® Contact Center using SIP header sample files, see Orchestration Designer Sample Applications on www.avaya.com/devconnect.

For more information, and to download the complete Avaya Voice Portal front-end self-service and Avaya Aura® Contact Center using SIP header sample files, see Dialog Designer Sample Applications on www.avaya.com/devconnect.

Chapter 19: Avaya Aura® Call Center Elite integration

Avaya Aura® Contact Center supports integration with Avaya Aura® Call Center Elite. Avaya Aura® Call Center Elite provides voice-based contact centers. Avaya Aura® Contact Center provides voice and multimedia-enabled contact centers.

A combined Avaya Aura® Contact Center and Avaya Aura® Call Center Elite contact center solution provides:

- Unified agent desktop
- Unified reporting and performance management
- Unified agent administration

Avaya Aura® Contact Center offers a multimedia complement to an Avaya Aura® Call Center Elite voice-based contact center. Adding Avaya Aura® Contact Center multimedia capabilities to an Avaya Aura® Call Center Elite contact center increases the number of communication channels with customers, offers more flexibility, and is cost-effective. Multimedia-enabled agents are more productive, responsive, mobile, and more cost effective compared to voice-only agents.

The Avaya Aura® Contact Center Multimedia Complement for Elite server type is no longer available for new sales. You can upgrade an existing Multimedia Complement for Elite or migrate it to a new server.

Avaya Aura® Contact Center supports the following multimedia contact types:

- Email
- SMS text messages
- Fax messages
- Scanned documents
- Voice mail messages
- Web Communications
- Social Networking

The Avaya Aura® Contact Center Multimedia Complement for Elite server type is no longer available for new sales. You can upgrade an existing Multimedia Complement for Elite or migrate it to a new server.

A combined Avaya Aura® Call Center Elite and multimedia Avaya Aura® Contact Center solution builds on the individual strengths of the two products to deliver a full featured voice and multimedia contact center solution.

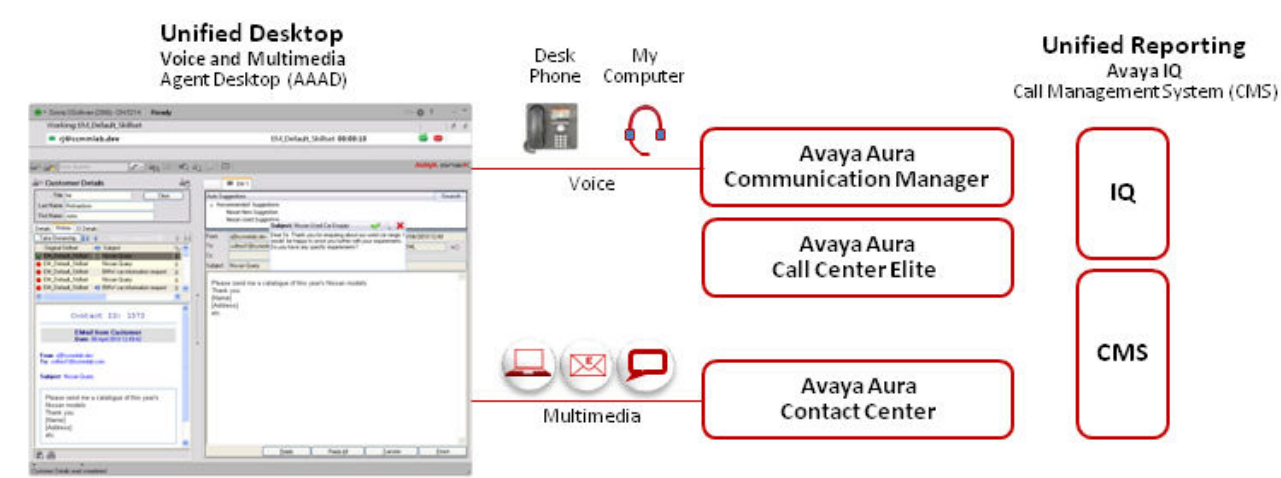


Figure 28: Example of an Avaya Aura® Call Center Elite and Contact Center integrated solution

Adding Avaya Aura® Contact Center multimedia capabilities to an Avaya Aura® Call Center Elite contact center requires a single additional Contact Center server, plus additional infrastructure to handle email based multimedia and Web communications. Adding Contact Center multimedia capabilities to an Avaya Aura® Call Center Elite call center does not impact voice call processing.

The Contact Center DVD installer simplifies Multimedia Complement for Elite installation and commissioning. Multimedia Complement for Elite installations offer the full range of multimedia agent skillsets, multimedia agent configuration, reporting, and pre-defined multimedia routing scripts.

For customers wishing to maintain their investment in Avaya Aura® Call Center Elite, Avaya Aura® Contact Center can be installed in parallel to provide multimedia capabilities. Avaya Aura® Contact Center supports SIP-enabled Avaya Aura® Unified Communications platform integration. You can use Avaya Aura® Contact Center to control the Avaya Aura® Unified Communications platform IP desk phones to handle voice contacts. This Avaya Aura® Unified Communications platform-based voice contact center can also be expanded to handle multimedia contacts, producing a voice and multimedia contact center on the Unified Communications platform.

The following table shows the supported Communication Manager–Avaya Aura® Call Center Elite system versions.

Platform	Supported Releases	Concurrent voice agents	Concurrent multimedia agents
Avaya Aura® Call Center Elite	3.x - 4 - 5.x - 6.x	Per Avaya Aura® Call Center Elite on Communication Manager release limit	3000

An Avaya Aura® Call Center Elite and multimedia Avaya Aura® Contact Center solution does not support the following:

- Instant Messages (IM) customer contact type
- Open Queue (not supported for voice)
- Video

An Avaya Aura® Call Center Elite and Avaya Aura® Contact Center solution supports Presence on Avaya Aura® Agent Desktop and peer-to-peer Instant Messaging (IM) between Agents and Experts. The Avaya Aura® Agent Desktop uses default reason codes for work, not ready, and logout actions for an agent that are configured in Contact Center Manager Administration agent profiles.

An Avaya Aura® Call Center Elite and Contact Center solution enables enterprises to deliver improved customer experience across many forms of contact and social media. The Contact Center solution communicates with customers using the customer's choice of media. Existing voice customers are maintained and continue to receive the familiar and personal phone experience. Existing and new customers can choose voice or email based channels. Multimedia aware customers can choose a communication media that suits their business needs or lifestyle, and experience the modern interactive and responsive service to which they are accustomed.

Multimedia-enabled contact centers are cost effective to operate and to communicate with. Multimedia-enabled agents deliver improved productivity, flexibility, choice, and mobility to customers.

Unified Agent Desktop

In a combined Avaya Aura® Call Center Elite and multimedia-enabled Avaya Aura® Contact Center solution some agents process only voice contacts, some agents process only multimedia customer contacts and some agents process both. Agents that process both voice and multimedia contacts are called blended agents.

Avaya Aura® Agent Desktop provides a single unified agent client-side software application that supports all contact types such as voice, email, SMS text messages, fax messages, scanned document messages, voice mail messages, and Web communications. The Agent Desktop multiplicity feature further enhances productivity by allowing agents to work on multiple customer contact Work Items simultaneously.

Agent Desktop connects to the Avaya Aura® Contact Center server to process multimedia contacts and to access the agent's multimedia statistics. Agents use the Agent Desktop—Agent Statistics feature to monitor their own productivity and performance with multimedia contacts.

Agent Desktop connects to the Communication Manager—Avaya Aura® Call Center Elite platform to process voice contacts and to access the agent's voice statistics. Agents use the Agent Desktop—Vu Stats feature to monitor their voice calls statistics.

Unified Agent Administration

Avaya Control Manager supports unified Call Center Elite and Avaya Aura® Contact Center agent administration. Control Manager provides seamless transition for customers running a mixed environment of Call Center Elite and AACC.

Control Manager supports:

- Adding agents simultaneously to both Call Center Elite and AACC
- Configuring agents to support voice calls using Call Center Elite.
- Configuring agent voice skills level assignments.
- Configuring agents to support multimedia contacts using AACC.
- Configuring agent multimedia skillsets.
- Moving Call Center Elite agents to work only on AACC multimedia contacts.
- Scheduling agents to move between skills and skillsets.

For more information about using Control Manager to configure AACC, see Using Avaya Control Manager on support.avaya.com.

Integrated Avaya Aura® Call Center Elite commissioning overview

The following is an overview of how to add multimedia capabilities to an existing Avaya Aura® Call Center Elite voice-based contact center by adding a single Avaya Aura® Contact Center server:

1. Read the Avaya Aura® Contact Center documentation to plan and engineer your multimedia addition.
2. Install and configure the necessary email, document scanning, and/or SMS text handling infrastructure as required.
3. Obtain an Avaya Aura® Contact Center multimedia license and software DVD.
4. Download the most recent Avaya Aura® Contact Center Service Packs.
5. Obtain a suitably engineered Windows Server 2008 Release 2 64-bit server.
6. Complete the *Avaya Aura® Contact Center Installation Checklist* (44400-310).
7. Add the Avaya Aura® Contact Center server to your contact center infrastructure, ensuring it can communicate with all Agent Desktop computers and with the Communication Manager–Avaya Aura® Call Center Elite platform.
8. Install Avaya Aura® Contact Center software using the “AACC Multimedia Complement for Elite” option. For more information about installing Avaya Aura® Contact Center, see *Avaya Aura® Contact Center Installation* (44400-311).

9. Commission Avaya Aura® Contact Center to add multimedia support to the Avaya Aura® Call Center Elite.

For more information, see *Avaya Aura® Contact Center Commissioning* (44400-312).

10. In Contact Center Manager Administration (CCMA), when adding the CCMM server to the servers list in CCMA, select “Elite Environment”. This configures CCMM to support Avaya Aura® Call Center Elite integration.
11. Using the CCMM Administration utility on the CCMM server, in the “Agent Desktop Configuration” —“Advanced” section, change the “Switch Type” to “SIP Avaya Aura 6.1”.
12. To enable Presence on Avaya Aura® Agent Desktop and peer-to-peer Instant Messaging (IM) between Agents and Experts, using the CCMM Administration utility on the CCMM server, in the “Agent Desktop Configuration” —“Advanced” section, change the “IM Provider” to “Microsoft OCS/Lync” or “Aura Presence Services” as appropriate to your solution.
13. In CCMA, for the “Elite Environment” enabled CCMM server, under “Multimedia Templates”, configure agent templates and profiles.

For more information about configuring agent templates and profiles, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611).

14. In CCMA, create Avaya Aura® Contact Center, Avaya Aura® Call Center Elite, and multimedia blended agents. Agents that process both voice and multimedia contacts are called blended agents. Do not enter a SIP URI for the blended Avaya Aura® Call Center Elite and multimedia agents.
15. In CCMA, configure the Avaya Aura® Contact Center agent skillsets, agent profiles, and routing rules.

For more information, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611).

16. In CCMA, assign a preferred template to each blended Avaya Aura® Call Center Elite and multimedia agent.
17. From each agent desktop computer, access the Avaya Aura® Contact Center Multimedia server to download and install Avaya Aura® Agent Desktop software. For more information about installing Avaya Aura® Agent Desktop, see *Avaya Aura® Agent Desktop User Guide* (44400-114).
18. On each agent desktop, log on to Avaya Aura® Agent Desktop to handle voice and multimedia contacts. Select the appropriate agent profile. On the “Telephony” tab, in the “Elite ACD” section, select the “Enable Elite ACD” check box. For more information about using Avaya Aura® Agent Desktop with Avaya Aura® Call Center Elite, see *Avaya Aura® Agent Desktop User Guide* (44400-114).
19. Backup the Avaya Aura® Contact Center functioning configuration. For more information about backing-up Avaya Aura® Contact Center databases, see *Avaya Aura® Contact Center Routine Maintenance* (44400-514).

The contact center agents are now ready to handle voice and multimedia communications with customers.

Chapter 20: 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 2008. When you install Windows Server 2008, Microsoft Remote Desktop Connection is installed but not enabled. You must enable the RDC manually. For information about enabling RDC, see the *Avaya Aura® Contact Center Server Administration* (44400-610).

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 (recommended)
- 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 remain 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 21: Product compatibility

This section specifies the interoperability and compatibility of Avaya Aura® Contact Center with the other supported components of a contact center solution.

- [Avaya Aura Unified Communications platform](#) on page 242
- [Avaya Communication Server 1000 platform](#) on page 245
- [Avaya Aura Experience Portal](#) on page 250
- [Additional voice services](#) on page 252

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

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 Aura® Agent Desktop supports Avaya Aura® Unified Communications phones and continues to support voice, email, and Web chat contact types.

Avaya Aura® Contact Center supports the following Avaya Aura® Unified Communications components:

Avaya Aura® component	Release
Avaya Aura® System Platform	6.x
Avaya Aura® Midsize Business Template (MBT)	5.2.x
Avaya Aura® Solution for Midsize Enterprise	6.2.x
Avaya Aura® Communication Manager	5.2, 6.x
Avaya Aura® SIP Enablement Services	5.2
Avaya Aura® Application Enablement Services	5.2, 6.x

Table continues...

Avaya Aura® component	Release
Avaya Aura® System Manager	6.x
Avaya Aura® Session Manager	6.x
Avaya Aura® Presence Services	6.x

! Important:

For more information about the supported Avaya Aura® Unified Communications Service Packs (SPs), Feature Packs (FPs), patches, and deployment types, refer to the Avaya Aura® 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 Avaya Aura® 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.

! Important:

Avaya Aura® Contact Center Release 6.4 does not support the Avaya Aura® Midsize Business Template (MBT) or Avaya Aura® Unified Communications Release 5.2 platforms for new installations. Existing Avaya Aura® Contact Center solutions using MBT or Avaya Aura® 5.2 can be expanded or upgraded.

Avaya Aura® Contact Center supports the following Avaya Aura® Call Center Elite releases:

Platform	Supported Releases	Concurrent voice agents	Concurrent multimedia agents
Avaya Aura® Call Center Elite	3.x , 4, 5.x , 6.0.1, 6.2	Per Avaya Aura® Call Center Elite on Communication Manager release limit.	3000

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 Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).

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	
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 MS Lync – Routed IM	Not Supported	
Shared MS Lync – 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
Support Call Center Elite on same Communication Manager	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 1600 Series IP deskphones
- Avaya 4600 Series IP deskphones
- Avaya 9600 Series IP deskphones
- Avaya 96x1 Series IP deskphones

- Avaya Aura® Agent Desktop embedded softphone:
 - Ensure you provision an IP_Agent license on the Communication Manager for each softphone used by the contact center.
 - The Communication Manager station associated with the Avaya Aura® Agent Desktop embedded softphone must not be configured as an Avaya 96x1 Series deskphone. Configure the Communication Manager station associated with the embedded softphone as one of the other supported H.323 phone types.
- Avaya one-X® Communicator Release 5.2 or later

Avaya Aura® Contact Center supports the following digital phones:

- Avaya 24xx Series deskphones
- Avaya 64xx 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 9611G IP deskphone
- Avaya 9621G IP deskphone
- Avaya 9641G IP deskphone

Avaya Aura® Contact Center supports SIP phones for DTMF functionality. Avaya Aura® Contact Center supports SIP phones for High Availability functionality.

Avaya Aura® 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
Avaya Communication Server PBX 51C	7.6
Avaya Communication Server PBX 81C	7.6

New Avaya Aura® Contact Center Release 6.4 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 6.4, 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.

Avaya Aura® Contact Center Release 6.4 does not support SIP-enabled Avaya Communication Server 1000 for new installations. Existing SIP-enabled Avaya Communication Server 1000 contact center installations can be expanded or upgraded.

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 packages are required in SIP-enabled solutions using an Avaya Communication Server 1000.

CS 1000 packages: 77, 153, 164, 242, 243, 324, 41, 42, 43, 50, 114, 155, 214, 215, 218, 247, 311, 324.

The following Avaya Communication Server 1000 patches are required in SIP-enabled solutions using an Avaya Communication Server 1000 Release 5.0, 5.5, or 6.0. These patches are not required in SIP-enabled solutions using Avaya Communication Server 1000 Release 7.0, 7.5 or 7.6.

CS 1000 Patch	Comment
MPLR29656	Required for call control and reporting
MPLR28954	Required for TR87 control on CS 1000 Release 6.0 only
MPLR28884	Required to fix one-way speech path on SIP REFER
MPLR27991	Required to fix SIP REFER issue on Signaling Server
MPLR29656	Required to get correct cause for OriginatedEvent only when using CS 1000 Release 5.5

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 3: 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 Union Break Time, Call Forcing, Alternate Call Answer, Host Delay Time for each agent
Walkaway trigger	Headset removal
Phone features	
Conference	6-way Conference
Transfer and conference	Separate transfer, conference, simple
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

Table continues...

Feature	Avaya Communication Server 1000 (AML)
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	
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 6.0, 7.0, and 7.0.1.

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 Intrinsic 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	CS 1000 SIP-enabled Contact Center	Avaya Aura SIP-enabled Contact Center
Landing Pads	Yes	Yes	Yes
UUI SIP header	No	Yes	Yes
P-Intrinsic SIP header	No	Yes	Yes
SIP INFO message using Context Creation	No	Yes	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	CS 1000 SIP-enabled Contact Center	Avaya Aura SIP-enabled Contact Center
Landing Pads	OI Open Queue and OI Universal Networking.	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.	No additional licenses required.
Back-end Avaya Aura® Experience Portal	N/A	No additional licenses required.	No additional licenses required.
SIP INFO message using Context Creation	N/A	No additional licenses required.	No additional licenses required.

! Important:

Avaya Aura® Contact Center Release 6.4 does not support SIP-enabled Avaya Communication Server 1000 for new installations. Existing Avaya Aura® Contact Center solutions using SIP-enabled Avaya Communication Server 1000 can be expanded or upgraded.

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

Transfer method	CS 1000 AML-based Contact Center	CS 1000 SIP-enabled 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 Intrinsic.	Maximum Call Attached Data is 4096 bytes. Maximum 5 ASCII key-value pairs of Contact Intrinsic.	Maximum Call Attached Data is 4096 bytes. Maximum 5 ASCII key-value pairs of Contact Intrinsic.
UUI SIP header using ASAI	N/A	96 bytes maximum.	96 bytes maximum.
P-Intrinsic SIP header	N/A	Depends on your solution. ^{Note 1}	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.	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-Intrinsic SIP header information:

- The amount of P-Intrinsic 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-Intrinsic.
- 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.
- If your solution has an Avaya Aura® Communication Manager in the call path, for improved P-Intrinsic support, Avaya recommends Communication Manager Release 6.0.1 SP8 or later.

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 4: Contact Center voice services product compatibility

Product name	Supported releases
Avaya IVR-CTI Integration server (MPS)	3.5
Avaya Agent Greeting	3.0X and later (for CS 1000 AML only.) (On SIP-enabled Contact Center, Agent Greeting is an integrated feature.)
Avaya Aura® Workforce Optimization (WFO)	11.0 and 12.0
Avaya Voice Portal	5.1 and later
Avaya Aura® Experience Portal	Release 6.0, 7.0, and 7.0.1
Avaya Proactive Outreach Manager (POM)	Release 3.0.1
Avaya CallPilot®	5.1 SU 01 or later
Avaya MPS 500	3.5 RB4, 3.5 RB5, and 4.1
IRA (formally MIRAN)	2.0, 3.0
Avaya MPS 1000	3.5 RB4, 3.5 RB5, and 4.1
Avaya Media Server (SIP-enabled contact center)	7.6
IP Media Services (IP RAN and music on CS 1000)	Avaya Media Server 7.0 or later
Remote Agent Observe	(Avaya Communication Server 1000 AML only)

Avaya CallPilot® and Avaya MPS are not supported in a SIP-enabled Contact Center. For the SIP-enabled Contact Center the Avaya Media Server component provides media services.

The following table lists other products supported with Contact Center Manager Server and Avaya Communication Server 1000.

Table 5: 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.

Unified Reporting and Performance management with Avaya IQ

Avaya IQ supports real-time and historical reports for both Avaya Aura® Contact Center and Avaya Aura® Call Center Elite resources. This includes reporting on multimedia contacts, such as email messages and scanned documents.

Avaya Performance Center (APC) real-time reports can integrate AACC agents and queues with Call Center Elite agents and queues. APC real-time reports also include the channel as an attribute of queues. The classic Avaya IQ real-time reports support AACC agents and queues as well, but the queue-based measure % in Service Level is not supported for multimedia channels such as email. AACC agents and Call Center Elite agents are treated as separate agent accounts in Avaya IQ and so they show up as separate agent identifiers in reports.

Contact Center Manager Server (CCMS) contains an additional Windows service used by Avaya IQ to support unified reporting. This additional CCMS Avaya Reporting Connector (ARConnector) service allows Avaya IQ to generate reports based on AACC events.

Extensive information collection and reporting capabilities ensure that Contact Center Key Performance Indicators (KPIs) are monitored and maintained across all Lines of Business (LOB), media types, and communication channels.

To generate reports on AACC, in Avaya IQ add a “Data Source Association” of type “AACC” for the CCMS server. If you are using the AACC High Availability feature, use the Managed IP address as the IP address of the “Data Source Association”. You can then use Avaya IQ to generate reports on the Avaya Aura® Contact Center multimedia Data Collection.

The CCMS ARConnector has some limitations in Avaya Aura® Contact Center High Availability solutions. When an AACC switchover occurs, Avaya IQ takes several minutes to reestablish a connection with the ARConnector on the new active server. This causes a gap in Avaya IQ reporting. The agent and skillset states are incorrect for 10 to 30 minutes following a switchover, after which time the states IQ and AACC automatically resynchronize.

Part 3: Licensing requirements

Chapter 22: 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 a 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 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.
- **Essential:** licensing for a single-server, single-site, voice-only contact center.

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, SIP-enabled, or multimedia-only), and on the ordering process you use.

License types

Contact Center License Manager supports the following license types:

- [Nodal Enterprise licensing](#) on page 257
- [Corporate Enterprise licensing](#) on page 257
- [Nodal NCC licensing](#) on page 258
- [Corporate NCC licensing](#) on page 258
- [Essential licensing](#) on page 259

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 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.

Essential licensing

Essential licensing supports entry-level, voice-only, single-site, single-server contact centers. All Essential licensing options are in a single license file managed by the co-resident License Manager.

Important:

Avaya Aura® Contact Center Release 6.4 does not support Essential licensing for new installations. Existing Avaya Aura® Contact Center solutions using Essential licensing can be expanded, upgraded, or migrated.

Avaya Aura® Contact Center supports upgrading from an entry-level, voice-only Essential license to a full-featured multimedia Enterprise license.

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 guest:** Contact Center License Manager supports only Avaya WebLM Virtualized Environment (VE) vAppliance, Release 6.3.2 or Release 6.3.8, as a remote WebLM server. You can download this vAppliance from Avaya PLDS. Install and commission a suitably licensed VE WebLM server in your solution. Contact Center License Manager obtains licenses from this remote WebLM server, and uses these licenses to control Avaya Aura® Contact Center licensed features. Avaya WebLM server does not support Corporate Licensing.

Avaya Aura® Contact Center deployments that use an Avaya WebLM server on a virtual guest do not support the Avaya Aura® Contact Center High Availability (HA) feature.
- **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 260
- [PLIC licensing mechanism](#) on page 261

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 Avaya Aura® Contact Center applications as required.

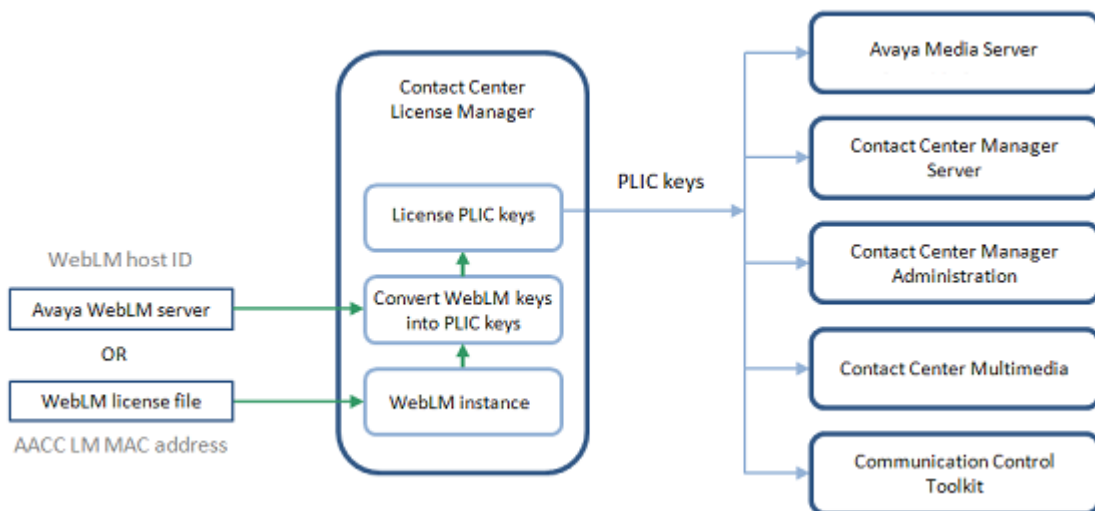
For deployments using an Avaya WebLM server, Contact Center License Manager supports only the Virtualized Environment deployment of Avaya WebLM server.

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 Media Server as a Media Server in Contact Center Manager Administration, Contact Center License Manager pushes the license keys to that Avaya Media Server. You must restart that Avaya Media Server so it can acquire these licenses. Do not configure WebLM licensing on Avaya Media Server servers.

Avaya Aura® Contact Center supports WebLM in nodal contact centers. WebLM does not support Avaya Aura® 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 Avaya Aura® Contact Center (AACC) applications.

Local WebLM license file:

You use the contact center server subnet NIC MAC address of the Contact Center License Manager server to obtain a SIP-enabled nodal license file from the Avaya Product Licensing and Delivery System (PLDS).

If the MAC address used in the license file does not match a MAC address from the Contact Center License Manager server, License Manager cannot start. WebLM uses an .xml file to store keys for licensed features.

Licenses on an Avaya WebLM server virtual guest:

If you use an Avaya WebLM Virtualized Environment (VE) vAppliance, Release 6.3.2 or Release 6.3.8, you must use the primary host ID of the Avaya WebLM server to obtain your Avaya Aura® Contact Center license.

You use the Avaya WebLM primary host ID to activate your Avaya Aura® 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 Avaya Aura® 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. Avaya Aura® Contact Center therefore supports only the PLDS standard license file (SLF) type. Avaya Aura® Contact Center does not support the WebLM Enterprise model.

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
- Remote 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 6: License file generation summary

Unique Number (license key)	Enterprise Nodal SIP	Enterprise Nodal AML	Enterprise Nodal MM-only	Corporate Enterprise	Essential Nodal SIP	Essential Nodal AML
LM server MAC address	Yes	Yes	Yes	Yes	Yes	Yes
WebLM host ID	Yes	No	Yes	No	Yes	No
CS 1000 Serial ID	No	Yes	No	No	No	Yes
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.

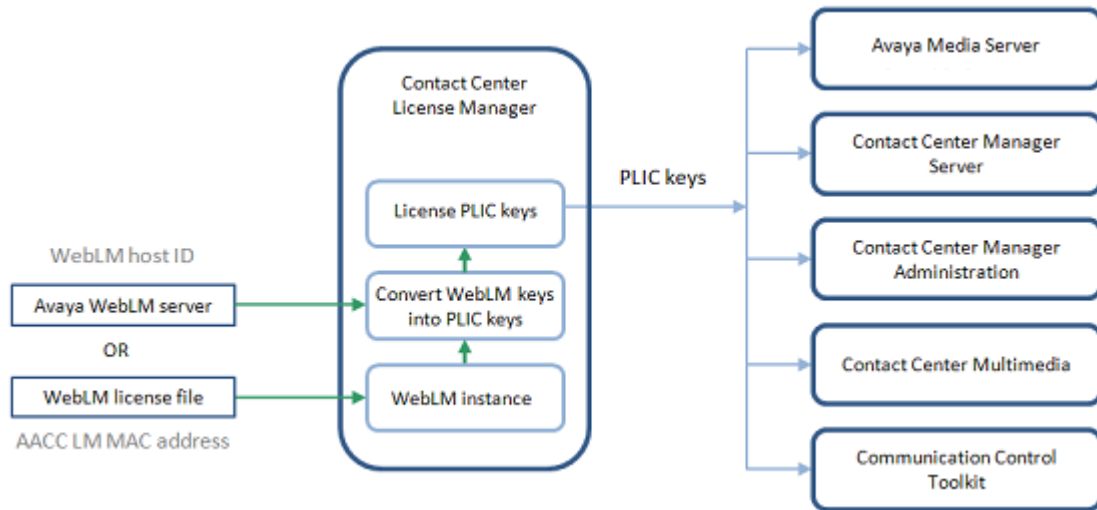
For more details about obtaining a license file, see the following:

- [How to obtain a license for a nodal SIP-enabled solution](#) on page 262
- [How to obtain a license for a nodal AML-based solution](#) on page 264
- [How to obtain a Corporate license](#) on page 265
- [How to obtain a license for a multimedia only solution](#) on page 266

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 a WebLM license file or a remote WebLM server to provide nodal licensing control.

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



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 WebLM license file from the Avaya Product Licensing and Delivery System (PLDS).
3. Load the 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 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 LM server MAC address, then License Manager provides license keys, and Avaya Aura® Contact Center processes customer contacts.

OR

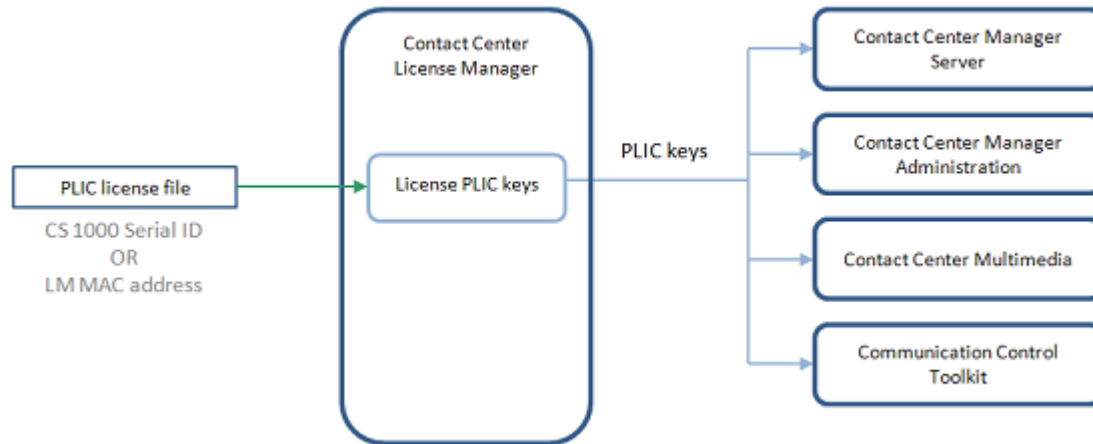
1. When using the Virtualized Environment deployment of Avaya WebLM server, obtain the Avaya WebLM host ID from the WebLM user interface.
2. Use the WebLM host ID to obtain WebLM license keys from the Avaya Product Licensing and Delivery System (PLDS).
3. Enter these license keys on the remote Avaya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

The following diagram shows 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.

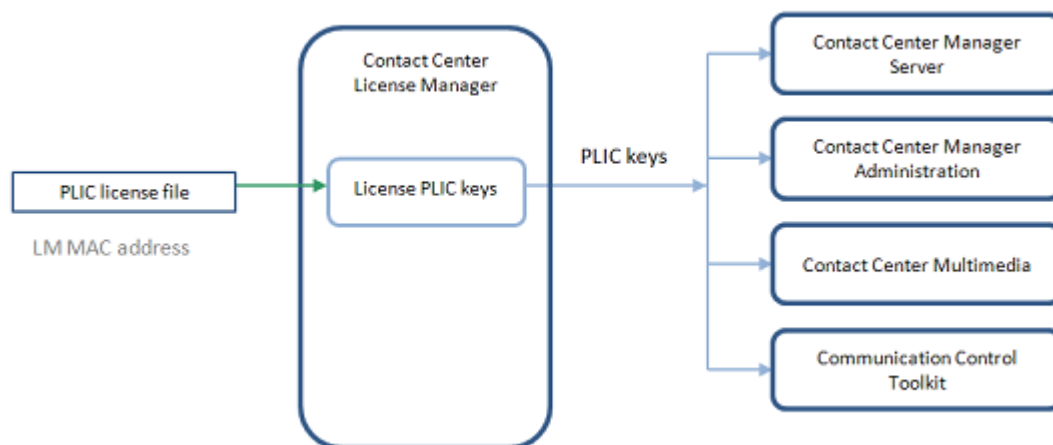
If you plan to use a Communication Control Toolkit Knowledge Worker Server, use the CS 1000 Serial ID or the MAC address of the Knowledge Worker server to obtain a license file. Contact Center License Manager is installed on every Communication Control Toolkit Knowledge Worker Server.

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.

The following diagram shows 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.

How to obtain a license for a multimedia only solution

The following Avaya Aura® Contact Center multimedia-only installation types support PLIC and WebLM licenses:

- AACC Multimedia Complement for Elite
- No Switch Configured Multimedia Only

These single-server solutions support a local PLIC license file or a local WebLM license file.

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 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 WebLM license file from the Avaya Product Licensing and Delivery System (PLDS).
3. Load the 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 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 LM 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
- Knowledge Worker server
- AACC Multimedia Complement for Elite
- No Switch Configured Multimedia Only

The following table shows where to install Contact Center License Manager for a given license type.

Table 7: Contact Center License Manager installation location

License type	Essential Nodal	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 — OR — Knowledge Worker server — OR — AACC Multimedia	Voice and Multimedia Contact Server — OR — Voice Contact Server — OR — Network Control Center Server	Voice and Multimedia Contact Server — OR — Voice Contact Server — OR — Knowledge Worker server	Voice and Multimedia Contact Server — OR — Voice Contact Server — OR — Network Control Center Server

License type	Essential Nodal	Enterprise Nodal	Enterprise Nodal Networked (Nodal NCC)	Corporate Enterprise	Corporate Enterprise Networked (Corporate NCC)
		Complement for Elite — OR — No Switch Configured Multimedia Only			

Avaya Media Server licensing considerations

Avaya Media Server requires licenses for the conference and (optionally) Agent Greeting features.

If you are using WebLM licensing, when you configure an Avaya Media Server as a Media Server in Contact Center Manager Administration, Contact Center License Manager pushes the license keys to that Avaya Media Server. You must restart Contact Center License Manager to push the licenses to Avaya Media Server. Do not configure WebLM licensing on Avaya Media Server servers.

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.

Avaya Media Server Zoning

Avaya Media Server (Avaya MS) Zoning allows contact center administrators to target a specific Avaya MS instance or prioritized list of instances when anchoring incoming contact center calls. The

administrator chooses the preferred Avaya 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

Offsite Agent is a solution that extends a Contact Center to an agent's preferred environment, allowing them to handle skillset calls regardless of location. Offsite Agent solutions connect contact center calls to the agent's telephone (home telephone or mobile), without the agent needing special hardware.

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 Aura® 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 Manager Administration – Client Administration* (44400-611).

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 *Avaya Aura® Contact Center Performance Management* (44400-710).

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.

Changes to Announcement and Dialog treatment licensing

In a SIP-enabled Contact Center, you must purchase the required number of ANNC and DIALOG licenses for your Contact Center implementation. Prior to Avaya Aura® Contact Center Service Pack 12 (SP12), Contact Center did not enforce the ANNC and DIALOG licenses. Avaya Aura® Contact Center now enforces these licenses.

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

KRS / PLIC license

- __sip-annc::sess
- __sip-dialog::sess

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

Table continues...

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 268.

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 to 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 8: 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_ESSENTIAL or 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	Maximum Contact Center Manager Network nodes	VALUE_CCTR_CCM_NET_NODE

Table continues...

PLIC license identifier	Description	WebLM license identifier
LM_IM_PRESENCE LM_CONTACTREC 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

Table continues...

PLIC license identifier	Description	WebLM license identifier
LM_OI LM_OIOpenQ LM_OIOpenN	SOA Development Kit	VALUE_CCTR_DEV_KIT
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 ag-recording::sess	Maximum Agent Greeting licenses	VALUE_CCTR_AGT_GREET
LM_OFF_SITE = 1	Maximum Offsite agent seats	VALUE_CCTR_OFFSITE_AGT
__sip-conf::sess	Maximum SIP ports. Consumed by Avaya Media Server.	For WebLM, Contact Center reads the number of licensed Avaya Media Server instances (VALUE_CCTR_AMS_INSTANCE) and automatically provides the SIP port licenses to the Avaya Media Server(s).
–	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
__sip-annc::sess	Maximum Announcement concurrent sessions.	VALUE_CCTR_ANNOUNCE_PORTS

Table continues...

PLIC license identifier	Description	WebLM license identifier
	Consumed by the Contact Center Task Flow Executor (TFE) component.	
__sip-dialog::sess	Maximum Dialog concurrent sessions. Consumed by the Contact Center Task Flow Executor (TFE) component.	VALUE_CCTR_DIALOG_PORTS
inst::auth	Maximum Avaya Media Server Instances. ID and value pushed to Avaya Media Server.	VALUE_CCTR_AMS_INSTANCE
ccoas::sess	Maximum Offsite Agent. ID and value pushed to Avaya Media Server.	VALUE_CCTR_AAOA
LM_CONTACTREC	Contact Recording. ID and value pushed to Avaya Media Server.	VALUE_CCTR_CONTACTREC
srtp::auth	TLS SRTP Signaling and Media Encryption. ID and value pushed to Avaya Media Server.	FEAT_CCTR_TLS_SRTP
LM_AMSZ	Avaya Media Server Zoning. ID and value pushed to Avaya Media Server.	FEAT_CCTR_AMS_ZONING

Licensing requirements for Agent Desktop features

Avaya Aura® 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 Aura® 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. — 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 Call Center Elite (My Computer mode)	—	—	—	Yes	Provision an Agent_SC license on Avaya Aura® Communication Manager for each phone used by Elite. See Note 1.
Handle voice contacts using softphone (My Computer mode)	—	—	—	No	Provision an IP_Agent license on Avaya Aura® Communication Manager for each

Table continues...

Agent Desktop feature	AACC license	License key	Type	CCMM	Note
					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.
Handle voice contacts in Offsite Agent mode. (Other Phone mode.) Supported in Avaya Communication Server 1000 AML-based solutions. This solution type requires a standalone Offsite Agent server.	Maximum Offsite agent	AACC LM consumes LM_OFF_SITE.	Site	No (Yes for NRRC support.)	Each LM_OFF_SITE increment consumes two Offsite Agent session licenses (ccoas::sess). To support Not Ready Reason Codes (NRRC), each agent must also have one (any) multimedia contact license.
	ccoas::sess	The standalone Offsite Agent server consumes ccoas::sess licenses from the local license file.	Seat		
Log on to MS Lync	—	—	—	Yes	Required for peer-to-peer Instant Messaging or for Instant Messaging (IM) contacts.
Log on to MS Office Communications Server	—	—	—	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.

Table continues...

Agent Desktop feature	AACC license	License key	Type	CCMM	Note
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	
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	
Predictive Outbound contacts (POM/ SER)	Maximum Predictive Outbound agents	LM_LOC_PRAN	Seat	Yes	

Table continues...

Agent Desktop feature	AACC license	License key	Type	CCMM	Note
Support Agent Greeting	Maximum Agent Greeting licenses	LM_LOC_GREN ag-recording::sess	Seat	No	
Support third call appearance button (Third Line Appearance) for voice	N/A	N/A	—	No	No additional AACC license requirement. Supported only when using Communication Manager Release 6.3.
Support voice call join	N/A	N/A	—	No	No additional AACC license requirement. Supported only when using Communication Manager Release 6.3.
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

Table continues...

Agent Desktop feature	AACC license	License key	Type	CCMM	Note
					(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 LM_LOC_WCAN or LM_LOC_IMAN	Seat	Yes	
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

Table continues...

Agent Desktop feature	AACC license	License key	Type	CCMM	Note
					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 466. - 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.

The Avaya Aura® Agent Desktop Call Center Elite voice integration does not support supervisor functions.

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.

! Important:

Avaya Media Server does not support grace period. In a SIP-enabled Contact Center using PLIC licensing, where Avaya Media Server is co-resident with Contact Center Manager Server, Avaya Media Server stops if Contact Center Manager Server goes into grace period. If Avaya Media Server is standalone, or if Contact Center uses WebLM licensing, Avaya Media Server maintains normal operation.

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.

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.

Supported License Manager servers

This section describes some of the licensed features in Contact Center. You cannot use Avaya NES License Manager Release 7.0 with Avaya Aura® Contact Center (AACC).

The following table shows the supported Contact Center License Manager servers.

Table 9: Contact Center License Manager servers

Compatible with	NES CC 6.0 Licenses	NES CC 7.0 Licenses	AACC Licenses
NES CC 6.0	Yes	Yes	Yes
NES CC 7.0	No	Yes	Yes
AACC 6.X	No	No	Yes

Part 4: Performance specifications

Chapter 23: Maximum capacities

This section specifies the overall maximum capacities for Avaya Aura® Contact Center Release 6.4.

Maximum capacity overview

The following table specifies the maximum overall capacity values supported by Avaya Aura® Contact Center.

Table 10: Overview of maximum Avaya Aura® Contact Center capacity figures

Switch Type	Number of active agents	Calls per hour
Avaya Aura® 6.1, 6.2, or 6.3 - SIP	3000	45 000
Avaya Aura® Contact Center Hardware Appliance	400	6000
Avaya Aura® Contact Center 3x OVA Deployment	400	6000
Avaya Communication Server 1000 - AML	5000	100 000
Avaya Communication Server 1000 - SIP	1500	30 000
Avaya Aura® Midsize Business Template 5.2.1 - SIP	300	6000
Avaya Aura® 5.2 - SIP	1000	15 000
Avaya Aura® Solution for Midsize Enterprise 6.1 or 6.2 - SIP	600	10 000
No Switch - Multimedia only	3000	12 000
Multimedia Complement to Avaya Aura® Call Center Elite	3000	12 000

The following conditions apply to the table:

- The capacities supported on a server are limited by the server platform. Use the guidelines in [Server Specifications](#) on page 305 to determine the capacity of your server.
- 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.

! Important:

Avaya Aura® Contact Center Release 6.4 does not support the Avaya Aura® Midsize Business Template (MBT) or Avaya Aura® Unified Communications Release 5.2 platforms for new

installations. Existing Avaya Aura® Contact Center solutions using MBT or Avaya Aura® 5.2 can be expanded or upgraded.

! Important:

Avaya Aura® Contact Center Release 6.4 does not support SIP-enabled Avaya Communication Server 1000 for new installations. Existing SIP-enabled Avaya Communication Server 1000 contact center installations can be expanded or upgraded.

For the complete list of capacity limits, see [Maximum agent capacity and call rate values](#) on page 288.

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 guidelines in [Server Specifications](#) on page 305 to determine the capacity of your server.
- 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.
- Avaya Aura® Contact Center Release 6.4 does not support the Avaya Aura® Midsize Business Template (MBT) or Avaya Aura® Unified Communications Release 5.2 platforms for new installations. Existing Avaya Aura® Contact Center solutions using MBT or Avaya Aura® 5.2 can be expanded or upgraded.
- Avaya Aura® Contact Center Release 6.4 does not support SIP-enabled Avaya Communication Server 1000 for new installations. Existing SIP-enabled Avaya Communication Server 1000 contact center installations can be expanded or upgraded.

Table 11: Contact Center capacity figures in detail

Parameter	SIP maximum	AML maximum
General parameters		
Number of logged-on agents: Configurations with greater than 1500 agents require special consideration for contact center subnet bandwidth and disk requirements. The maximum of 5000 logged on agents is only applicable for the Avaya Communication Server 1000 Release 7.0, 7.5, or 7.6.	• Avaya Aura® 6.1, 6.2, or 6.3 Unified Communications platform based SIP: 3,000 • Avaya Aura® Solution for Midsize Enterprise based SIP: 600 • Avaya Aura® 5.2 Unified Communications platform based SIP: 1,000	5,000

Table continues...

Parameter	SIP maximum	AML maximum
	• Avaya Aura® Midsize Business Template based SIP: 300 • Avaya Communication Server 1000 based SIP: 1,500	
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 • AACC Multimedia Complement for Elite: 3,000 • Avaya Aura® Solution for Midsize Enterprise based SIP: 600 • Avaya Aura® Midsize Business Template based SIP: 300 • Avaya Communication Server 1000 based SIP: 1,500	3,000
Number of agents defined in the system	10,000	10,000
Number of phones: Communication Server 1000	10,000	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 The product contains three predefined scripts. Therefore, you can create 997 scripts.	1,000 (997)	1,000 (997)
Maximum script size—Master_Script (characters)	100,000	100,000

Table continues...

Maximum capacities

Parameter	SIP maximum	AML maximum
Maximum script size—other scripts (characters)	50,000	50,000
Number of applications (that is, exit points from the Master_Script) The product contains five predefined applications. Therefore, you can create 800 applications for Release 6.0 or 1000 applications for the current release.	805 (800)	1,005 (1,000)
Number of user defined call variables	500	500
Maximum number of supported SIP Contact Intrinsic per contact	32 key-value pairs. Each key-value pair has a maximum <i>key</i> length of 25 characters and a maximum <i>value</i> 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.	1,500	1,500
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 9995 activity codes.	10,000 (9,995)	10,000 (9,995)
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 Communication Server 1000 based SIP: 30,000 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.
Co-resident Multimedia server new contacts backlog	4,000	4,000
Number of waiting contacts	3,000	3,000

Table continues...

Parameter	SIP maximum	AML maximum
Call resources parameters		
Number of IVR queues (Communication Server 1000)	150	150
Number of IVR ports	1,000	1,000
Number of ACCESS ports (Communication Server 1000)	NA	191
Number of routes	513	513
Avaya only tested 1000 trunk members. Avaya has no plans to test the 4400-trunk limit. Number of trunks (Communication Server 1000)	4,400	4,400
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 Routed IM and integration with Avaya Presence Services or Microsoft OCS/Lync.	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

Table continues...

Parameter	SIP maximum	AML maximum
Number of presence changes per hour	200,000	N/A
Assignment parameters		
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 1000).	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.	1,000	1,000

Table continues...

Parameter	SIP maximum	AML maximum
Networking parameters		
Number of call processing nodes in the network (including local node) The number of configured nodes is 30; however, only 20 nodes can be configured in the routing table.	30	30
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	1,000,000	1,000,000

Table continues...

Parameter	SIP maximum	AML maximum
contacts to the Multimedia Offline database. For more information about the Multimedia Archive Utility, see <i>Avaya Aura® Contact Center Routine Maintenance</i> (44400-514).		
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 299.	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 299.
Third-party interface parameters		
Number of MLS applications	Not applicable	16
Number of MLS DN registrations across all MLS applications	Not applicable	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.	Not applicable	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%

Table continues...

Parameter	SIP maximum	AML maximum
Number of CCMS servers per Avaya Communication Server 1000	3 (Only to support phased migration between Contact Center releases)	3
Number of AML-based application servers per Communication Server 1000	Not applicable	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 Aura® Agent Desktop	10,000	10,000

Orchestration Designer application Variables and Intrinsic

Avaya Aura® Contact Center Orchestration Designer (OD) applications support the following variables and intrinsic 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 variables have a value that can change for each contact. These variables follow the contact through the system and pass from one OD	Yes	Yes	OD applications have read	500

Table continues...

Type	Description	AML	SIP	Access	Maximum
call variable	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.			and write access to call variables.	
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 12: 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

Table continues...

Parameter	Maximum
Email servers	
Maximum number of SMS mailboxes which can be configured	50
Maximum number of Scanned Document mailboxes which can be configured	50
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
Maximum number of addresses per Sender Group	50
Keyword Groups	
Maximum number of Keyword Groups	3000
Maximum number of Keywords per Keyword Group	50
Barred Outgoing Addresses	50

Contact Center 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 the Avaya Communication Server 1000 and SIP.

Table 13: Call service and cost per call

	Avaya Communication Server 1000 - AML	SIP
Parameter	Services for each call	Services for each call
Basic Call	1	1
Queue to Skillset	2	2
Queue to Agent	0	0
Give Controlled Broadcast (S/S)	1	N/A (see Notes)
Voice Services Collect Digits	0	0
Give IVR	1	2
Give RAN	2	2
Give Music	1	1
HDX Send Info	1	1
Voice Services Collect Digits	0	0
Give IVR	1	2
Give RAN	2	2
Give Music	1	1
HDX Send Info	1	1
HDX Request/Response	1	1
Intrinsics	5	6
If/Then's Executed	5	5
Proportion of Calls Transferred	5%	5%

Table continues...

	Avaya Communication Server 1000 - AML	SIP
Proportion of Calls Conferenced	5%	5%
Proportion of Calls Transferred to a DN	N/A	N/A
MLS Screen Pops	1.2	N/A
MLS Messages	0	N/A
Queue to Network Skillset	2	N/A (see Notes)

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).
- Give Controlled Broadcast (S/S) and Queue to Network Skillset for SIP are not supported in this release.

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 union 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.
- `Avaya\Contact Center\Journal` folder is created during installation. This folder contains the Database Journal Files, which are used for Geographic Redundancy.
- `Avaya\Contact Center\ShadowJournals` folder is created during installation. This folder is used if Geographic Redundancy is configured and this server is running as the Redundant server.

During the installation you can select the drive letter that these folders or files are 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:

$$= 9\,000 * 0.3 * 0.5 * 10 * 2$$

$$= 27\,000 \text{ MB}$$

Communication Control Toolkit capacity

The call capacity is 100 000 simple calls per hour (CPH) with data for a maximum of 5000 agents.

CCT-IVR is an optional component that supports an additional 16 000 CPH running on the IVR lines.

Communication Control Toolkit is supported only on Windows Server 2008. CCT-IVR is supported only on Windows Server 2003. They are therefore not supported co-resident.

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 a standalone Communication Control Toolkit server 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 (Communication Control Toolkit, CCT-IVR, or both)
 - A solution running both Communication Control Toolkit and CCT-IVR requires more system resources than a system running only Communication Control Toolkit or CCT-IVR. Communication Control Toolkit is supported only on Windows Server 2008. CCT-IVR is supported only on Windows Server 2003. They are therefore not supported co-resident.

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.

Configure at least one Landing Pad per simultaneous call.

If the peak call rate increases above the rate configured for, 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 24: Server Specifications

This section describes sample Avaya Aura® Contact Center solutions and the 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 with 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 and server specification](#) on page 308
- [Mid-range solution and server specification](#) on page 311
- [High-end solution and server specification](#) on page 317

The Entry-level, Mid-range, and High-end servers can be physical servers or, where supported, virtualized guest machines.

The Entry-level server is not supported for new installations. Existing installations are supported on existing platforms.

Avaya recommends using the High-end server specification for all new installations.

For information about achieving the maximum performance from your server hardware, see [Server performance and BIOS settings](#) on page 326.

Avaya Aura® Contact Center is also offered as a Hardware Appliance. The Hardware Appliance includes Avaya Aura® Contact Center software installed and partially pre-configured on a supplied rack-mount server. The Avaya Aura® Contact Center Hardware Appliance does not support Platform Vendor Independence (PVI). For more information about the Hardware Appliance server specification, see [Hardware Appliance server specification](#) on page 332.

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 VMware guest (virtual machine).

Table 14: Supported server specifications for each server type

Server type	Voice PABX	Non-Virtualized Deployments					Virtualized Deployments				
		Entry-level single 4 core	Mid-range dual 4 core	High-end dual 6 core	High-end dual 8 core	High-end dual 10 core	Entry-level single 4 core	Mid-range dual 4 Core	High-end dual 6 core	High-end dual 8 core	High-end dual 10 core
		8–logical CPU	16–logical CPU	24–logical CPU	32–logical CPU	40–logical CPU	8–vCPU	16–vCPU	24–vCPU	32–vCPU	40–vCPU
Voice and Multimedia Contact Server with Avaya Media Server	Aura SIP	No	Yes	Yes	Yes	Yes	No	No	No	No	No
Voice and Multimedia Contact Server without Avaya Media Server	Aura SIP	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
	CS 1000 AML	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
Voice Contact Server Only	Aura SIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	CS 1000 AML	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia Contact Server Only	Aura SIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	CS 1000 AML	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia Complement for Elite	Avaya Aura® Call Center Elite	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Voice and Multimedia Contact Server with Avaya	No Switch Configured	No	Yes	Yes	Yes	Yes	No	No	No	No	No

Table continues...

Server type	Voice PABX	Non-Virtualized Deployments					Virtualized Deployments				
		Entry-level single 4 core	Mid-range dual 4 core	High-end dual 6 core	High-end dual 8 core	High-end dual 10 core	Entry-level single 4 core	Mid-range dual 4 Core	High-end dual 6 core	High-end dual 8 core	High-end dual 10 core
		8–logical CPU	16–logical CPU	24–logical CPU	32–logical CPU	40–logical CPU	8–vCPU	16–vCPU	24–vCPU	32–vCPU	40–vCPU
Media Server											
Network Control Center Server	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Knowledge Worker Server Only	CS 1000 AML	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Avaya Media Server standalone on Linux	Aura SIP	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Avaya Aura® Contact Center 3x OVA deployment	Aura SIP	No	No	No	No	No	No	No	No	Yes	Yes
AACC-M	Aura SIP	No	No	No	No	No	No	No	Yes	Yes	Yes

For more information about server specifications, see the following sections.

*** Note:**

The VMware hypervisor requires one virtual CPU (vCPU). For VMware deployments, the maximum number of vCPUs provisioned across all guests on a VMware host must amount to one less vCPU than the number of physical cores in the host server. The total maximum number of vCPUs = (host total physical cores - 1).

Entry-level solution and server specification

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 Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
	CS 1000 AML	Not Supported	Not Supported	N/A	N/A
	CS 1000 SIP	Not Supported	Not Supported	N/A	N/A
Voice and Multimedia Contact Server with Avaya Media Server	Aura SIP	Not Supported	Not Supported	N/A	N/A
	CS 1000 AML	Not Supported	Not Supported	N/A	N/A
	CS 1000 SIP	Not Supported	Not Supported	N/A	N/A
Voice Contact Server Only	Aura SIP	300	100	6K	500 / 800
	CS 1000 AML	300	100	6K	500 / 800
	CS 1000 SIP	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
	CS 1000 SIP	800	N/A	N/A	2.0K / 4.0K
Knowledge Worker Server	CS 1000 AML	1000	N/A	50K	N/A
Multimedia Complement for Elite	Elite	Not Supported	Not Supported	N/A	N/A
Voice and Multimedia Contact Server with Avaya Media Server	No Switch Configured	Not Supported	Not Supported	N/A	N/A
Network Control Center Server	All switch types	Supported	400	N/A	N/A
CCMS standalone (Not for new installs)	Aura SIP	800	N/A	10K	2.0K / 4.0K
	CS 1000 AML	1000	N/A	20K	2.0K / 4.0K
	CS 1000 SIP	800	N/A	8K	2.0K / 4.0K
CCMA standalone (Not for new installs)	Aura SIP	800	400	10K	2.0K / 4.0K
	CS 1000 AML	1000	400	20K	2.0K / 4.0K
	CS 1000 SIP	800	400	8K	2.0K / 4.0K

Table continues...

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}
CCT standalone (Not for new installs)	Aura SIP	800	N/A	10K	2.0K / 4.0K
	CS 1000 AML	1000	N/A	50K	2.0K / 4.0K
	CS 1000 SIP	800	N/A	8K	2.0K / 4.0K
Avaya Media Server standalone	Linux	Not Supported	Not Supported	N/A	N/A
	MS Windows	Not Supported	Not Supported	N/A	N/A
Avaya Aura® Contact Center 3x OVA deployment	Aura SIP	Not Supported	Not Supported	N/A	N/A
AACC-M	Aura SIP	Not Supported	Not Supported	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, Web chat contacts have a weighting equivalent to two email messages. One Web chat is equivalent to two email messages.
- For System Contact Rate calculations, IM contacts have a weighting equivalent to voice contacts. One IM contact is equivalent to one voice contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + (Web Chat * 2))

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). Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes.

Note: For VMware deployments, the maximum number of vCPUs provisioned across all guests on a VMware host must amount to one less vCPU than the number of physical cores in the host server. The total maximum number of vCPUs = (host total physical cores - 1). The VMware hypervisor requires one vCPU.

Note: For virtualized servers, decrease the Avaya Aura® Contact Center agent count and call rate by 15%. Alternately, increase the CPU benchmark rating by 15% for Avaya Aura® Contact Center.

Note: The Aura SIP agent count and call rate limits apply to Avaya Aura® Communication Manager Release 6.0.1 or later configurations.

Note: Avaya Media Server is not supported on an entry-level server.

Note: Avaya Aura® Contact Center High Availability is not supported on an entry-level server.

Note: To achieve the stated capacities, configure your server hardware for maximum performance. For more information, see [Server performance and BIOS settings](#) on page 326.

Note: Avaya Call Recording (ACR) is not supported on an entry-level server.

Note: Avaya Aura® Contact Center Release 6.4 does not support standalone CCMS, standalone CCT, or standalone CCMA for new installations. Existing Avaya Aura® Contact Center solutions using standalone servers can be expanded or upgraded.

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 single 4–core 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 6.4 for the entry-level server in order to support the rated capacities.

The entry-level server is not supported for new installations. Existing installations are supported on existing platforms.

Specification	Configuration	Comment
CPU	Quad Core Xeon E5640 2.67GHz	You must select a CPU that exceeds the benchmark rating for the Quad Core E5640 2.67 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 • For virtualized servers, decrease the Avaya Aura® Contact Center agent count and call rate by 15%. Alternately, increase the CPU benchmark rating by 15% for Avaya Aura® Contact Center. • AMD processors of a higher specification are also supported. The AMD CPU benchmark score must be at least 10 percent greater than the Intel E5640 benchmark score. • Non supported processors include: Intel Celeron and Intel Itanium (IA 64).  Note: CPUs based on more than ten cores are not supported.
RAM	12 GB	
Disk Type and Speed	SCSI, SATA, SAS, Minimum 7200 RPM	• For 3.5 inch disks the minimum disk speed is 7200 RPM. • For 2.5 inch disks the minimum disk speed is 10000 RPM. • For more than 300 agents, the minimum disk speed is 10000 RPM. • IDE drives are not supported. • Solid State Drives (SSDs) are not supported.
C: (partition)	80 GB NTFS	Minimum OS partition size
D: (partition)	80 GB NTFS	Application partition
DVD Drive	One dual-layer DVD drive	Minimum speed is 4X.
CCMS Database partition	200 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server

Table continues...

Specification	Configuration	Comment
		• Voice Contact Server • Multimedia Complement for Elite • No Switch Configured Multimedia only • Network Control Center Server
CCMM Database partition	300 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server • Multimedia Contact Server
CCT Database partition	10 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server • Voice Contact Server • CCT Knowledge Worker Server
Total Disk size	670 GB	Avaya recommends using battery backed hardware RAID 1 with identical drives.
Network Interface	Dual NIC 100 Mbit/s or faster	Only Ethernet supported.

*** Note:**

For information about achieving the maximum performance from your server hardware, see [Server performance and BIOS settings](#) on page 326.

For servers operating at 40% 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 and server specification

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 Media Server	Aura SIP	300	60	6K	0.8K / 1.2K
	CS 1000 AML	500	100	10K	0.8K / 1.2K
	CS 1000 SIP	300	60	6K	0.8K / 1.2K
Voice and Multimedia Contact Server with Avaya Media Server	Aura SIP	150	30	3K	300 / 600
	Aura SIP	200	40	2K	300 / 600
	CS 1000 SIP	200	40	2K	300 / 600
Voice Contact Server Only	Aura SIP	1500	300	30K	4.0K / 8.0K
	CS 1000 AML	3000	400	60K	4.0K / 8.0K
	CS 1000 SIP	750	200	15K	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
	CS 1000 SIP	1000	N/A	N/A	4.0K / 8.0K
Knowledge Worker Server	CS 1000 AML	5000	N/A	100K	N/A
Multimedia Complement for Elite	Elite	2000	300	N/A	4.0K / 8.0K
Voice and Multimedia Contact Server with Avaya Media Server	No Switch Configured	1000	300	N/A	0.8K / 1.2K
Network Control Center Server	All switch types	Supported	600	N/A	N/A
CCMS standalone (Not for new installs)	Aura SIP	1500	N/A	20K	4.0K / 8.0K
	CS 1000 AML	5000	N/A	100K	6.0K / 12K
	CS 1000 SIP	1000	N/A	15K	4.0K / 8.0K
CCMA standalone (Not for new installs)	Aura SIP	1500	600	20K	4.0K / 8.0K
	CS 1000 AML	5000	600	100K	6.0K / 12K
	CS 1000 SIP	1000	600	15K	4.0K / 8.0K
CCT standalone (Not for new installs)	Aura SIP	1500	N/A	20K	4.0K / 8.0K
	CS 1000 AML	5000	N/A	100K	6.0K / 12K
	CS 1000 SIP	1000	N/A	15K	4.0K / 8.0K

Table continues...

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}
Avaya Media Server standalone	Linux	700	N/A	—	N/A
	MS Windows	490	N/A	—	N/A
Avaya Aura® Contact Center 3x OVA deployment	Aura SIP	Not supported	Not supported	N/A	N/A
AACC-M	Aura SIP	Not supported	Not supported	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, Web chat contacts have a weighting equivalent to two email messages. One Web chat is equivalent to two email messages.
- For System Contact Rate calculations, IM contacts have a weighting equivalent to voice contacts. One IM contact is equivalent to one voice contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + (Web chat * 2)).

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). Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes.

Note: For VMware deployments, the maximum number of vCPUs provisioned across all guests on a VMware host must amount to one less vCPU than the number of physical cores in the host server. The total maximum number of vCPUs = (host total physical cores - 1). The VMware hypervisor requires one vCPU.

Note: For virtualized servers, decrease the Avaya Aura® Contact Center agent count and call rate by 15%. Alternately, increase the CPU benchmark rating by 15% for Avaya Aura® Contact Center.

Note: The Aura SIP agent count and call rate limits apply to Avaya Aura® Communication Manager Release 6.0.1 or later configurations.

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, except for Avaya Media Servers. The servers in Avaya Media Server HA pairs must meet the high-end server specification.

Note: To achieve the stated capacities, configure your server hardware for maximum performance. For more information, see [Server performance and BIOS settings](#) on page 326.

Note: Avaya Aura® Contact Center Release 6.4 does not support standalone CCMS, standalone CCT, or standalone CCMA for new installations. Existing Avaya Aura® Contact Center solutions using standalone servers can be expanded or upgraded.

Note: Avaya Aura® Contact Center Release 6.4 does not support standalone Avaya Media Server on Windows. Existing Avaya Aura® Contact Center solutions using standalone Avaya Media Server on Windows can be expanded or upgraded.

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 Call Recording

The following tables lists the maximum number of Avaya Media Server agent sessions supported by the mid-range server.

Operating System	No Avaya Call Recording (ACR) and Avaya Media Server installed on physical mid-range server	No Avaya Call Recording (ACR) and Avaya Media Server installed on mid-range virtualized guest	Avaya Call Recording (ACR) enabled and Avaya Media Server installed on physical mid-range server	Avaya Call Recording (ACR) enabled and Avaya Media Server installed on mid-range virtualized guest
Linux	700 maximum agent sessions	Not supported	455 maximum agent sessions	Not supported
Windows	490 maximum agent sessions	Not supported	319 maximum agent sessions	Not supported

To support more agent sessions, add additional Avaya Media Server servers to your solution, or refer to the high-end server specifications.

Mid-range dual 4–core 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 6.4 for the mid-range server in order to support the rated capacities for the mid-range server type

Specification	Configuration	Comment
CPU	Dual Quad Core Xeon X5667 3.07 GHz	You must select a CPU that exceeds the benchmark rating for the Dual Quad Core Xeon X5667 3.07 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 - For virtualized servers, decrease the Avaya Aura® Contact Center agent count and call rate by 15%. Alternately, increase the CPU benchmark rating by 15% for Avaya Aura® Contact Center. - Avaya Media Server is supported only on Intel Xeon Dual Quad core, Dual 6–core, 8–core, or 10–core CPUs. Avaya Media Server does not support AMD processors. - Avaya Aura® Contact Center supports AMD processors of a higher specification. The AMD CPU benchmark score must be at least 10 percent greater than the Intel X5667 benchmark score. Avaya Media Server does not support AMD processors.

Table continues...

Specification	Configuration	Comment
		Non supported processors include: Intel Celeron and Intel Itanium (IA 64).  Note: CPUs based on more than ten cores are not supported.
RAM	12 GB	16 GB RAM required for High Availability and or virtualized environments.
Disk Type and Speed	SCSI, SATA, SAS, Minimum 7200 RPM	- For 3.5 inch disks, the minimum disk speed is 7200 RPM. - For 2.5 inch disks, the minimum disk speed is 10000 RPM. - For more than 500 agents, the minimum disk speed is 10000 RPM. - For Avaya Media Server, the minimum disk speed is 15000 RPM. - IDE drives are not supported. - Solid State Drives (SSDs) are not supported.
C: (partition)	80 GB NTFS	Minimum OS partition size. When installing Avaya Media Server software on a Linux server, Avaya Media Server requires a single flat hard disk partition with a minimum of 80 GB.
D: (partition)	80 GB NTFS	Application partition
DVD Drive	One dual-layer DVD drive	Minimum speed is 4X.
CCMS Database partition	200 GB NTFS	Required for the following server types: - Voice and Multimedia Contact Server - Voice Contact Server - Multimedia Complement for Elite - No Switch Configured Multimedia only - Network Control Center Server
CCMM Database partition	300 GB NTFS	Required for the following server types: - Voice and Multimedia Contact Server - Multimedia Contact Server - Multimedia Complement for Elite - No Switch Configured Multimedia only

Table continues...

Specification	Configuration	Comment
CCT Database partition	10 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server • Voice Contact Server • Multimedia Complement for Elite • No Switch Configured Multimedia only • CCT Knowledge Worker Server
Total Disk size	670 GB	• Duplicate drives with identical specifications required. Battery backed hardware RAID controller required for High Availability configurations. • In solutions using Avaya Aura® Contact Center High Availability, the database partitions on the active, standby, and optional Remote Geographic Node servers must be identical.
Network Interface	Dual NIC 1 Gbit/s	• Only Ethernet is supported. • Quad NICs are required for virtualized environments where this server is a VMware ESXi host. • Avaya Media Server configurations require a NIC that supports Receiver Side Scaling (RSS) with a minimum of 4 queues.

*** Note:**

For information about achieving the maximum performance from your server hardware, see [Server performance and BIOS settings](#) on page 326.

For servers operating at 40% 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 and server 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 Media Server	Aura SIP	600	100	12K	1.2K / 2.4K
	CS 1000 AML	1000	200	20K	1.2K / 2.4K
	CS 1000 SIP	600	100	12K	1.2K / 2.4K
Voice and Multimedia Contact Server with Avaya Media Server	Aura SIP	300	50	6K	600 / 1200
	Aura SIP	400	80	4K	600 / 1200
	CS 1000 SIP	400	80	4K	600 / 1200
Voice Contact Server Only	Aura SIP	3000	600	45K	6.0K / 12K
	CS 1000 AML	5000	600	100K	6.0K / 12K
	CS 1000 SIP	1500	300	30K	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
	CS 1000 SIP	1500	N/A	N/A	6.0K / 12K
Knowledge Worker Server	CS 1000 AML	5000	N/A	100K	N/A
Multimedia Complement for Elite	Elite	3000	600	N/A	6.0K / 12K
Voice and Multimedia Contact Server with Avaya Media Server	No Switch Configured	3000	600	N/A	6.0K / 12K
Network Control Center Server	All switch types	Supported	600	N/A	N/A
CCMS standalone (Not for new installs)	Aura SIP	3000	N/A	45K	6.0K / 12K
	CS 1000 AML	5000	N/A	100K	6.0K / 12K
	CS 1000 SIP	1500	N/A	30K	6.0K / 12K
CCMA standalone (Not for new installs)	Aura SIP	3000	600	45K	6.0K / 12K
	CS 1000 AML	5000	600	100K	6.0K / 12K
	CS 1000 SIP	1500	600	30K	6.0K / 12K
CCT standalone (Not for new installs)	Aura SIP	3000	N/A	45K	6.0K / 12K
	CS 1000 AML	5000	N/A	100K	6.0K / 12K

Table continues...

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
	CS 1000 SIP	1500	N/A	30K	6.0K / 12K
Avaya Media Server standalone	Linux	1000	N/A	—	N/A
	MS Windows	700	N/A	—	N/A
Avaya Aura® Contact Center 3x OVA deployment. Note 3	Aura SIP	400	80	6K	600 / 1200
AACC-M Note 4	Aura SIP	400	80	6K	600 / 1200

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

- For System Contact Rate calculations, Web chat contacts have a weighting equivalent to two email messages. One Web chat is equivalent to two email messages.
- For System Contact Rate calculations, IM contacts have a weighting equivalent to voice contacts. One IM contact is equivalent to one voice contact, up to the 10,000 IM per hour limit.
- For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + IM + Email + (Web chat * 2))

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). Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes.

Note 3: The Avaya Aura® Contact Center three OVA deployment (Avaya Aura® Contact Center OVA, Avaya Media Server OVA, and WebLM OVA) is supported only on the 8-core and 10-core high-end servers.

Note 4: AACC-M refers to a solution where Avaya Media Server and Avaya Aura® Contact Center are virtualized on one VMware host. For more information, see [Avaya Media Server and Contact Center on one VMware host](#) on page 330.

Note: For VMware deployments, the maximum number of vCPUs provisioned across all guests on a VMware host must amount to one less vCPU than the number of physical cores in the host server. The total maximum number of vCPUs = (host total physical cores - 1). The VMware hypervisor requires one vCPU.

Note: For virtualized servers, decrease the Avaya Aura® Contact Center agent count and call rate by 15%. Alternately, increase the CPU benchmark rating by 15% for Avaya Aura® Contact Center.

Note: The Aura SIP agent count and call rate limits apply to Avaya Aura® Communication Manager Release 6.0.1 or later configurations

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 server hardware for maximum performance. For more information, see [Server performance and BIOS settings](#) on page 326.

Table continues...

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 Release 6.4 does not support standalone CCMS, standalone CCT, or standalone CCMA for new installations. Existing Avaya Aura® Contact Center solutions using standalone servers can be expanded or upgraded. Note: Avaya Aura® Contact Center Release 6.4 does not support standalone Avaya Media Server on Windows. Existing Avaya Aura® Contact Center solutions using standalone Avaya Media Server on Windows can be expanded or upgraded. 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 Call Recording

The following tables lists the maximum number of Avaya Media Server agent sessions supported by the high-end server.

Operating System	No Avaya Call Recording (ACR) and Avaya Media Server installed on physical mid-range server	No Avaya Call Recording (ACR) and Avaya Media Server installed on mid-range virtualized guest	Avaya Call Recording (ACR) enabled and Avaya Media Server installed on physical mid-range server	Avaya Call Recording (ACR) enabled and Avaya Media Server installed on mid-range virtualized guest
Linux	1000 maximum agent sessions	500 maximum agent sessions	650 maximum agent sessions	325
Windows	700 maximum agent sessions	Not supported	455 maximum agent sessions	Not supported

To support more agent sessions, add additional Avaya Media Server servers to your solution.

High-end server specification

Avaya Aura® Contact Center supports the following high-end server specifications:

- High-end server with dual 6–core CPU
- High-end server with dual 8–core CPU
- High-end server with dual 10–core CPU

These server specifications support the same maximum agent capacity and call rate figures.

The following table lists the minimum specifications for servers with 6–core CPUs in an Avaya Aura® Contact Center High-end solution. These are the minimum specifications for Avaya Aura® Contact Center Release 6.4 for the high-end server in order to support the rated capacities for the high-end server type.

High-end server specification for servers with dual 6–core CPUs		
Specification	Configuration	Comment
CPU	Dual 6–Core Xeon X5680 3.33GHz	You must select a CPU that exceeds the benchmark rating for the Dual 6–Core Xeon X5680 3.33GHz 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 - For virtualized servers, decrease the Avaya Aura® Contact Center agent count and call rate by 15%. Alternately, increase the CPU benchmark rating by 15% for Avaya Aura® Contact Center. - Avaya Media Server is supported only on Intel Xeon Dual Quad core, Dual 6–core, 8–core, or 10–core CPUs. Avaya Media Server does not support AMD processors. - Avaya Aura® Contact Center supports AMD processors of a higher specification. The AMD CPU benchmark score must be at least 10 percent greater than the Intel X5680 benchmark score. Avaya Media Server does not support AMD processors. - Non supported processors include: Intel Celeron and Intel Itanium (IA 64).  Note: CPUs based on more than ten cores are not supported.
RAM	16 GB	32 GB required for virtualized configurations or for capacities in excess of 2000 concurrent agents.
Disk Type and Speed	SCSI, SATA, SAS, Minimum 10000 RPM	- For 3.5 inch disks, the minimum disk speed is 10000 RPM. - For 2.5 inch disks, the minimum disk speed is 15000 RPM. - For more than 1000 agents, the minimum disk speed is 10000 RPM. - For Avaya Media Server, the minimum disk speed is 15000 RPM.

Table continues...

High-end server specification for servers with dual 6-core CPUs		
Specification	Configuration	Comment
		• IDE drives are not supported. • Solid State Drives (SSDs) are not supported.
C: (partition)	80 GB NTFS	OS partition. When installing Avaya Media Server software on a Linux server, Avaya Media Server requires one flat hard disk partition with a minimum of 80 GB.
D: (partition)	80 GB NTFS	Application partition.
DVD Drive	One dual-layer DVD drive	Minimum speed is 4X.
CCMS Database partition	200 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server • Voice Contact Server • Multimedia Complement for Elite • No Switch Configured Multimedia only • Network Control Center Server
CCMM Database partition	300 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server • Multimedia Contact Server • Multimedia Complement for Elite • No Switch Configured Multimedia only
CCT Database partition	10 GB NTFS	Required for the following server types: • Voice and Multimedia Contact Server • Voice Contact Server • Multimedia Complement for Elite • No Switch Configured Multimedia only • CCT Knowledge Worker Server
Total Disk size	670 GB minimum When installing Avaya Media Server software on a Linux server, Avaya Media Server requires one flat hard disk partition with a minimum of 80 GB.	• In solutions using Avaya Aura® Contact Center High Availability, the database partitions on the active, standby, and optional Remote Geographic Node servers must be identical.

Table continues...

High-end server specification for servers with dual 6–core CPUs		
Specification	Configuration	Comment
RAID	Hardware RAID-1	RAID-1 requires a battery backed hardware RAID controller and duplicate drives with identical specifications.
Network Interface	Dual 1 Gbit/s	• Only Ethernet supported. • Quad 1 Gbit/s required for virtualized configurations that include both Avaya Media Server and Avaya Aura® Contact Center guests on the same physical host. • Avaya Media Server configurations require a NIC that supports Receiver Side Scaling (RSS) with a minimum of 4 queues.

The following table lists the minimum specifications for servers with 8–core CPUs in an Avaya Aura® Contact Center High-end solution. These are the minimum specifications for Avaya Aura® Contact Center Release 6.4 for the high-end server in order to support the rated capacities for the high-end server type.

High-end server specification for servers with dual 8–core CPUs		
Specification	Configuration	Comment
CPU	Dual Intel Xeon E5-2670 2.60GHz (or faster)	You must select a CPU that equals or exceeds the benchmark rating for the Dual 8–core Intel Xeon E5-2670 2.60GHz 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 • For virtualized servers, decrease the Avaya Aura® Contact Center agent count and call rate by 15%. Alternately, increase the CPU benchmark rating by 15% for Avaya Aura® Contact Center. • Avaya Media Server is supported only on Intel Xeon Dual Quad core, Dual 6–core, 8–core, or 10–core CPUs. Avaya Media Server does not support AMD processors. • Avaya Aura® Contact Center supports AMD processors of a higher specification. The AMD CPU benchmark score must be at least 10 percent greater than the Intel

Table continues...

High-end server specification for servers with dual 8-core CPUs		
Specification	Configuration	Comment
		E5-2670 benchmark score. Avaya Media Server does not support AMD processors. Non supported processors include: Intel Celeron and Intel Itanium (IA 64).  Note: CPUs based on more than ten cores are not supported.
RAM	32 GB minimum	For maximum performance, all DIMM slots must be populated.
Disk Type and Speed	ESATA, SAS, Minimum 10000 RPM	- Avaya recommends using 15000 RPM disks. - For 2.5 inch disks, the minimum disk speed is 15000 RPM. - For Avaya Media Server, the minimum disk speed is 15000 RPM. - IDE drives are not supported. - Solid State Drives (SSDs) are not supported.
DVD Drive	One dual-layer DVD drive	16X or faster recommended. DVD and Blu-ray combo drives are supported.
Total Disk size	900 GB minimum When installing Avaya Media Server software on a Linux server, Avaya Media Server requires one flat hard disk partition with a minimum of 80 GB.	In solutions using Avaya Aura® Contact Center High Availability, the database partitions on the active, standby, and optional Remote Geographic Node servers must be identical.
RAID	Hardware RAID-1	RAID-1 requires a battery backed hardware RAID controller and duplicate drives with identical specifications.
Network Interface	Dual 1 Gbit/s	- Only Ethernet is supported. - Quad 1 Gbit/s required for virtualized configurations that include both Avaya Media Server and Avaya Aura® Contact Center guests on the same physical host. - Avaya Media Server configurations require a NIC that supports Receiver Side

Table continues...

High-end server specification for servers with dual 8–core CPUs		
Specification	Configuration	Comment
		Scaling (RSS) with a minimum of 4 queues.

The following table lists the minimum specifications for servers with 10–core CPUs in an Avaya Aura® Contact Center High-end solution. These are the minimum specifications for Avaya Aura® Contact Center Release 6.4 for the high-end server in order to support the rated capacities for the high-end server type.

High-end server specification for servers with dual 10–core CPUs		
Specification	Configuration	Comment
CPU	Dual Intel Xeon E5-2680 v2 2.8GHz (or faster)	You must select a CPU that equals or exceeds the benchmark rating for the Dual 8–core E5-2680 v2 2.8GHz 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 - For virtualized servers, decrease the Avaya Aura® Contact Center agent count and call rate by 15%. Alternately, increase the CPU benchmark rating by 15% for Avaya Aura® Contact Center. - Avaya Media Server is supported only on Intel Xeon Dual Quad core, Dual 6–core, 8–core, or 10–core CPUs. Avaya Media Server does not support AMD processors. - Avaya Aura® Contact Center supports AMD processors of a higher specification. The AMD CPU benchmark score must be at least 10 percent greater than the Intel E5-2680 v2 benchmark score. Avaya Media Server does not support AMD processors. - Non supported processors include: Intel Celeron and Intel Itanium (IA 64). * Note: CPUs based on more than ten cores are not supported.
RAM	32 GB minimum	For maximum performance, all DIMM slots must be populated.

Table continues...

High-end server specification for servers with dual 10-core CPUs		
Specification	Configuration	Comment
Disk Type and Speed	ESATA, SAS, Minimum 10000 RPM	- Avaya recommends using 15000 RPM disks. - For 2.5 inch disks, the minimum disk speed is 15000 RPM. - For Avaya Media Server, the minimum disk speed is 15000 RPM. - IDE drives are not supported. - Solid State Drives (SSDs) are not supported.
DVD Drive	One dual-layer DVD drive	16X or faster recommended. DVD and Blu-ray combo drives are supported.
Total Disk size	900 GB minimum When installing Avaya Media Server software on a Linux server, Avaya Media Server requires one flat hard disk partition with a minimum of 80 GB.	In solutions using Avaya Aura® Contact Center High Availability, the database partitions on the active, standby, and optional Remote Geographic Node servers must be identical.
RAID	Hardware RAID-1	RAID-1 requires a battery backed hardware RAID controller and duplicate drives with identical specifications.
Network Interface	Dual 1 Gbit/s	- Only Ethernet is supported. - Quad 1 Gbit/s required for virtualized configurations that include both Avaya Media Server and Avaya Aura® Contact Center guests on the same physical host. - Avaya Media Server configurations require a NIC that supports Receiver Side Scaling (RSS) with a minimum of 4 queues.

*** Note:**

For information about achieving the maximum performance from your server hardware, see [Server performance and BIOS settings](#) on page 326.

For servers operating at 40% 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.

Server performance and BIOS 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 behaviour 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.

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 and RAID-5. RAID technology provides disk data redundancy as well as error detection and correction. For maximum security and mission-

critical solutions, Avaya recommends that all Contact Center servers contain a RAID controller. Hardware RAID-1 and RAID-5 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:

- For Intel based hosts: Enable Intel virtualization (VT-x) and if available enable Extended Page Tables (EPT)

- For AMD based hosts: Enable AMD virtualization (AMD-V) and if available enable Rapid Virtualization Indexing (RVI). Note: Avaya Media Server does not support AMD processors.

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 to improve server and Avaya Aura® Contact Center performance.

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.

Avaya Media Server and Contact Center on one VMware host

Virtualized solution

This section describes an Avaya Aura® Contact Center for Midsize Enterprise (AACC-M) solution where Avaya Media Server and Avaya Aura® Contact Center are virtualized on one VMware host.

When Avaya Aura® Contact Center and Avaya Media Server are virtualized on the same VMware host server, the host server supports only:

- One Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Media Server running on a guest operating system (Windows Server 2008 Release 2, 64-bit, Service Pack 1).
- One standalone Avaya Media Server server running on a guest operating system (Red Hat Enterprise Linux 6.x 64-bit only).

This configuration supports only two guests on the host; one guest for the Voice and Multimedia Contact Server (Windows), and another guest for Avaya Media Server (Linux). No other guests are supported on this VMware host. This section also specifies these supported VMware guest specifications.

! Important:

This Avaya Aura® Contact Center virtualized solution does not support Avaya Aura® Contact Center High Availability. Virtualized Avaya Media Server does not support High Availability.

The following table lists the installation options, maximum number of agents, and maximum call rates of a virtualized Avaya Aura® Contact Center solution.

Virtualized server applications	Type	Agents maximum	CCMA Supervisors	System Contact Rate (cph)	MM Rate (WCph/Eph)
Voice and Multimedia Contact Server without Avaya Media Server and a standalone Avaya Media Server server on Linux.	Aura — SIP	400 Note 1	80	4K Note 2	600 / 1200 Note 2
• Note 1: This is limited to a maximum of 300 agents active on customer calls, 100 agents on post-call activity with an additional 100 customer calls receiving treatment. • Note 2: The System Contact Rate is the maximum contact rate across all modalities that can be supported. For a voice only system, this equates to the maximum call rate.					

Virtualization specifications

When Avaya Aura® Contact Center and Avaya Media Server are virtualized on the same VMware host server, the host server must meet or exceed the High-end server specification. For more information about the High-end servers, see [High-end solution and server specification](#) on page 317.

The following table lists the minimum specifications for the VMware guests when Avaya Aura® Contact Center and Avaya Media Server are virtualized on the same VMware host server.

Server type	Minimum specification	Configuration	Comment
Voice and Multimedia Contact Server without Avaya Media Server VMware guest	CPU cores	12 logical CPU cores	-
	RAM	12 GB allocated	-
	Total Hard Disk size	670 GB	Thick Provision Lazy Zeroed.
	Network Interface Card (NIC)	Minimum 2 NIC configuration	One VMware Virtual adapter connected to a dedicated VSwitch for Avaya Aura® Contact Center network with one dedicated physical NIC. The NICs must be 1 Gbit/s or faster.
	DVD drive	One DVD drive	-
	Operating System	Windows Server 2008 Release 2 64-bit server	Standard or Enterprise edition.
	C: (partition)	80 GB	OS partition only.
	D: (partition)	80 GB	Application partition.
	CCMS and CCT Databases partition	210 GB	F drive.
	CCMM Database partition	300 GB	G drive.
Avaya Media Server VMware guest	CPU cores	12 logical CPU cores	-
	RAM	12 GB allocated	-
	Total Hard Disk size	80 GB	The Avaya Media Server applications require 3GB of disk space. The additional space provides for prompts, tones, scripted music, and announcement files, and agent greeting recordings. Avaya recommends installing Avaya Media Server on a different partition to the operating system partition. Configure the partitions for Thick Provision Lazy Zeroed.
	Network Interface Card (NIC)	Minimum 2 NIC configuration	One VMware Virtual adapter connected to a dedicated VSwitch for Avaya MS network with one dedicated physical NIC. The NICs must be 1 Gbit/s or faster.

Table continues...

Server type	Minimum specification	Configuration	Comment
	DVD Drive	One DVD drive	-
	Operating System	Linux Red Hat 6.5 64-bit version	-

Hardware Appliance capacity limits

Hardware Appliance limits

The following table lists the maximum number of agents and maximum call rates of an Avaya Aura® Contact Center Hardware Appliance solution.

Server type	Voice Platform type	Maximum logged-in Agents	Maximum CCMA Supervisors	Maximum System Contact Rate (cph) ¹	Maximum multimedia rate (WCph/Eph) ²
Avaya Aura® Contact Center Hardware Appliance with Voice and Multimedia Contact Server with Avaya Media Server	Aura SIP	300	50	6K	600/1200
	Aura SIP	400	80	4K	600/1200

Note 1: The Maximum System Contact Rate is the maximum supported contact rate for all contact types combined. The Maximum System Contact Rate is the maximum number of voice and multimedia contacts Avaya Aura® Contact Center can handle in one hour. For a voice only solution, the Maximum System Contact Rate is the maximum voice call rate (BHCC).

Note 2: Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Web Chats per hour (WCph). Email contacts per hour (Eph).

Note: The Hardware Appliance supports 100 queued contacts at the maximum agent capacity.

Note: The Aura SIP agent count and call rate limits apply to configurations using Avaya Aura® Communication Manager Release 6.0.1 or later.

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: The Hardware Appliance server does not support Avaya Aura® Contact Center High Availability.

Note: You can use CCMA on this server to manage agents supervisors associated both with this server or with remote CCMS servers. However, you can manage all agents only up to the maximum supervisor capacity for this server.

The Avaya Aura® Contact Center Hardware Appliance package includes an optimized high specification rack mount server. For more information about the Hardware Appliance server supplied by Avaya, see [Hardware Appliance server specifications](#) on page 333.

Hardware Appliance server specification

The Contact Center Hardware Appliance is a Dell R620 rack mount server preconfigured to support Contact Center.

Contact Center is a collection of real-time applications running on the Microsoft Windows Server 2008 R2 SP1 operating system. Contact Center provides real-time call control, multimedia handling, and real-time statistical reporting.

Important:

The Contact Center Hardware Appliance server supplied by Avaya is optimized to provide the real-time computational, networking, and logging resources required by Contact Center. You must not modify the Hardware Appliance server, unless instructed to do so by Avaya:

- Do not add additional internal hardware devices to this server.
- Do not change or upgrade the server BIOS version or settings.
- Do not change the server hardware settings.
- Do not update the server firmware.
- Do not change or upgrade the device drivers.
- Do not modify the hard disk partitions.
- Do not change the *Windows Update* application settings on the server.
- Do not upgrade the Java Runtime Environment (JRE) supplied on the Hardware Appliance.

Due to the real-time processing that Contact Center applications perform, you must not install any other application class software on the server. You can install only the supported antivirus and remote support utility class software on this server.

Install only the Microsoft Windows Server 2008 R2 SP1 Operating System patches and hotfixes supported by Contact Center. For more information about the supported Operating System patches, see the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Compatibility List* on www.avaya.com/support.

The following table lists the server specifications for the Contact Center Hardware Appliance Dell R620 server.

Specification	Quantity	Configuration	Comment
Form factor	1	Rack mount, 1U chassis	PowerEdge R620 rack mount server.
CPU	2	Intel Xeon E5-2670 2.60GHz, 20M Cache, 8.0GT/s QPI, Turbo, 8C, 115W, DDR3-1600MHz	—

Table continues...

Specification	Quantity	Configuration	Comment
RAM	8	4GB RDIMM, 1333 MHz, Low Volt, Dual Rank	—
Hard Disk	2	900 GB, SAS 6 Gbps, 2.5 inch, 10K RPM Hard Drive	The 900 GB hard disk is pre-configured with Operating System, application, and database partitions.
RAID Controller	1	PERC H710 Integrated RAID Controller, 512MB NV Cache	—
RAID Type	N/A	RAID-1	2x 900 GB hard disk drives
Optical Drive	1	16X DVD +/-RW Drive SATA with SATA Cable	—
Network Interface	4	1 Gbps NICs on motherboard	Only Ethernet supported.
Power supply	2	750 Watt AC auto-sensing, hot pluggable Power Supply	—
Power cables	2	Power cables	Localized to region.
Additional interfaces		• 2 front USB ports • 2 back USB ports • Front video connector	—
Additional hardware	1	Rack mount kit	—
Weight		55 lbs approximately 25 kilograms approximately	
BTU/HR		2891 BTU/hr maximum per 750 W power supply.	

Chapter 25: SIP Contact Center configuration requirements

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

General requirements

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

SIP-enabled Contact Center feature limitations

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

- In a SIP-enabled Contact Center using an Avaya Communication Server 1000, Call Forward (CFW) is not supported. CFW must be disabled on Agent phones. Call Forward is not supported on agent phones. Call Forward All Calls and Call Forward No Answer are not supported. The Call Presentation Class of Service settings can be used to direct calls back to the application.
- In a SIP-enabled Contact Center using a Communication Manager, Avaya Aura® Contact Center supports a limited configuration of the Communication Manager - Coverage Path feature. For more information, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).
- In a SIP-enabled Contact Center, blind (single-step) transfers are not supported. However, early transfer completion is supported. Early transfer completion is the ability to complete a supervised (two-step) transfer while the far end is still ringing. In a SIP-enabled Contact Center, references to blind transfer mean supervised transfer with early transfer completion.
- Each SIP-enabled Avaya Communication Server 1000 agent phone supports a single key.
- Trunk information in Historical Reports is not supported.
- Host Enhanced Routing is not supported.
- The “Let call ring” call presentation class is not supported. The call might ring for a maximum of 32 seconds, because of a SIP signaling timeout.
- Call Force Delay for Instant Message (IM) contacts is not supported.
- The Instant Messaging CDN alias and number must be configured the same.

- Walk-away is not supported.
- Agents must not use their desk phone or Agent Desktop to phone, transfer a call, or conference a call to a phone number that is:
 - routed to a CDN (Route Point). For example, a Virtual Directory Number (VDN) routed to a CDN (Route Point).
 - converted to a CDN (Route Point). For example when using digit manipulation on the call server.
 - call forwarded to a CDN (Route Point).

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

Dependent platform and switch compatibility

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

Table 15: SIP-enabled switch compatibility

Platform	Release
Avaya Aura® Unified Communications platform	6.1, 6.2
Avaya Communication Server 1000 + Signaling Server + Network Routing Service (NRS)	7.0
Avaya Communication Server 1000 + Session Manager 6.1	7.5, 7.6

Important:

Avaya Aura® Contact Center Release 6.4 does not support the Avaya Aura® Midsize Business Template (MBT) or Avaya Aura® Unified Communications Release 5.2 platforms for new installations. Existing Avaya Aura® Contact Center solutions using MBT or Avaya Aura® 5.2 can be expanded or upgraded.

Important:

Avaya Aura® Contact Center Release 6.4 does not support SIP-enabled Avaya Communication Server 1000 for new installations. Existing SIP-enabled Avaya Communication Server 1000 contact center installations can be expanded or upgraded.

Upgrade path

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

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

Digital Signal Processing Considerations

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

- [Voice over Internet Protocol](#) on page 337
- [PABX Digital Signal Processors](#) on page 338
- [Avaya Aura® Shuffling](#) on page 339
- [PABX DSP consumption examples](#) on page 339
- [Avaya Communication Server 1000 DSP](#) on page 340
- [Avaya Aura® Unified Communications platform DSP](#) on page 340

Voice over Internet Protocol

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

- **Signaling**—Voice over IP is used by industry standard protocols and proprietary Avaya signaling protocols. The Avaya Communication Server 1000 PABX uses a proprietary signaling protocol called Unistim for phone set signaling. Avaya Aura® Contact Center uses industry standard signaling protocols such as SIP and H.323.
- **Media**—VoIP supports many media variants such as audio, video, and Instant Messaging. Communication systems use codecs to encode media streams for transmission and to decode the media for playback. Codecs encode and decode media such as VoIP audio (G.711, G.729, G.726).

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

Example 1:

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

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

Example 2:

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

- **Signaling**: the gateway translates from ISDN D-Channel signaling to SIP signaling and visa versa.

- Media: a DSP is required to transcode ISDN Pulse-code modulation (PCM) audio into G.711 audio for SIP communications.

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

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

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

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

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

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

PABX Digital Signal Processors

Digital Signal Processors (DSPs) can be used to transcode or convert media from one protocol to another. Transcoding is the direct digital-to-digital conversion from one encoding type to another. The Avaya Communication Server 1000 PABX Media Gateway Controller (MGC) card has a 96 channel DSP daughter board that it uses to transcode TDM media to IP media and vice versa.

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

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

You must engineer your Avaya Aura® Unified Communications platform or Avaya Communication Server 1000 PABX with a sufficient number of Digital Signal Processor channels to handle the TDM and VoIP transcoding in your contact center solution.

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

Avaya Aura® Shuffling

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

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

Important:

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

PABX DSP consumption examples

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

- Each TDM customer consumes one DSP. Customer calls typically enter Avaya Aura® Communication Manager or Avaya Communication Server 1000 on the TDM side of the PABX. These calls require transcoding from TDM to VoIP for Avaya Media Server and Avaya Aura® Contact Center. For example, if you have 10 TDM calls waiting, and 5 TDM calls answered by agents with IP desk phones, your PABX is consuming 15 PABX DSP channels.
- Each TDM agent consumes one DSP channel while on a Contact Center call. Customer calls can enter Communication Manager or Avaya Communication Server 1000 on the VoIP side of the switch. If your contact center uses TDM agents then these calls require transcoding from VoIP to TDM for the TDM agents. For example, if you have 10 TDM calls waiting, 5 TDM calls answered by 2 TDM agents, and 3 IP Agents, your solution is consuming $10+5+2=17$ DSP channels.
- If a customer call arrives into an enterprise through SIP, and is finally transferred to a TDM user, for example using ISDN, then Avaya Aura® Communication Manager or Avaya

Communication Server 1000 consumes one DSP channel to tandem this call from VoIP to TDM.

- If a customer call arrives into an enterprise using TDM (PSTN - ISDN), and is finally transferred to a TDM user, for example using ISDN, Avaya Aura® Communication Manager or Avaya Communication Server 1000 normally optimizes the call so the call no longer tandems though DSPs, and all DSP resources are released.
- If a customer call originates on a SIP carrier, the call enters the contact center through the SIP voice proxy. Avaya Aura® Contact Center supports SIP Enablement Services, Session Manager, and Avaya NES Networking Routing Service as SIP voice proxies. The SIP proxy routes the call directly to Avaya Aura® Contact Center which anchors the call on an Avaya Media Server. VoIP agents handle this call. There is no DSP requirement for this call scenario.

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

Avaya Communication Server 1000 DSP

Engineer the Avaya Communication Server 1000 system so it is capable of supporting SIP, in particular engineer the DSP hardware resources to support TDM and IP transcoding. Incoming PSTN calls require one DSP per call. Agents with TDM phones each require another DSP. For more information, see *Communication Server 1000M Large System Planning and Engineering* (NN43021-220) and *Communication Server 1000E Planning and Engineering* (NN43041-220).

Avaya Aura® Unified Communications platform DSP

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

Dialed Number Identification Service

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

DNIS Options in SIP-enabled contact centers

Session Manager and Avaya Communication Server 1000 support DNIS information for Contact Center using the To header technique.

- [Incoming SIP Invite message with DNIS information in the To header](#) on page 341
- [Avaya Communication Server 1000 systems](#) on page 341
- [Session Manager systems](#) on page 343

Session Manager and Midsize Business Template support DNIS information for Contact Center using the Virtual Directory Number “DNIS” prefix technique.

- [Incoming SIP Invite message with DNIS information in the History-Info header](#) on page 341
- [Midsize Business Template systems](#) on page 342
- [Session Manager systems](#) on page 343

Incoming SIP Invite message with DNIS information in the To header

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

Session Manager and Avaya Communication Server 1000 support DNIS information for Contact Center using this To header technique.

Avaya Communication Server 1000 systems

Avaya Communication Server 1000 provides DNIS information in the SIP To header of the incoming SIP Invite message to Avaya Aura® Contact Center.

You must apply the Avaya Communication Server 1000 patch MPLR30797 to support this functionality.

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

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

Midsize Business Template systems

Midsize Business Template systems cannot provide DNIS information in the To address, but they can provide DNIS information in the SIP “History-Info” header of the incoming SIP Invite message.

On the Midsize Business Template—Communication Manager create a Virtual Directory Number (VDN) for each DNIS required. The VDN name must contain the capitalized keyword “DNIS”.

The following example shows the Virtual Directory Number “DNIS” naming convention. The example VDN name shown is configured to be “DNIS8456464”. The VDN name contains a “DNIS” prefix followed by a unique identification number. This unique identification number does not have to match the extension number.

```
display vdn 8456464                                     Page 1 of 3
VECTOR DIRECTORY NUMBER
Extension: 845-6464
Name*: DNIS8456464
Destination: Vector Number      64
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none

VDN of Origin Annc. Extension*:
1st Skill*:
2nd Skill*:
3rd Skill*:

* Follows VDN Override Rules
```

Figure 29: Example of configuring VDN name with DNIS prefix

Contact Center retrieves the DNIS number from the incoming SIP Invite message by parsing the URI that Communication Manager builds into the ‘History-Info’ header. The URI is based on the value of the VDN ‘extension’ field.

For example:

History-Info: “DNIS8456464” <sip:8456464@sipccocs.com>;index=1.2.

In this example Contact Center retrieves a DNIS number of “8456464” from the URI in the “History-Info” header. Contact Center then uses this DNIS number to route or treat the call.

Session Manager systems

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

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

Office Communications Server 2007 hardware requirements

The following table provides the hardware requirements of the Office Communications Server (OCS) network portion of the SIP Contact Center solution and details the OCS server types required to achieve the corresponding agent capacity. These values are based on scaling down the Microsoft-issued statistics for user capacity in an OCS configuration. The Microsoft figures in the third column are based Microsoft-stated 5 percent usage level.

This table does not account for non-Contact Center activity on the part of the OC client users. (for example, if other users use the OCS network and servers for non-Contact Center activity).

Table 16: OCS server requirements

Topology	Servers	Number of OC users (Microsoft numbers)	Scaled maximum number of Contact Center agents
Standard Edition (SE)	1 SE Front End server 1 Access Edge server	< 5000	< 200
Enterprise Edition (EE) Consolidated	4 Front End servers 1 Backend SQL server 1 Access Edge server	< 30 000	< 1500
Enterprise Edition Expanded Mid-range SQL	4 Front End servers 2 IIS servers 1 Backend SQL server 1 Access Edge server	< 50 000	< 1500
Enterprise Edition Expanded High-end SQL	8 Front End servers 2 IIS servers	< 125 000	< 1500

Table continues...

Topology	Servers	Number of OC users (Microsoft numbers)	Scaled maximum number of Contact Center agents
	1 Backend SQL server 1 Access Edge server		

The following table describes the reference hardware for the servers in the OCS network.

Table 17: OCS server hardware requirements

Component	Front End servers (SE or EE), Access Edge, or IIS server	EE Backend SQL server (mid-range)	EE Backend SQL server (high-end)	A/V Access Edge Conferencing
CPU	Dual processor, dual core 2.6 GHz	Dual processor, dual core 2.6 GHz	Quad processor, dual core 2.6 GHz	Dual processor, dual core 2.6 GHz
Disk	2 x 18 GB For collocated Standard Edition server, add 2 x 36 GB, 15K RPM, RAID 0 for database log files and 2 x 36 GB, 15K RPM, RAID 0 for database data.	2 x 18 GB For collocated Standard Edition server, add 2 x 36 GB, 15K RPM, RAID 0 for database log files and 2 x 36 GB, 15K RPM, RAID 0 for database data.	Drive 1 (2 x 18 GB) for OS and Page File Drive 2 (4 x 36GB, 15K RPM, RAID 0+1) for database log file Drive 3 (4 x 36GB, 15K RPM, RAID 0+1) for database log file Drive 4 (8 x 36GB, 15K RPM, RAID 0+1) for database files	2 x 18 GB
Cache	1 MB Layer 2 for each core	1 MB Layer 2 for each core	2 MB Layer 2 for each core	1 MB Layer 2 for each core
Memory	2 GB (4 GB for Standard Edition Server or Consolidated Enterprise Edition Server)	2 GB (4 GB for Standard Edition Server or Consolidated Enterprise Edition Server)	16 GB	4 GB
Network	Gbit NIC	Gbit NIC	Gbit NIC	2 x Gbit NIC

Chapter 26: Server virtualization support

Avaya Aura® Contact Center supports server virtualization. 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 term guest refers to a virtual machine on the host server.

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:

- VMware ESXi Release 5.0, 5.1, and 5.5 (with VMFS 5.54 or later)
- Microsoft Hyper-V

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 guests 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 Release 6.4 supports migration from physical to virtual servers, and from virtual to physical servers. This is dependant on the server you are migrating to satisfying the server specifications. For more information about migration, see *Avaya Aura® Contact Center Upgrade and Patches* (44400-410).

VMware support

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 guests on a large x86-based host hardware server. You must ensure that each guest (virtual machine) on which you plan to install Contact Center software satisfies the capacity requirements and specifications for your contact center. Use the guidelines in [Server Specifications](#) on page 305 to determine the capacity requirements and specifications for your contact center configuration.

Navigation:

- [VMware features](#) on page 354
- [VMware vSphere host considerations](#) on page 355
- [Guidance for storage requirements](#) on page 356
- [VMware Guest Operating Systems](#) on page 357
- [Overview of commissioning Contact Center with VMware](#) on page 357
- [Performance monitoring and management](#) on page 359
- [High Availability and virtualization](#) on page 360
- [Avaya Aura Contact Center VMware Snapshot considerations](#) on page 360
- [Avaya Media Server VMware snapshot considerations](#) on page 361
- [VMware networking best practices](#) on page 361
- [Time synchronization considerations](#) on page 362
- [Troubleshooting VMware](#) on page 362

The following table shows Avaya Aura® Contact Center VMware support for each server type and platform.

Table 18: Avaya Aura® Contact Center VMware support by server type

Voice Platform	Server type	Guest OS	Supported
SIP-enabled Avaya Aura® Unified Communications platform	Voice and Multimedia Contact Server without Avaya Media Server	Windows	Yes
	Voice Contact Server Only	Windows	Yes
	Multimedia Contact Server Only	Windows	Yes
	Voice and Multimedia Contact Server with Avaya Media Server	Windows	No
	Avaya Media Server	Linux	Yes ^{Note 1}
AML-based Avaya Communication Server 1000 (CS 1000)	Voice and Multimedia Contact Server without Avaya Media Server	Windows	Yes
	Voice Contact Server Only	Windows	Yes
	Multimedia Contact Server Only	Windows	Yes
	Knowledge Worker Server Only	Windows	Yes
Avaya Aura® Call Center Elite	AACC Multimedia Complement for Elite	Windows	Yes
No voice platform (No Switch configured)	Voice and Multimedia Contact Server with Avaya Media Server	Windows	No
All voice platform types	Network Control Center Server Only	Windows	Yes
• Note 1: Where Avaya Media Server on Linux is installed as a VMware guest on the same VMware host as Avaya Aura® Contact Center, Avaya Aura® Contact Center supports only two guests on the host server; one guest for Avaya Media Server (Linux), and another guest for the Voice and Multimedia Contact Server (Windows). No other guests are supported on this VMware host.			

The Windows version of Avaya 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 Media Server is installed on a physical Linux server.

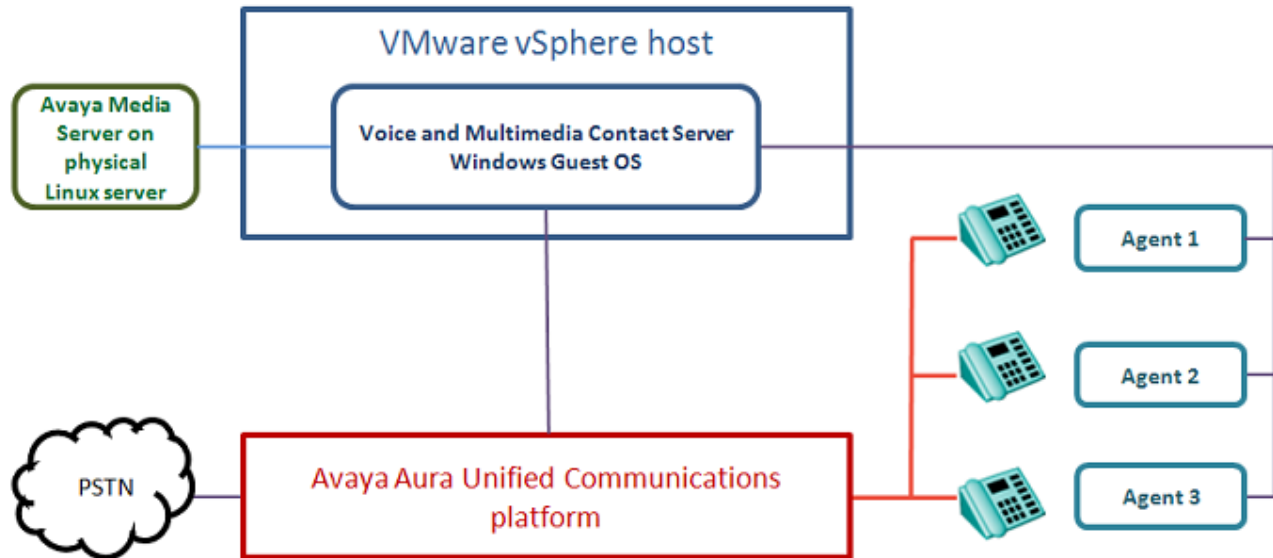


Figure 30: A typical SIP-enabled solution with virtualized Avaya Aura® Contact Center

The following diagram shows another virtualized SIP-enabled example solution. The diagram shows a Voice and Multimedia Contact Server on a Windows virtual guest. Avaya Media Server is installed on a virtual Linux guest. Avaya Media Server and the Voice and Multimedia Contact Server are installed on separate VMware host servers.

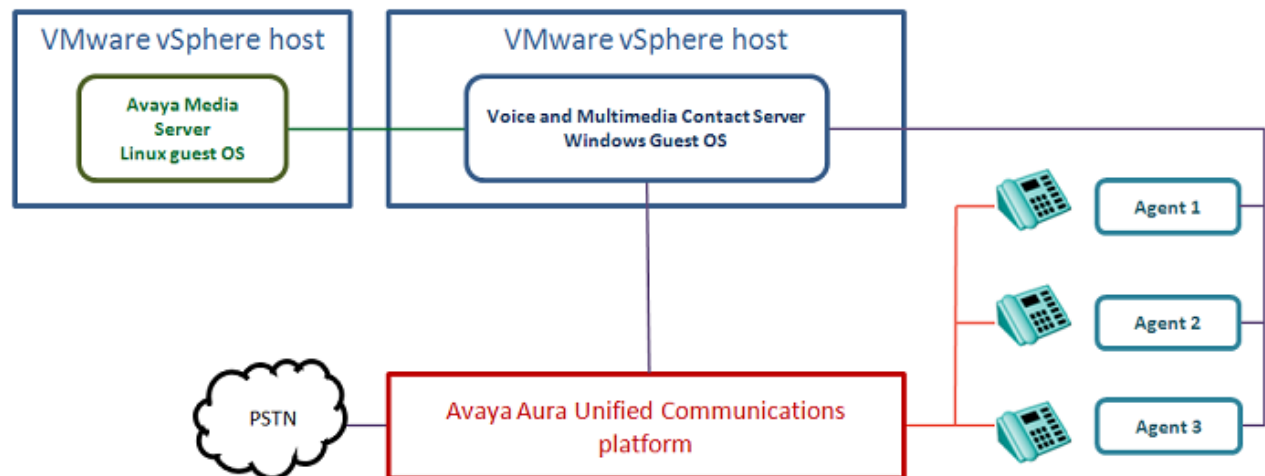


Figure 31: An example solution with Avaya Media Server and Avaya Aura® Contact Center on separate VMware host servers

For these small to medium size solution types, Avaya Aura® Contact Center supports Network Control Center as a VMware guest 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 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 Media Server.

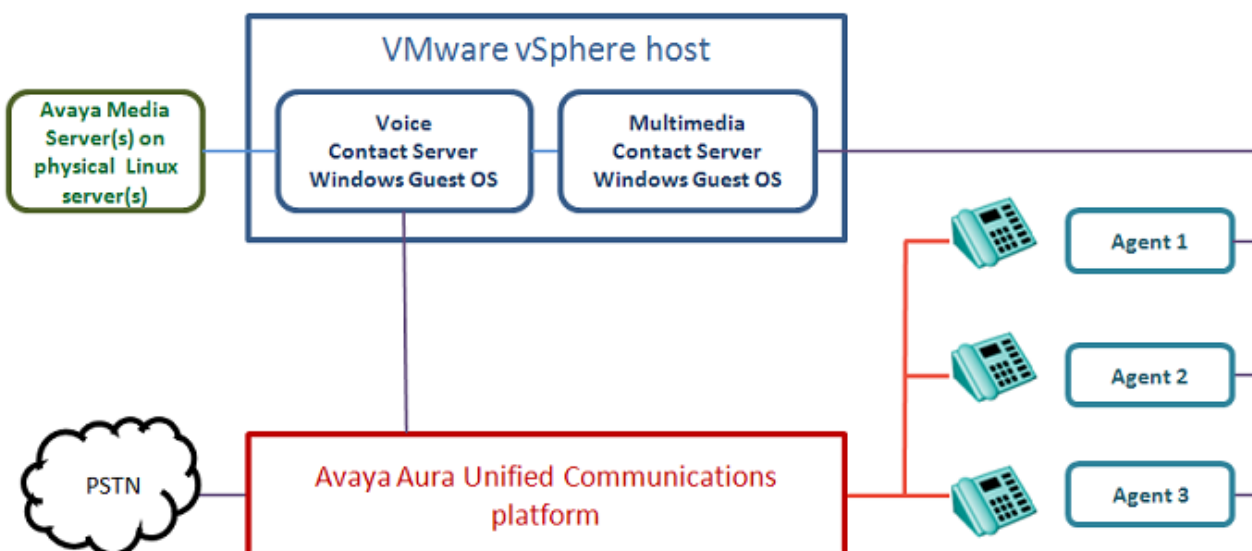


Figure 32: A typical SIP-enabled solution with virtualized Avaya Aura® Contact Center (large solution)

The following diagram shows another virtualized large SIP-enabled example solution. The diagram shows a Voice Contact Server on a Windows virtual machine, and Multimedia Contact Server on another Windows virtual guest. Avaya Media Server is installed on a virtual Linux guest. In this example, the Voice Contact Server and the Multimedia Contact Server are virtualized on one VMware host server. Avaya Media Server is virtualized on a separate VMware host server. Depending on the number of agents required, a large SIP-enabled solution might require more than one virtual Avaya Media Server.

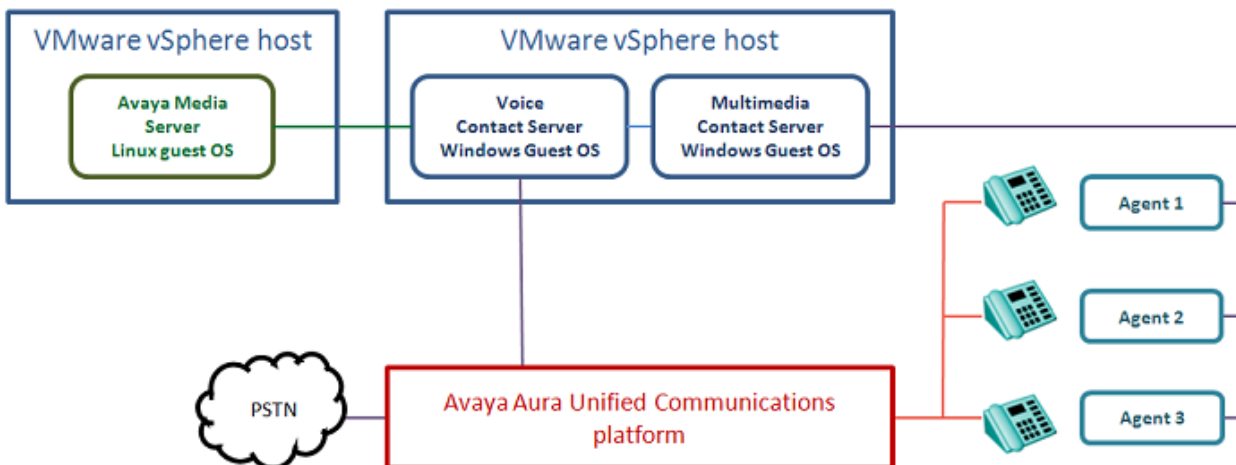


Figure 33: A typical large solution with Avaya Media Server and Avaya Aura® Contact Center on separate VMware host servers

Avaya Aura® Contact Center also supports Voice Contact Server and Multimedia Contact Server virtualized on separate VMware host servers.

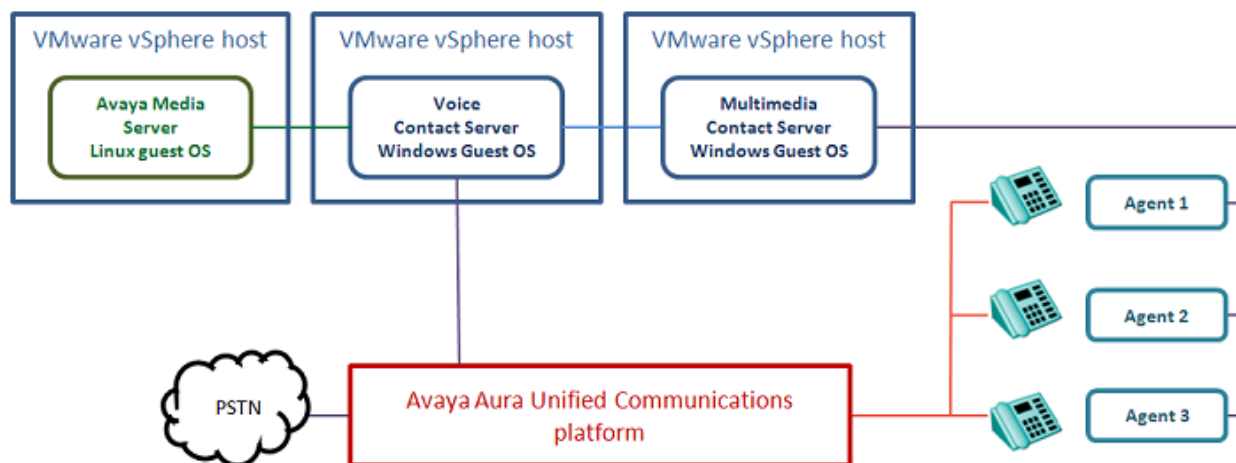


Figure 34: A typical large solution with all contact center servers on separate VMware host servers

For these large solution types, Avaya Aura® Contact Center supports Network Control Center as a VMware guest on the same host as the Voice Contact Server or the Multimedia Contact Server.

Example of Avaya Media Server and Avaya Aura® Contact Center on the same VMware host server

The following diagram shows a typical virtualized solution with Avaya Aura® Contact Center and Avaya Media Server on the same VMware host server. 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 guest operating system (OS). Avaya Media Server is installed on a Linux guest. In this example solution, Avaya Media Server and Avaya Aura® Contact Center are on the same VMware host server.

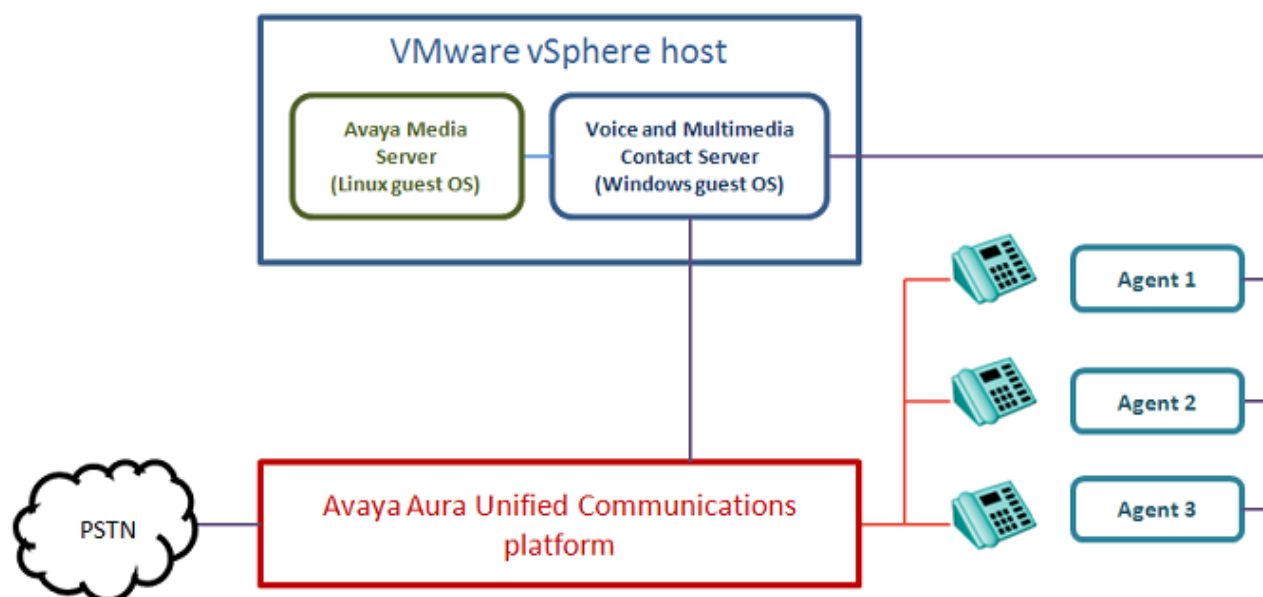


Figure 35: A typical solution with Avaya Media Server and Avaya Aura® Contact Center on the same VMware host server

When Avaya Aura® Contact Center and Avaya Media Server are virtualized on the same VMware host server, the host server supports only:

- One Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Media Server running on a guest operating system (Windows Server 2008 Release 2, 64-bit, Service Pack 1).
- One standalone Avaya Media Server server running on a guest operating system (Red Hat Enterprise Linux only).

This configuration supports only two guests on the host; one guest for the Voice and Multimedia Contact Server (Windows), and another guest for Avaya Media Server (Linux). No other guests are supported on this VMware host.

Avaya Aura® Contact Center does not support Network Control Center as a VMware guest on the same host server as Avaya Media Server. Avaya Aura® Contact Center supports Network Control Center as a VMware guest on a different VMware host. For more information about the VMware specifications for this type of solution, see [Avaya Media Server and Contact Center on one VMware host](#) on page 330.

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.

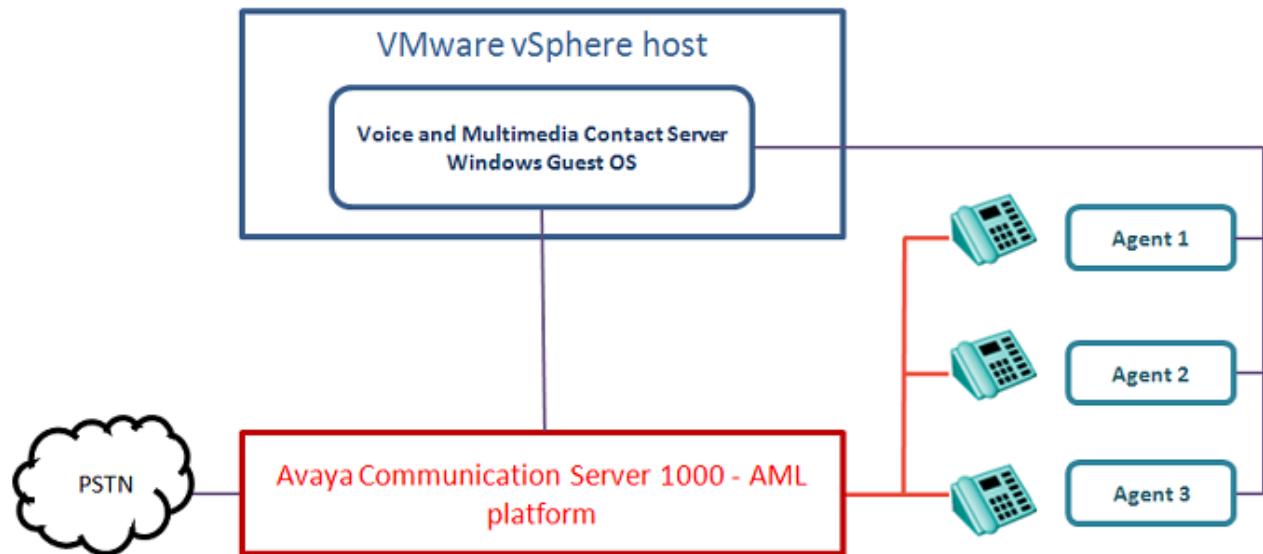


Figure 36: A typical CS 1000 AML-based solution with virtualized Contact Center (small to medium solution)

For this solution type, Avaya Aura® Contact Center supports Network Control Center as a VMware guest 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.

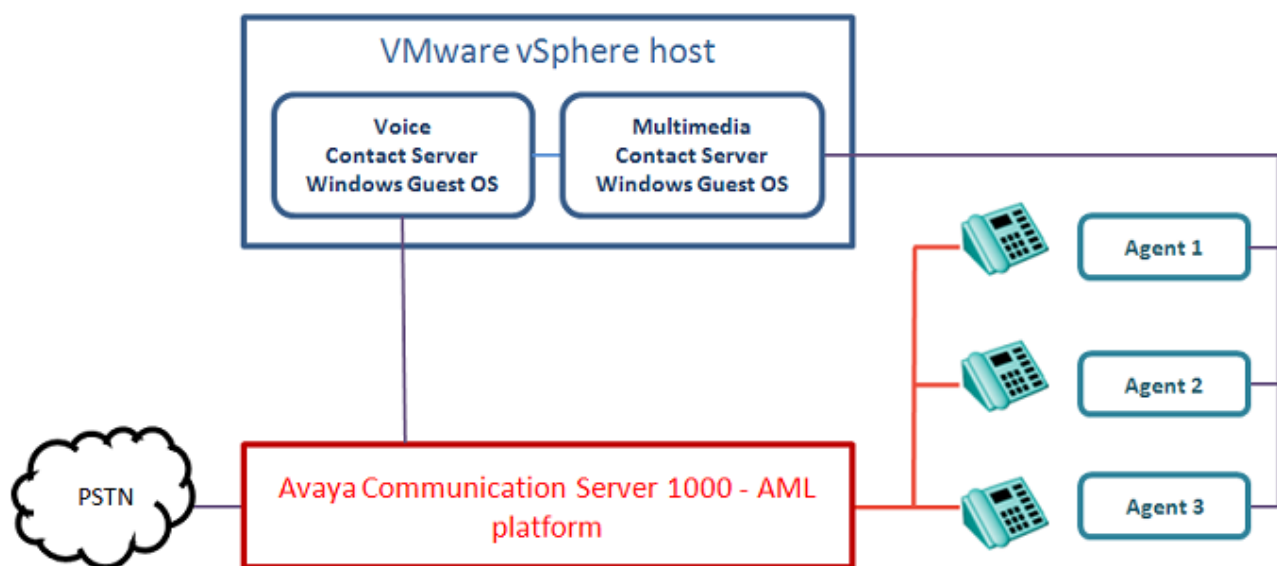


Figure 37: A typical CS 1000 AML-based solution with virtualized Contact Center (large solution)

Avaya Aura® Contact Center also supports Voice Contact Server and Multimedia Contact Server virtualized on separate VMware host servers.

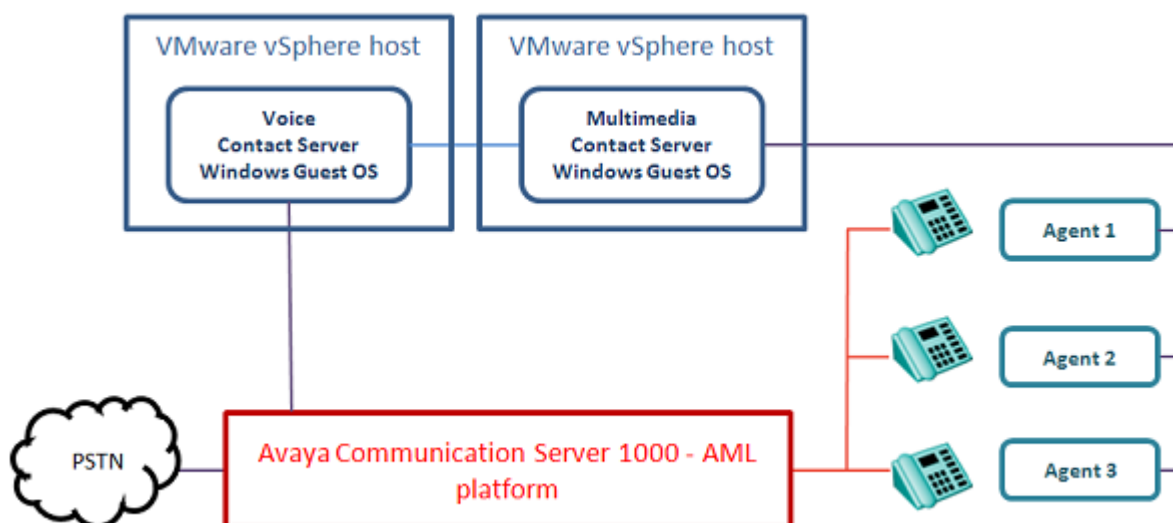


Figure 38: A typical CS 1000 based solution with contact center servers on separate VMware host servers

For this solution type, Avaya Aura® Contact Center supports Network Control Center as a VMware guest on the same host as the Voice Contact Server and the Multimedia Contact Server.

Example of a Call Center Elite based Contact Center solution

The following diagram shows a typical virtualized Avaya Aura® Contact Center solution. This solution is based on the Avaya Aura® Call Center Elite voice-based call center. The diagram shows AACC Multimedia Complement for Elite software on a Windows guest operating system (OS).

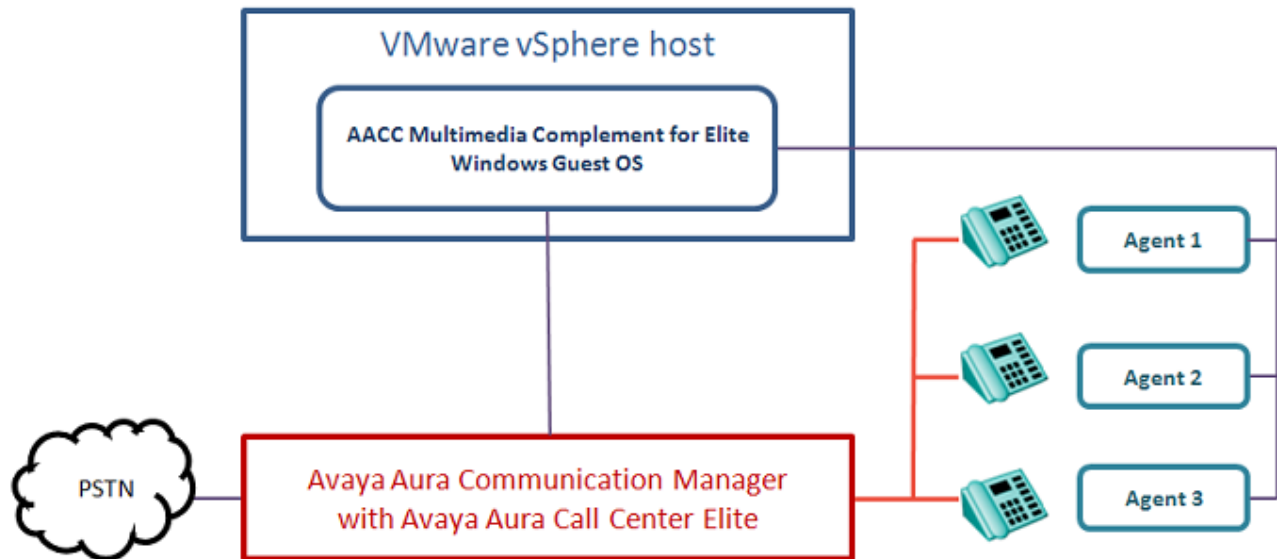


Figure 39: Virtualized Contact Center solution

For this solution type, Avaya Aura® Contact Center supports Network Control Center as a VMware guest on the same host as the AACC Multimedia Complement for Elite server.

VMware features

Avaya Aura® Contact Center is a collection of real-time applications running on the MS Windows Server 2008 R2 SP1 operating system. Avaya Aura® Contact Center provides real-time call control, multimedia handling, and statistical reporting.

Avaya Media Server is a real-time media processing application running on the Red Hat Enterprise Linux (RHEL) operating system. Avaya 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 Media Server Virtual Machines (VMs). These features are therefore not supported while Avaya Aura® Contact Center or Avaya Media Server are active.

Some VMware features are not supported by Avaya Aura® Contact Center or Avaya Media Server. Some other VMware features are supported only while the Avaya Aura® Contact Center or Avaya Media Server Virtual Machines are stopped for maintenance.

The following table shows the Avaya Aura® Contact Center (AACC) and Avaya 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 Media Server VM	Supported during Avaya 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 360	No	See Avaya Media Server VMware snapshot considerations on page 361
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 (guests) 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 and AMD AMD-V)

The first generation of hardware virtualization assistance includes VT-x from Intel and AMD-V from AMD. 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 EPT and AMD RVI)

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 both in AMD processors, where it is called Rapid Virtualization Indexing (RVI) or nested page tables (NPT), and 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 guest 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 Guest 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 guest 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.

Overview of commissioning 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 guest 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 BIOS 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 BIOS settings](#) on page 326.
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:
 - For Intel based hosts: Enable Intel virtualization (VT-x) and if available enable Extended Page Tables (EPT).
 - For AMD based hosts: Enable AMD virtualization (AMD-V) and if available enable Rapid Virtualization Indexing (RVI).

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 guest virtual machine, configure and use VMXNET 3 networking.
11. Using the vSphere client, configure each Contact Center guest virtual machine with the CPU, memory, and disk space required for your contact center configuration. For more information about the CPU, memory, hard disk, and networking requirements, see [Server Specifications](#) on page 305.
12. On each Contact Center guest virtual machine, completely disable time synchronization to the host time. During Contact Center commissioning, the Contact Center guest 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 guest virtual machine for Avaya Aura® Contact Center:
 - If you are installing a Contact Center application (CCMS, CCMA, CCT, LM or CCMM), configure disk partitions and install guest Windows Server 2008 Release 2 operating system.
 - If you are installing Avaya Media Server, configure disk partitions and install guest Red Hat Enterprise Linux operating system.
15. On each Avaya Aura® Contact Center guest virtual machine, perform the Contact Center server preparation procedures. For more information, see *Avaya Aura® Contact Center Installation* (44400-311).
16. Install Avaya Aura® Contact Center software on the guest 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 guest virtual machine.
20. Continue to monitor all the resources of the vSphere host server, focusing on CPU, memory, and disk drive resources.

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 resxtop, 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 guest (virtual machine) configuration settings.

Important:

Avaya Aura® Contact Center supports High Availability only where the Primary and Backup Avaya Media Servers are installed on physical servers. Virtualized Avaya Media Servers do not support High Availability.

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 *Consolidate* snapshots at the end of the maintenance window, before putting the Contact Center virtual machine back into production. For more information about consolidating snapshots, refer to VMware documentation.
- 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 2008 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 2008 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 *Avaya Aura® Contact Center Routine Maintenance* (44400-514).

Avaya 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 Media Server on VMware:

- Snapshots must be taken during an Avaya Media Server maintenance window. Do not take a snapshot of an Avaya 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 *Consolidate* snapshots at the end of the maintenance window, before putting the Avaya 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 Media Server database backup (and restore) procedures and practices. For more information, see *Avaya Aura® Contact Center Routine Maintenance* (44400-514).

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 VMkernel 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 guest 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 aborted 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.

Hyper-V support

Avaya Aura® Contact Center supports Microsoft Hyper-V.

The following table shows Avaya Aura® Contact Center Hyper-V support for each server type and platform.

Table 19: Avaya Aura® Contact Center Hyper-V support by server type

Voice Platform	Server type	Virtual OS	Support
SIP-enabled Avaya Aura® Unified Communications platform	Voice and Multimedia Contact Server without Avaya Media Server	Windows	No
	Voice Contact Server Only	Windows	Yes
	Multimedia Contact Server Only	Windows	Yes
	Voice and Multimedia Contact Server with Avaya Media Server	Windows	No
	Avaya Media Server	Linux	No
AML-based Avaya Communication Server 1000 (CS 1000)	Voice and Multimedia Contact Server without Avaya Media Server	Windows	No
	Voice Contact Server Only	Windows	Yes
	Multimedia Contact Server Only	Windows	Yes
	Knowledge Worker Server Only	Windows	Yes
Avaya Aura® Call Center Elite	AACC Multimedia Complement for Elite	Windows	No
No voice platform (No Switch configured)	Voice and Multimedia Contact Server with Avaya Media Server	Windows	No
All voice platform types	Network Control Center Server Only	Windows	Yes

Avaya Media Server is not supported on Microsoft Hyper-V.

Each supported Contact Center server type must be installed stand-alone in its own single virtual machine instance on Hyper-V.

Hyper-V disk controller support

Microsoft Hyper-V virtual machines use a virtual IDE controller for the Operating System disk partition, even when the underlying Hyper-V server hardware uses a SCSI disk controller. When you install Avaya Aura® Contact Center software on a physical server, the DVD installer *System Readiness Checks* utility examines the physical server hardware for suitability. When you install Avaya Aura® Contact Center software on a virtual machine, the DVD *System Readiness Checks* utility examines the virtual machine for suitability. Avaya Aura® Contact Center does not support IDE controllers. When installing Avaya Aura® Contact Center software on a Hyper-V virtual machine, the *System Readiness Checks* utility might display a “Hard drive type – IDE” warning message. You can ignore this warning if the underlying physical Hyper-V Server hardware uses one of the supported disk controllers: SCSI, SATA, or SAS.

Virtual Machine hardware requirements

Provision the Virtual Machine with the same (or higher) specification as is listed for the physical server, plus an additional CPU overhead of 15 percent over the recommended value in the physical server specification.

The Virtual Machine must have the same amount of allocated hard disk space as the equivalent physical server and the hard disk must have the same size partitions as the equivalent physical server. The networking requirements in Contact Center are the same as the networking requirement of each virtual machine.

You must configure the allocated memory on the Virtual Machine to support Contact Center. For more information, see [Server Specifications](#) on page 305.

Chapter 27: Common server requirements

This section specifies the server hardware and software requirements common to all Avaya Aura® Contact Center server types installed on the Microsoft Windows operating system.

The requirements in this section apply to the following Contact Center servers:

- Voice and Multimedia Contact Server with Avaya Media Server
- Voice and Multimedia Contact Server without Avaya Media Server
- Voice Contact Server Only
- Multimedia Contact Server Only
- Multimedia Complement for Avaya Aura® Call Center Elite
- No Switch Configured - Voice and Multimedia Contact Server with Avaya Media Server (Multimedia only)
- Network Control Center Server Only
- Knowledge Worker 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 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 Media Server on Linux server requirements, see [Avaya Media Server on Linux configuration requirements](#) on page 431.

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 2008 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 2008 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 the 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 2008 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 20: 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 2008 Release 2 Server operating system is installed here.
Application partition	typically D:	An additional NTFS partition on disk 0 or an NTFS partition on a different disk.
DVD ROM drive	typically E:	DVD ROM.
Database partition	typically F:	CCMS Database.
(Optional) Database partition	typically G:	Optional CCMM Database and multimedia attachments partition.

For more information about Avaya Aura® Contact Center server disk partition specifications, and to select a suitable server disk partition specifications for your servers, see [Server Specifications](#) on page 305.

Operating system requirements

The following table provides the operating system compatibility for Avaya Aura® Contact Center.

Table 21: Avaya Aura® Contact Center operating system requirements

Operating system	International versions supported	Minimum service pack required
Windows Server 2008 Release 2, Standard Edition and Enterprise Edition, 64-bit, Service Pack 1.	English French	Service Pack 1

Operating system	International versions supported	Minimum service pack required
 Note: Only the 64-bit version is supported.	German Italian 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 2008 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 Web site) 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 web site at <https://support.avaya.com/security>. From the Avaya Support web site, 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 www.avaya.com/support.

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 Web site at www.avaya.com/support.

Java Runtime Environment updates

Contact Center supports only specific versions of Java Runtime Environment (JRE). The Contact Center Installer installs a supported JRE version, and Contact Center service packs install required JRE updates. 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 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 2008 Release 2 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, 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.

The Contact Center supported antivirus products are:

- Symantec AntiVirus 11.0.5, 11.0.6, or 12
- McAfee 8.8
- Microsoft ForeFront 2010

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 Web site 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 and RAID-5. RAID technology provides disk data redundancy as well as error detection and correction. For maximum security and mission-critical solutions, Avaya recommends that all Contact Center servers contain a hardware RAID-1 controller with battery backup. Hardware RAID-1 and RAID-5 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.

Chapter 28: High Availability server requirements

Avaya Aura® Contact Center supports High Availability (HA) resiliency for Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), Contact Center Multimedia (CCMM), Avaya Media Server, and Contact Center Manager Administration (CCMA). 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. Avaya Aura® 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
- Warm standby High Availability

This section provides information about Standby server, Remote Geographic Node server, and network requirements.

This section also describes how to optimize the Mission Critical Contact Center High Availability (HA) feature for your network.

Mission Critical High Availability

Avaya Aura® Contact Center Mission Critical High Availability is supported with a number of Contact Center solutions running on the Avaya Aura® Unified Communications platform. While these Avaya Aura® Contact Center solutions are similar in behavior, differences are seen depending on the platform components of each solution. Avaya Aura® 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 6.2

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 that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Manager Administration (CCMA) configured as a High Availability pair.

- Two Multimedia Contact Servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA on a Voice and Multimedia Contact Server. You can use two Voice and Multimedia Contact Servers configured as a High Availability pair instead of two Voice Contact Servers and two Multimedia Contact Servers. A Voice and Multimedia Contact Server supports fewer agents than a separate Voice Contact Server and Multimedia Contact Server.
- Two or more Avaya Media Server Linux-based servers, configured as a High Availability pair. Avaya Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.
- Two Avaya Aura® Session Manager instances, Release 6.1 or 6.2.
- 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 that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), License Manager, and Contact Center Manager Administration (CCMA) configured as a High Availability pair.
- Two Multimedia Contact Servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA on a Voice and Multimedia Contact Server. You can use two Voice and Multimedia Contact Servers configured as a High Availability pair instead of two Voice Contact Servers and two Multimedia Contact Servers. A Voice and Multimedia Contact Server supports fewer agents than a separate Voice Contact Server and Multimedia Contact Server.
- Two or more Avaya Media Server Linux-based servers, configured as a High Availability pair. Avaya Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.
- One Avaya Aura® Session Manager (SM) instance.
- One Avaya Aura® Application Enablement Services (AES) server.
- One Avaya Aura® Communication Manager (CM) server.
- Redundant Ethernet switches.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

*** Note:**

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

To achieve Mission Critical High Availability using Midsize Enterprise you must have a SIP-enabled Contact Center with the following:

- Two Voice Contact Servers that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), License Manager, and Contact Center Manager Administration (CCMA) configured as a High Availability pair.
- Two Multimedia Contact Servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA on a Voice and Multimedia Contact Server. You can use two Voice and Multimedia Contact Servers configured as a High Availability pair instead of two Voice Contact Servers and two Multimedia Contact Servers. A Voice and Multimedia Contact Server supports fewer agents than a separate Voice Contact Server and Multimedia Contact Server.
- Two or more Avaya Media Server Linux-based servers, configured as a High Availability pair.
Avaya Media Server High Availability is supported only on Linux-based servers in Mission Critical High Availability solutions.
- Two Midsize Enterprise 6.2 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 Avaya Aura® Contact Center servers (CCMS, CCMA, CCT, and CCMM) 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 Aura® Agent Desktop clients must be registered in this domain, or in domains with a two-way trust relationship with this Contact Center server domain.

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

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

Contact Center Administrators use the active server in daily operation. Configuration changes made to the active system during normal operation are automatically copied to the standby applications, therefore the standby applications are configured and ready to take over processing from the active system. Statistical data is also automatically copied to the standby applications. Data is replicated to the standby applications 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 that include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT) and Contact Center Manager Administration (CCMA) configured as a High Availability pair.
- Optionally, two Multimedia Contact Servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA on a Voice and Multimedia Contact Server. You can use two Voice and Multimedia Contact Servers configured as a High Availability pair instead of two Voice Contact Servers and two Multimedia Contact Servers. 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 Avaya Aura® Contact Center servers (CCMS, CCMA, CCT, and CCMM) 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 Aura® Agent Desktop clients must be registered in this domain, or in domains with a two-way trust relationship with this Contact Center server domain.

One set of Avaya Aura® Contact Center applications (a CCMS, a CCT, and an optional CCMM) actively processes scripts and contacts. This set of applications is called the active set. Another set of Contact Center applications in the same contact center system, runs in hot-standby mode. This standby set of Contact Center applications monitors and shadows the active applications in the system and does not process calls. The standby CCMS monitors the active CCMS. The standby CCT monitors the active CCT. The standby CCMM monitors the active CCMM. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts.

Contact Center Administrators use the active server in daily operation. Configuration changes made to the active system during normal operation are automatically copied to the standby applications, therefore the standby applications are configured and ready to take over processing from the active system. Statistical data is also automatically copied to the standby applications. Data is replicated to the standby applications in real-time.

Warm standby High Availability

Avaya Aura® Contact Center supports the following Warm standby High Availability solutions.

Avaya Aura® Call Center Elite voice and Avaya Aura® Contact Center multimedia complement configuration:

- Two AACC Multimedia Complement for Elite servers configured as a High Availability pair.
- Avaya Aura® Call Center Elite.
- Redundant Ethernet switches.
- This configuration is supported only for Campus High Availability.

Avaya Aura® Contact Center Multimedia in standalone configuration:

- Two No Switch Configured — Voice and Multimedia Contact Server with Avaya Media Server servers configured as a High Availability pair.
- Redundant Ethernet switches.
- This configuration is supported only for Campus High Availability.

All of the above components must be in the same network subnet or campus network location.

Warm standby High Availability solutions do not support geographic redundancy.

Avaya Aura® Contact Center supports Warm standby High Availability (HA) resiliency for Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Multimedia (CCMM).

One set of Avaya Aura® Contact Center applications (a CCMS, a CCT, and an optional CCMM) actively processes scripts and contacts. This set of applications is called the active set. Another set of Contact Center applications in the same contact center system, runs in standby mode. This standby set of Contact Center applications monitors and shadows the active applications in the system and does not process calls. The standby CCMS monitors the active CCMS. The standby CCT monitors the active CCT. The standby CCMM monitors the active CCMM. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts.

Contact Center Administrators use the active server in daily operation. Configuration changes made to the active system during normal operation are automatically copied to the standby applications, therefore the standby applications are configured and ready to take over processing from the active system. Statistical data is also automatically copied to the standby applications. Data is replicated to the standby applications 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 (Avaya Aura® CM) 6.2, Avaya Aura® Session Manager (SM) 6.2, and Avaya Aura® Application Enablement Services (AES) 6.1.2.0.32 or 6.2.

OR

- Avaya Aura® Communication Manager (Avaya Aura® CM) 6.0.1, Avaya Aura® Session Manager (SM) 6.1, and Avaya Aura® Application Enablement Services (AES) 6.1.

OR

- Avaya Aura® Solution for Midsize Enterprise (ME) 6.2

*** Note:**

The Avaya Aura® Solution for Midsize Enterprise (ME) 6.2 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 Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).

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 22: Avaya Aura® Unified Communications platform HA support level summary

PABX	Release	HA Level	Agent experience after Contact Center switchover
Avaya Aura® CM/SM/AES	6.0.1/6.1/6.2	Mission Critical HA	Agent logon state is maintained.
ME	6.2	Mission Critical HA	Agent logon state is maintained.
Avaya Aura® Unified Communications Virtualized Environment (VE)	6.2	Contact Center supports High Availability without AES resiliency	Agent logon state is maintained.
! Important: If a Contact Center application or server fails, voice calls in progress between a customer and an agent are maintained in Mission Critical High Availability.			

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, calls in progress between a customer and an agent are maintained, 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 23: Avaya Communication Server 1000 High Availability support level summary

CS 1000 Release	HA Level	Agent experience after switchover
7.0, 7.5, 7.6	Hot-standby HA	Agents log back on.
! Important: If a Contact Center application or server fails, voice calls in progress between a customer and an agent are maintained in Hot-standby High Availability.		

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 24: Contact Center application High Availability support level summary

PABX	Release	AML/SIP	HA Level	Agent Experience after switchover
Avaya Aura® CM/SM/AES	6.0.1/6.1/6.2	SIP	Mission Critical HA	Agent logon state is maintained.
ME ^{Note 1}	6.2	SIP	Mission Critical HA	Agent logon state is maintained.
CS 1000	7.0, 7.5, 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.				

Table continues...

PABX	Release	AML/SIP	HA Level	Agent Experience after switchover
! Important: If a Contact Center application or server fails, voice calls in progress between a customer and an agent are maintained in High Availability solutions.				

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 guest (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 are used only to shadow data from the active server; they have no other responsibility. 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 patch level and the same operating system updates.

If the active and Remote Geographic Node 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 Remote Geographic Node servers must have the same VMware guest (virtual machine) configuration settings.

Campus network requirements

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.

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 is assigned a static IP address. After the active server in each replication pair is determined, 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 that active application using the Managed IP address. If the standby server takes over call processing and becomes the active application, it hosts this same Managed IP address. The active server stops hosting the Managed IP when it stops being the active server. When the standby server starts-up to take over call processing, it attaches the Managed IP address to its network interface.

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, 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 High Availability pair must be 172.1.1.Z. The network subnet IP address range is controlled by the subnet mask.

Dynamic Host Configuration Protocol (DHCP)

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.

Network resiliency

Use Link Aggregation Control Protocol (LACP) and NIC Teaming to eliminate network points of failure in the contact center solution.

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 balance. The process of grouping NICs is called teaming. By teaming more than one physical NIC to a logical NIC, high availability is maximized. If one NIC fails, the network connection does not cease and continues to operate on other NICs.

Typically, you configure Network Interface Card (NIC) teaming using hardware specific utilities supplied by your server or hardware manufacturer. For more information about configuring NIC teaming, see your server documentation.

Campus High Availability supports LAN environments where the round trip delay between the Active and Standby servers is less than 80ms, with less than 0.5% packet loss.

Geographic network requirements

In a Geographic High Availability environment the active and Remote Geographic Node servers are typically located in different subnets (WAN).

The main advantages of Geographic High Availability are:

- Support for database shadowing over WAN.
- Added resiliency and Disaster Recovery in the event of primary site failure.

Avaya recommends using Link Aggregation Control Protocol (LACP) and NIC Teaming to eliminate network points of failure in the contact center solution.

Dynamic Host Configuration Protocol (DHCP)

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.

Network resiliency

Use Link Aggregation Control Protocol (LACP) and NIC Teaming to eliminate network points of failure in the contact center solution.

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 balance. The process of grouping NICs is called teaming. By teaming more than one physical NIC to a logical NIC, high availability is maximized. If one NIC fails, the network connection does not cease and continues to operate on other NICs.

Typically, you configure Network Interface Card (NIC) teaming using hardware specific utilities supplied by your server or hardware manufacturer. For more information about configuring NIC teaming, see your server documentation.

Geographic High Availability supports WAN environments where the round trip delay between the Active and Remote Geographic Node servers is less than 80ms, with less than 0.5% packet loss.

Chapter 29: Voice and Multimedia Contact Server without Avaya Media Server configuration requirements

This section provides the configuration requirements for a Voice and Multimedia Contact Server without Avaya 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 Media Server is supported only on the Microsoft Windows Server 2008 Release 2 64-bit operating system.

Voice and Multimedia Contact Server without Avaya 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 Avaya Aura® 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 Avaya Aura® Agent Desktop, use the CCMM Administration utility to configure Avaya Aura® 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.

Common Server Requirements: The Voice and Multimedia Contact Server without Avaya Media Server specifications are in addition to the common server specifications. For more information, see [Common server requirements](#) on page 366.

Hardware requirements

The Voice and Multimedia Contact Server without Avaya Media Server hardware specification depends on your solution type, agent count, and call flow rate. You can install the Voice and Multimedia Contact Server without Avaya Media Server software on a physical server or on a virtual guest.

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 Media Server.

Table 25: Voice and Multimedia Contact Server without Avaya Media Server supported server specifications

Platform	Physical server			Virtual guest		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	No	Yes	Yes	No	No	Yes
CS 1000 AML	No	Yes	Yes	No	No	Yes

For more information about Avaya Aura® Contact Center server specifications, and to select a server specification suitable for your agent count and call flow rate, see [Server Specifications](#) on page 305.

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.
- **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 Aura® Agent Desktop is a client of Communication Control Toolkit so they support the same features.

! Important:

If your phone supports Multiple Appearance Reduction Prime (MARP) or 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 26: Basic Communication Control Toolkit and Avaya Aura® Agent Desktop functions

Event	SIP-enabled Avaya Aura® & CS 1000	AML-based CS 1000
Make Call	Yes	Yes
Hold Current Call	Yes The CS 1000 Swap Hold switch feature is not supported. For CS 1000, the Auto Hold Allowed (AHA) feature must be configured.	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 (up to six parties on CS 1000)	Yes (up to six parties)
Complete Conference Call	Yes	Yes
Call Forward	No	Yes
Cancel Call Forward	No	Yes
Join Conference	Yes, Avaya Aura® only	No
Deflect Calls	No	No

Table continues...

Event	SIP-enabled Avaya Aura® & CS 1000	AML-based CS 1000
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 DTMF is not supported in Knowledge Worker solutions.
Mute/Unmute	No	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 Aura® Agent Desktop and Communication Control Toolkit.

Table 27: Contact Center-specific functions

Event	SIP-enabled Avaya Aura® & CS 1000	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

Table continues...

Event	SIP-enabled Avaya Aura® & CS 1000	AML-based CS 1000
Agent Whisper	No	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 28: Communication Control Toolkit events

Event	SIP-enabled Avaya Aura® & CS 1000	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

Table continues...

Event	SIP-enabled Avaya Aura® & CS 1000	AML-based CS 1000
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)
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)

Table continues...

Variable	Description	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 Geographic Redundancy.
- `Avaya\Contact Center\Databases\ShadowJournals` folder is created during installation. This folder is used if Geographic Redundancy is configured and this server is running as the Redundant server.

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 Aura® Agent Desktop client computers do not support the following applications running concurrently with Avaya Aura® 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 Avaya Aura® 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* (44400-610) 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 373.

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 374.

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 Server 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*.
- 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 30: 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 2008 Release 2 64-bit 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.

Common Server Requirements: The Voice Contact Server specifications are in addition to the common server specifications. For more information, see [Common server requirements](#) on page 366.

Hardware requirements

The Voice Contact Server hardware 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 guest.

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 29: Voice Contact Server supported server specifications

Platform	Physical server			Virtual guest		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	Yes	Yes	Yes	Yes	Yes	Yes
CS 1000 AML	Yes	Yes	Yes	Yes	Yes	Yes

For more information about Avaya Aura® Contact Center server specifications, and to select a server specification suitable for your agent count and call flow rate, see [Server Specifications](#) on page 305.

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.
- **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 Aura® Agent Desktop is a client of Communication Control Toolkit so they support the same features.

Important:

If your phone supports Multiple Appearance Reduction Prime (MARP) or 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 30: Basic Communication Control Toolkit and Avaya Aura® Agent Desktop functions

Event	SIP-enabled Avaya Aura® & CS 1000	AML-based CS 1000
Make Call	Yes	Yes
Hold Current Call	Yes The CS 1000 Swap Hold switch feature is not supported. For CS 1000, the Auto Hold Allowed (AHA) feature must be configured.	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 (up to six parties on CS 1000)	Yes (up to six parties)
Complete Conference Call	Yes	Yes
Call Forward	No	Yes
Cancel Call Forward	No	Yes
Join Conference	Yes, Avaya Aura® only	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 DTMF is not supported in Knowledge Worker solutions.
Mute/Unmute	No	No
Consult	Yes	Yes (but must designate as transfer or conference)
Park/Unpark	No	No
Message Waiting Indicator	No	No

Table continues...

Event	SIP-enabled Avaya Aura® & CS 1000	AML-based CS 1000
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 Aura® Agent Desktop and Communication Control Toolkit.

Table 31: Contact Center-specific functions

Event	SIP-enabled Avaya Aura® & CS 1000	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	No	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 32: Communication Control Toolkit events

Event	SIP-enabled Avaya Aura® & CS 1000	AML-based CS 1000
Ringin 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
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 Aura® Agent Desktop client computers do not support the following applications running concurrently with Avaya Aura® 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 Avaya Aura® 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* (44400-610) 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 373.

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 374.

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 Server 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 31: 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 2008 Release 2 64-bit operating system. Multimedia Contact Server supports High Availability.

In a solution using one of these servers, agents download and install Avaya Aura® Agent Desktop software from this server.

In a solution where agents use Avaya Aura® 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 Avaya Aura® 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 Avaya Aura® 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 Avaya Aura® 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 Avaya Aura® Agent Desktop, use the CCMM Administration utility to configure Avaya Aura® 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.

Common Server Requirements: The Multimedia Contact Server specifications are in addition to the common server specifications. For more information, see [Common server requirements](#) on page 366.

Hardware requirements

The Multimedia Contact Server hardware 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 guest.

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 33: Multimedia Contact Server supported server specifications

Platform	Physical server			Virtual guest		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	Yes	Yes	Yes	Yes	Yes	Yes
CS 1000 AML	Yes	Yes	Yes	Yes	Yes	Yes

For more information about Avaya Aura® Contact Center server specifications, and to select a server specification suitable for your agent count and call flow rate, see [Server Specifications](#) on page 305.

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)

Table continues...

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 Geographic Redundancy.
- `Avaya\Contact Center\Databases\ShadowJournals` folder is created during installation. This folder is used if Geographic Redundancy is configured and this server is running as the Redundant server.

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 Aura® Agent Desktop client computers do not support the following applications running concurrently with Avaya Aura® 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 Avaya Aura® 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* (44400-610) 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 373.

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 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*.
- 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 Server 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 32: Voice and Multimedia Contact Server with Avaya Media Server configuration requirements

This section provides the configuration requirements for a Voice and Multimedia Contact Server with Avaya 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 Media Server (Avaya MS)

Voice and Multimedia Contact Server with Avaya Media Server is supported only on the Microsoft Windows Server 2008 Release 2 64-bit operating system.

The Voice and Multimedia Contact Server with Avaya 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 Avaya Aura® 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 Avaya Aura® Agent Desktop, use the CCMM Administration utility to configure Avaya Aura® 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.

Common Server Requirements: The Voice and Multimedia Contact Server with Avaya Media Server specifications are in addition to the common server specifications. For more information, see [Common server requirements](#) on page 366.

Hardware requirements

The Voice and Multimedia Contact Server with Avaya Media Server hardware specification depends on your solution type, agent count, and call flow rate.

* Note:

Voice and Multimedia Contact Server with Avaya Media Server is not supported on a virtual guest.

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 Media Server software.

Table 34: Voice and Multimedia Contact Server with Avaya Media Server supported server specifications

Platform	Physical server			Virtual guest		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	No	Yes	Yes	No	No	No

You can buy a Voice and Multimedia Contact Server with Avaya Media Server as a hardware appliance. The AACC Hardware Appliance comprises a Dell™ R620™ server with the Windows

Server 2008 operating system and the AACC software preloaded. The Hardware Appliance has a fixed specification.

For more information about Avaya Aura® Contact Center server specifications, and to select a server suitable for your agent count and call flow rate, see [Server Specifications](#) on page 305.

Avaya Media Server software components

Avaya Media Server is a software-based media processing platform. The Avaya Media Server architecture is uniquely scalable for all core functions of the platform, including media processing, signaling, application execution, and content management.

The Avaya Aura® Contact Center DVD includes the core Avaya Media Server software and an additional component, Contact Center Services for Avaya Media Server. On the Linux operating system, the Avaya Media Server installer and the Contact Center Services for Avaya Media Server installer are separate executables.

Contact Center Services for Avaya Media Server provides the applications needed for the Agent Greeting feature. This feature allows agents to pre-record their personal greetings. The feature plays the greeting automatically when an agent answers a call.

Avaya Media Server media files and media management

Media files are WAV audio files that contain speech, music, or signaling tones. Avaya Media Server supports custom (customer generated) media files and default (canned) media files. You configure the custom media files using the Avaya Media Server Element Manager. You update and configure the default media files directly in the locale specific folders on the Avaya Media Server.

Content Store

The Avaya Media Server Content Store provides a persistent storage capability for configuration data and media files. You use the Avaya Media Server Element Manager Web administration utility to configure and manage the contents of the Content Store. If you have more than one Avaya Media Server, you can designate one server to be the primary Avaya Media Server. You can then configure the other Avaya Media Servers to replicate (copy) the configuration data and media files from the Content Store on the primary Avaya Media Server. This configures all of the Avaya 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 Media Server fails the remaining Avaya Media Servers are configured correctly and can continue processing media and contact center calls.

Custom media

Avaya Media Server stores (customer generated) custom media files in a media Content Store. Typically, a customer records their own announcements and stores the WAV media file recordings

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

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

Custom media organization

In Avaya Media Server Element Manager (EM), you organize custom media 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 must create one locale-specific content group for treatments such as RAN.

Avaya 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
ko_kr	Korean	Korea
pt_br	Portuguese	Brazil
ru_ru	Russian	Russia
zh_cn	Chinese (Simplified)	China
zh_tw	Chinese (Simplified)	Taiwan

You can create one or more additional content groups for music. Typically you store different types of music media in different content groups. 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 Media Server locale-specific content group. To use scripted

music in OD flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the Avaya Media Server content groups containing the music files. The OD flow applications or scripts reference these routes to access the treatment files and scripted music on the Avaya Media Server.

The following example shows the structure of a content namespace for a contact center based in Canada, which uses English recorded announcements, and has three optional music types; folk, jazz, and rock. The SIP domain for the contact center is ocs-nmclab.com. The locale configured on the CCMS server is en_ca.

The media content namespace structure is as follows:

ocs-nmclab.com <= media content namespace, matches SIP domain name

- en_ca <= locale-specific media content group (announcements)
- folk <= media content group (folk music)
- jazz <= media content group (jazz music)
- rock <= media content group (rock music)

Default media files

Contact Center Avaya 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 ringback 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 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_xx.wav) where xx is the country portion of the locale (for example, ringback_us.wav, ringback_ru.wav)

The default media files are stored in the Operating System file structure (not in the Avaya Media Server content namespace). The canned media files are stored in Linear 16-bit PCM recording format.

If you choose to create your own recordings, you must replace the existing default media files with files of the exact same name. For example, if you choose to record your own media files for single digit numerals, then you must save the files as one.wav and two.wav to match the existing default media file names. Then you replace the existing default media files with the media files of your own recordings. You must then delete the existing Avaya Media Server transcoded output files. For example, if you are using PCMA transcoding, delete the one.wav and two.wav media files from the locale-specific PCMA folder. This forces Avaya Media Server to pick up your new Linear 16-bit PCM recording and generate a new transcoded output file of your recording.

Default media files are not stored in the Avaya Media Server Content Store, and are therefore not replicated to other Avaya Media Servers. If you update the canned or default media files on one Avaya Media Server, you must copy the updated default media files to all other Avaya Media Servers.

The Asian 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

All audio media files must have a .wav file name extension, for example hatchi.wav, jiu.wav, and seven.wav.

Default media organization

Each Avaya Media Server installation includes a number of default (canned) media files. These default media files are stored in a country and locale specific folder on the Avaya Media Server.

On a Windows operating system, the default location for the default media files is:

```
D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\Announcements
\contactcenter\default\xx\yy\l16
```

Where xx is the country portion of the locale and yy is the language portion of the locale.

On a Linux operating system server, the default location for the default media files is:

```
/opt/avaya/ma/MAS/platdata/Announcements/contactcenter/default/xx/yy/l16
```

Where xx is the country portion of the locale and yy is the language portion of the locale.

For example, the Linux operating system Avaya Media Server directory locations for Canadian English and French are:

```
/opt/avaya/ma/MAS/platdata/Announcements/contactcenter/default/ca/en/l16
```

```
/opt/avaya/ma/MAS/platdata/Announcements/contactcenter/default/ca/fr/l16
```

Media file formats

Avaya Media Server provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbts/sec. Create your announcement and music media files with this encoding before copying them onto the Avaya Media Server server.

Communication Control Toolkit supported SIP functionality

The tables in this section indicate which functions are supported by Communication Control Toolkit. Avaya Aura® 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 35: Basic Communication Control Toolkit and Avaya Aura® Agent Desktop functions

Event	SIP-enabled Avaya Aura® and CS 1000
Make Call	Yes
Hold Current Call	Yes The CS 1000 Swap Hold switch feature is not supported. For CS 1000, the Auto Hold Allowed (AHA) feature must be configured.
Unhold Call	Yes (Retrieve Call)
Drop Current Call (Release)	Yes
Blind Transfer Call	No
Initiate Supervised Transfer	Yes
Complete Transfer	Yes
Initiate Conference Call	Yes (up to six parties on CS 1000)
Complete Conference Call	Yes
Call Forward	No
Cancel Call Forward	No
Join Conference	Yes, (Avaya Aura® only)
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

Table continues...

Event	SIP-enabled Avaya Aura® and CS 1000
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 Aura® Agent Desktop and Communication Control Toolkit .

Table 36: Contact Center-specific functions

Event	SIP-enabled Avaya Aura® and CS 1000
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
Work Ready Key support	No
Agent Whisper	No
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 37: Communication Control Toolkit events

Event	SIP-enabled Avaya Aura® and CS 1000
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
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

Table continues...

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 Geographic Redundancy.
- `Avaya\Contact Center\Databases\ShadowJournals` folder is created during installation. This folder is used if Geographic Redundancy is configured and this server is running as the Redundant server.

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 Aura® Agent Desktop client computers do not support the following applications running concurrently with Avaya Aura® 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 Avaya Aura® 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* (44400-610) 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 373.

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 Media Server antivirus software

This section describes the Voice and Multimedia Contact Server with Avaya Media Server antivirus software requirements.

For antivirus software requirements, see [Additional guidelines for the use of antivirus software](#) on page 374.

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 Server 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*.
- 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 Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

Avaya 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 Media Server in the default location, adjust these file and folder paths to match your actual installation.

Chapter 33: Avaya Media Server on Linux configuration requirements

This section provides the configuration requirements for an Avaya Media Server Linux server. Each SIP-enabled contact center requires one or more Avaya Media Server in the solution. Avaya Media Server supports SIP-enabled voice contact routing, and it provides conferencing and Agent Greeting capabilities in SIP-enabled contact centers.

Avaya Media Server is supported only in SIP-enabled contact centers.

In an Avaya Aura® Contact Center solution, Avaya 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 Media Server Release 7.6 is supported on the Red Hat Enterprise Linux 6.4 64-bit operating system. In a Contact Center High Availability solution, Avaya Media Server is supported only when installed standalone on a Linux operating system.

Avaya Aura® Contact Center does not support standalone Avaya Media Server on Windows for new installations.

Avaya Media Server software components

Avaya Media Server is a software-based media processing platform. The Avaya Media Server architecture is uniquely scalable for all core functions of the platform, including media processing, signaling, application execution, and content management.

The Avaya Aura® Contact Center DVD includes the core Avaya Media Server software and an additional component, Contact Center Services for Avaya Media Server. On the Linux operating system, the Avaya Media Server installer and the Contact Center Services for Avaya Media Server installer are separate executables.

Contact Center Services for Avaya Media Server provides the applications needed for the Agent Greeting feature. This feature allows agents to pre-record their personal greetings. The feature plays the greeting automatically when an agent answers a call.

Licensing requirements

Avaya Media Server requires licenses for Contact Center Services for Avaya Media Server, and optionally for the Agent Greeting feature.

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 Media Server. When Avaya Aura® Contact Center uses WebLM licensing, Avaya Media Server does not require a license file or any specific licensing configuration. Do not configure WebLM licensing on Avaya Media Server servers.

Hardware requirements

The Avaya Media Server hardware 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 Media Server software standalone on the following server specifications.

Table 38: Avaya Media Server supported server specifications

Platform	Physical server			Virtual guest		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	No	Yes	Yes	No	No	Yes
Avaya MS in a HA pair	No	No	Yes	No	No	No

For more information about Avaya Media Server standalone server specifications, and to select a server specification suitable for your agent count and call flow rate, see [Server Specifications](#) on page 366.

For information about Avaya Media Server and Avaya Aura® Contact Center virtualized on one VMware host server, see [Avaya Media Server and Contact Center on one VMware host](#) on page 330.

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 373.

Antivirus software

For Avaya Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

Avaya 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 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 374.

Chapter 34: Multimedia Complement for Elite server configuration requirements

This section provides the configuration requirements for a Multimedia Complement for Elite server. Install this server to add multimedia contact routing support to a new or existing Avaya Aura Call Center Elite voice-based solution. This server supports contact routing for Web chat, SMS text messaging, and email messages, with additional support for peer-to-peer Instant Messaging (IM). Contact Center Multimedia support adds additional communication channels for customers; improving productivity, responsiveness, and flexibility.

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)

The Multimedia Complement for Elite server is supported only on the Microsoft Windows Server 2008 Release 2 64-bit operating system.

The Multimedia Complement for Elite 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.

In a solution using one of these servers, agents download and install Avaya Aura® Agent Desktop software from this server.

Common Server Requirements: The Multimedia Complement for Elite server specifications are in addition to the common server specifications. For more information, see [Common server requirements](#) on page 366.

Hardware requirements

The Multimedia Complement for Elite server hardware specification depends on your solution type, agent count, and call flow rate. You can install Multimedia Complement for Elite software on a physical server or on a virtual guest.

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 Complement for Elite.

Table 39: Multimedia Complement for Elite supported server specifications

Platform	Physical server			Virtual guest		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Elite	No	Yes	Yes	No	Yes	Yes

For more information about Avaya Aura® Contact Center server specifications, and to select a server suitable for your agent count and call flow rate, see [Server Specifications](#) on page 305.

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 Geographic Redundancy.

- Avaya\Contact Center\Databases\ShadowJournals folder is created during installation. This folder is used if Geographic Redundancy is configured and this server is running as the Redundant server.

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 Aura® Agent Desktop client computers do not support the following applications running concurrently with Avaya Aura® 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 Avaya Aura® 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* (44400-610) 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 373.

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 Complement for Elite server antivirus software

This section describes the Multimedia Complement for Elite server antivirus software requirements.

For antivirus software requirements, see [Additional guidelines for the use of antivirus software](#) on page 374.

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 Server 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.
- 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 35: No Switch Configured Multimedia Only configuration requirements

This section provides the configuration requirements for a No Switch Configured Multimedia Only server. Install this server to provide multimedia contact routing. This server supports contact routing for web communications, fax messages, SMS text messaging, and email messages, with additional support for peer-to-peer Instant Messaging (IM). Choose this server type when there is no existing voice-based call center, or when multimedia integration with a voice contact center is not required.

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 Media Server (Avaya MS)

A No Switch Configured Multimedia Only server is supported only on the Microsoft Windows Server 2008 Release 2 64-bit operating system.

Avaya Media Server High Availability is not supported on the Windows operating system. Avaya Media Server High Availability is supported only on the Linux operating system. If you plan to implement High Availability for the No Switch Configured Multimedia Only solution, you must uninstall Avaya Media Server software from both the primary and the backup Multimedia Only servers.

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.

In a solution using one of these servers, agents download and install Avaya Aura® Agent Desktop software from this server.

Common Server Requirements: The No Switch Configured Multimedia Only server specifications are in addition to the common server specifications. For more information, see [Common server requirements](#) on page 366.

Hardware requirements

The No Switch Configured Multimedia Only server hardware specification depends on your solution type, agent count, and call flow rate.

*** Note:**

The No Switch Configured Multimedia Only software is not supported on a VMware guest.

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 No Switch Configured Multimedia Only.

Table 40: No Switch Configured Multimedia Only supported server specifications

Platform	Physical server			Virtual guest		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
No Switch	No	Yes	Yes	No	No	No

For more information about Avaya Aura® Contact Center server specifications, and to select a server specification suitable for your agent count and call flow rate, see [Server Specifications](#) on page 305.

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)

Table continues...

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 Geographic Redundancy.
- `Avaya\Contact Center\Databases\ShadowJournals` folder is created during installation. This folder is used if Geographic Redundancy is configured and this server is running as the Redundant server.

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 Aura® Agent Desktop client computers do not support the following applications running concurrently with Avaya Aura® 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 Avaya Aura® 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* (44400-610) 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 373.

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.

No Switch Configured Multimedia Only antivirus software

This section describes the No Switch Configured Multimedia Only server antivirus software requirements.

For antivirus software requirements, see [Additional guidelines for the use of antivirus software](#) on page 374.

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 Server 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.
- 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 Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

Avaya 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 Media Server in the default location, adjust these file and folder paths to match your actual installation.

Chapter 36: 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 2008 Release 2 64-bit 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. For example, in a network with Avaya Aura® Contact Center Release 6.3 and Avaya Aura® Contact Center Release 6.2 nodes, the NCC must be Release 6.3. All nodes in the network must be Avaya Aura® Contact Center Release 6.2 or later.

Common Server Requirements: The Network Control Center server specifications are in addition to the common server specifications. For more information, see [Common server requirements](#) on page 366.

Hardware requirements

The Network Control Center server hardware 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 guest.

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 41: Network Control Center supported server specifications

Platform	Physical server			Virtual guest		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
Aura SIP	Yes	Yes	Yes	Yes	Yes	Yes
CS 1000 AML	Yes	Yes	Yes	Yes	Yes	Yes

For more information about Avaya Aura® Contact Center server specifications, and to select a server specification suitable for your agent count and call flow rate, see [Server Specifications](#) on page 305.

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 373.

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 374.

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 Server 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 37: Knowledge Worker Server configuration requirements

This section provides the configuration requirements for a Knowledge Worker Server. Install this server to provide Computer-Telephony Integration (CTI) functionality and call data handling capabilities.

Knowledge Worker Server is supported only in Avaya Communication Server 1000 AML-based solutions. Knowledge Worker solutions support only voice calls, they do not support multimedia contacts. Knowledge Worker solutions do not support routed voice contacts or skill-based routing. A Knowledge Worker terminal cannot log on to an ACD queue or answer calls routed to a queue. A Knowledge Worker terminal can make and answer regular calls.

This server includes the following Avaya Aura® Contact Center components:

- Communication Control Toolkit (Knowledge Worker)
- Contact Center License Manager

Knowledge Worker Server is supported only on the Microsoft Windows Server 2008 Release 2 64-bit operating system.

Knowledge Worker Server does not support High Availability.

Common Server Requirements: The Knowledge Worker Server specifications are in addition to the common server specifications. For more information, see [Common server requirements](#) on page 366.

Hardware requirements

The Knowledge Worker Server hardware specification depends on your solution type, agent count, and call flow rate. You can install Knowledge Worker Server software on a physical server or on a virtual guest.

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 Knowledge Worker Server.

Table 42: Knowledge Worker Server supported server specifications

Platform	Physical server			Virtual guest		
	Entry-level	Mid-range	High-end	Entry-level	Mid-range	High-end
CS 1000 AML	Yes	Yes	Yes	Yes	Yes	Yes

For more information about Avaya Aura® Contact Center server specifications, and to select a server specification suitable for your agent count and call flow rate, see [Server Specifications](#) on page 305.

Communication Control Toolkit Knowledge Worker supported functionality

The tables in this section indicate which functions are supported by the Knowledge Worker version of Communication Control Toolkit.

Important:

If your phone supports Multiple Appearance Reduction Prime (MARF) or Multiple Appearance Directory Number (MADN) you must disable the configurations. These configurations are not supported in Communication Control Toolkit.

The following tables list the basic Communication Control Toolkit call control functions.

Table 43: Basic Communication Control Toolkit functions

Event	Avaya Communication Server 1000 (AML-based)
Make Call	Yes
Hold Current Call	Yes The CS 1000 Swap Hold switch feature is not supported.
Unhold Call	Yes (Retrieve Call)
Drop Current Call (Release)	Yes
Blind Transfer Call	Yes
Initiate Supervised Transfer	Yes
Complete Transfer	Yes
Initiate Conference Call	Yes (up to six parties)
Complete Conference Call	Yes
Call Forward	Yes
Cancel Call Forward	Yes
Join Conference	No

Table continues...

Event	Avaya Communication Server 1000 (AML-based)
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)	Yes (on Agent Terminals only)
Get/Set UUI	No (UUI attached as call data)
Send DTMF (for example, credit card number to IVR)	Yes DTMF is not supported in Knowledge Worker solutions.
Mute/Unmute	No
Consult	Yes (but must designate as transfer or conference)
Park/Unpark	No
Message Waiting Indicator	No
HER (Host Enhanced Routing)	Yes
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.

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 373.

Knowledge Worker Server antivirus software

This section describes the Knowledge Worker Server antivirus software requirements.

For antivirus software requirements, see [Additional guidelines for the use of antivirus software](#) on page 374.

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):

- The folder where you store Server 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.

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.

Communication Control Toolkit and Avaya Communication Server 1000 Telephony Manager on the ELAN subnet

In situations where both Communication Control Toolkit and Communication Server 1000 Telephony Manager are present, take extra care in the treatment of the ELAN subnet. When connecting the ELAN subnet to a router, follow the Communication Server 1000 Telephony Manager strict guidelines for filtering and routing. Your configuration must meet the requirements for the Communication Server 1000 Telephony Manager. *Communication Server 1000M and Meridian 1 Large System Planning and Engineering* (NN43021-220) prescribes ELAN engineering details for Contact Center application engineering.

The ELAN subnet is designed and tested for inter-Avaya product communications. These external communications over the ELAN subnet, therefore, present an unknown factor and thereby potential negative impact to the overall operation of the telephone switch and auxiliary processors.

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.

Knowledge worker environment requirements

In a knowledge-worker environment, Communication Control Toolkit communicates on the contact center subnet and, in turn, the ELAN subnet to the switch.

Chapter 38: 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
- Multimedia Complement for Elite
- No Switch Configured Multimedia only
- Network Control Center Server

The following Avaya Aura® Contact Center servers require one or more browser-based administration client computer:

- Knowledge Worker Server
- Avaya 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 44: Administration client hardware requirements for Windows XP and Windows Vista

Hardware item	Minimum requirements	Additional information
CPU	Intel-based CPU - Pentium IV 1.8GHz	Dual- and quad-CPU systems are supported with or without Hyperthreading enabled. AMD processors of the same or higher specification are also supported. Unsupported processors include Intel Celeron, and Intel Itanium (IA64) processors.
RAM	1 GB	—
Hard disk space	60 GB	60 GB is recommended only to store large reports.
Hard disk partitioning	No specific partitioning requirements	—
Hard disk type	IDE/SCSI Bus for hard drives	—
Hard disk speed	2.5 inch disk minimum speed: 10000 RPM 3.5 inch disk minimum speed: 7200 RPM	—
DVD ROM	One dual-layer DVD ROM drive	—
Network interface	One network interface card	—
Video card	One video card and monitor	1024*768 pixels minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—

Table 45: Administration client hardware requirements for Windows 7 and Windows 8.1

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. These CPU features are required to run Microsoft Windows 7.0 and Microsoft Windows 8.1. Dual- and quad-CPU systems are supported with or without Hyperthreading enabled. AMD processors of the same or higher specification are also supported.

Table continues...

Hardware item	Minimum requirements	Additional information
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 46: Administration client operating system requirements

Operating system	International versions supported (See Note)	Minimum service pack
Windows XP Professional	English French German Italian LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese	Service Pack 2 or later

Table continues...

Operating system	International versions supported (See Note)	Minimum service pack
	Japanese Korean	
Windows Vista Business 32-bit Windows Vista Enterprise 32-bit	English	SP1 or later
Windows 7 (32-bit and 64-bit)	English	
Windows Server 2008 Release 2 Standard Edition and Enterprise Editions 64-bit	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)	
Windows 8.1 (32-bit and 64-bit)	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)	
 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 a 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.

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 2008 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. For more information about manually installing ActiveX controls, see *Avaya Aura® Contact Center Commissioning* (44400-312).

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. For more information on how to configure your Citrix server to publish ADD as a published application, or how to configure your Citrix server to allow users to access CCMA, see *Avaya Aura® Contact Center Installation* (44400-311).

Contact Center Manager Administration and Agent Desktop Displays are supported only with the following versions of Citrix server:

- Citrix Presentation Server 4.5
- Citrix XenApp 6.0
- Citrix XenApp 6.5

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 Aura® 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.

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 8.0 (32-bit version only), 9.0 (32-bit version only), 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.

Chapter 39: Agent Desktop client requirements

This section provides the requirements for the Avaya Aura® Agent Desktop client computers. Avaya Aura® 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 Aura® Agent Desktop. You can use the click-once deployment or an MSI file. With a click-once deployment, agents download and install Avaya Aura® 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 Aura® Agent Desktop software from the Voice and Multimedia Contact Server.
- In a large solution using a Multimedia Contact Server, agents download and install Avaya Aura® Agent Desktop software from the Multimedia Contact Server.
- In an Elite Complement solution, agents download and install Avaya Aura® Agent Desktop software from the Multimedia Complement for Elite server.
- In a No Switch Configured multimedia only solution, agents download and install Avaya Aura® Agent Desktop software from the No Switch Configured Voice and Multimedia Contact Server.

In a deployment using an MSI file, administrators can push Avaya Aura® Agent Desktop to agent PCs using a silent install.

 Note:

Agent Desktop does not support Network Address Translation (NAT).

Avaya Aura® Agent Desktop localized languages

Avaya Aura® 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 Aura® 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 47: Agent Desktop client hardware requirements for Windows XP and Windows Vista

Hardware item	Minimum requirements	Additional information
CPU	Intel-based CPU - Pentium III 733 MHz	Pentium IV, Intel Xeon (32- and 64-bit), Dual core Xeon and Intel Xeon DP are supported.

Table continues...

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. Unsupported processors include Intel Celeron, and Intel Itanium (IA 64) processors.
RAM	1 GB	2 GB minimum is required, if you run other memory intensive applications at the same time as Agent Desktop.
Hard disk space	> 4 GB	—
Hard disk partitioning	No specific partitioning requirements	—
Hard disk type	IDE/SCSI Bus for hard drives	—
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	Video card and monitor	1024 x 768 pixels minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—
Serial ports	Not required	—

Table 48: Agent Desktop client hardware requirements for Windows 7 and Windows 8.1

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. These CPU features are required to run Microsoft Windows 7.0 and Microsoft Windows 8.1. Dual- and quad-CPU systems are supported with or without Hyperthreading enabled.

Table continues...

Hardware item	Minimum requirements	Additional information
		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 Aura® Agent Desktop client computers.

Table 49: Avaya Aura® Agent Desktop client computer operating system requirements

Operating system	International versions supported	Minimum service pack
Microsoft Windows XP Professional	English French German Italian LA Spanish Brazilian Portuguese Russian	Service Pack 2 or later

Table continues...

Operating system	International versions supported	Minimum service pack
	Simplified Chinese Traditional Chinese Japanese Korean	
Microsoft Windows Vista Business	English	Service Pack 1 or later
Microsoft Windows Vista Enterprise	English	Service Pack 1 or later
Microsoft Windows 7 (32-bit and 64-bit) ^{Note 1}	English	—
Microsoft Windows 8.1 (32-bit and 64-bit) ^{Note 2}	English French German Italian LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese Korean	—
Note 1: If you are using Agent Desktop in <i>My Computer</i> mode on a client computer with the Microsoft Windows 7 operating system, you must install Windows 7 Service Pack 1 or later. Note 2: Windows 8.1 environment does not support the <i>My Computer</i> mode in Agent Desktop, since embedded phone operation is not supported in Windows 8.1.		

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 (Avaya Aura® CM), 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:

$$n_{\text{average}} = \text{Roundup}(C / 3600)$$

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:

$$n_{\text{active}} = \text{Roundup}(F * C / 3600)$$

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
3Mbps	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:

$N_{\max} = 40$

$c = 380 \text{ multimedia contacts} + 200 \text{ voice contacts} = 580 \text{ per hour.}$

$c = 580.$

$\text{avg\_contact\_size} = 10\text{KBytes} = 80\text{Kb}$

$\text{avg\_att\_size} = 0\text{KBytes}$

Calculation:

As $N_{\max}$ is less than 50, set $F = 10$

The guidance on minimum bandwidth is therefore

$n_{\text{active}} = 10 * 580 / 3600 = 1.61$

$BWMM_{\min} = n_{\text{active}} * ((\text{avg\_contact\_size} * 64) + 2000) + (\text{avg\_att\_size} * (\text{att\_rate\_in} + \text{att\_rate\_out}) / 100)$

$BWMM_{\min} = 1.61 * ((80 * 64) + 2000) + (0)$

$BWMM_{\min} = 11463.2\text{Kbps}$

$11463.2\text{Kbps} / 1024 = 11.192\text{Mbps}$

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

$\text{avg\_session\_length}$ (Average length in seconds of IM session) = 240

Data size: 50 Kbps per active IM contact

Network bandwidth requirement:

$\text{Bandwidth} = (c * 50\text{Kbps} * \text{avg\_session\_length}) / 3600$

$\text{Bandwidth} = (200 * 50\text{Kbps} * 240) / 3600$

$\text{Bandwidth} = 666 \text{ Kbs} = .67 \text{ Mbps}$

$\text{Bandwidth} = 0.67 \text{ Mbps}$

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 Aura® 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.

Agent Desktop client requirements

This customer is using IM, Presence and Web statistics. Agents are not using Pull Mode.

Example contact center data:

```
Nmax = 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:

$n_{active} = \text{Roundup}(F * C / 3600)$

$n_{active} = 3 * 2000 / 3600 = 1.666$

$BWMM_{min} = n_{active} * ((avg\_contact\_size * 64) + 2000) + (avg\_att\_size * (att\_rate\_in\% + att\_rate\_out\%)/100)$

$BWMM_{min} = 1.666 * ((160 * 64) + 2000) + (800 * 0.2)$

$BWMM_{min} = 20658.4\text{Kbps}$

$20658.4\text{Kbps} / 1024 = 20.17\text{Mbps}$

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:

$\text{Bandwidth} = (c * 50\text{Kbps} * avg\_session\_length) / 3600$

$\text{Bandwidth} = (500 * 50\text{Kbps} * 240) / 3600$

$\text{Bandwidth} = 1666.6\text{ Kbs} = 1.67\text{ Mbps}$

$\text{Bandwidth} = 1.67\text{ Mbps}$

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:

$\text{Bandwidth} = (N * 7\text{Kb} * avg\_pres) / 3600$

$\text{Bandwidth} = (100 * 7\text{Kb} * 6000) / 3600$

$\text{Bandwidth} = 1166.6\text{Kbps} = 1.17\text{ Mbps}$

$\text{Bandwidth} = 1.17\text{ Mbps}$

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:
 $\text{Bandwidth} = (1280 * \text{avg\_search} * N) / 3600$
 $\text{Bandwidth} = (1280 * 12 * 100) / 3600$
 $\text{Bandwidth} = 426.6 \text{ Kbps}$
 $\text{Bandwidth} = 0.427 \text{ Mbps}$

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:
 $\text{Bandwidth} = (3.2 \text{ Kb} * 50 * 100) / 60$
 $\text{Bandwidth} = 266 \text{ Kbps} = .266 \text{ Mbps}$
 $\text{Bandwidth} = 0.266 \text{ Mbps}$

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)

VMware Horizon View VDI support

Avaya Aura® 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 Aura® 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 Aura® 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 Aura® 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 thick client software on the client computer.
4. Create a template and snapshot of this Agent Desktop master computer.
5. Using VMware Horizon View, add one or 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 Aura® Agent Desktop, you must use a desk phone. The Avaya Aura® Agent Desktop *My Computer* embedded softphone mode is not supported in virtualized desktop deployments.

Client Citrix support

Agent Desktop is supported 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 which are available on the Windows Server 2008 operating system of the Citrix server.

On the Contact Center Multimedia (CCMM) server the Avaya Aura® Agent Desktop folder is typically located in:

D:\Avaya\Contact Center\Multimedia Server\Agent Desktop\client folder.

This folder contains the entire Agent Desktop application. You can copy this folder onto any client computer and run Agent Desktop by clicking `AAAD.exe`. Copy this folder on the CCMM server to the 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. For more information on how to configure your Citrix server to publish Agent Desktop as a published application, see *Avaya Aura® Contact Center Installation* (44400-311).

The Citrix server publishing Agent Desktop must be located in the same Local Area Network (LAN) as the Contact Center Multimedia server.

Agent Desktop is supported only with the following versions of Citrix server:

- Citrix Presentation Server 4.5
- Citrix XenApp 6.0
- Citrix XenApp 6.5

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.

Citrix deployments of Agent Desktop are supported with Avaya Communication Server 1000 AML-based Offsite Agent. Application Module Link (AML) is an internal protocol used by Avaya Aura® Contact Center to communicate directly with Avaya Communication Server 1000.

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.

Agent Desktop thick client deployment

If you do not want to use the click-once features of Avaya Aura® Agent Desktop, it is possible to deploy it as a thick client. This differs from the click-once deployment method of installing and starting Agent Desktop by entering a URL address in a Web browser. The Agent Desktop thick

client deployment requires you to manually copy the contents of the `Avaya\Contact Center\Multimedia Server\Agent Desktop\client` folder from your Avaya Aura® Contact Center server to each client computer. Launch Agent Desktop using the `CCAD.exe` file located in the `Avaya\Contact Center\Multimedia Server\Agent Desktop\client` folder.

The required folder is located on the Contact Center server that Contact Center Multimedia is installed on.

If you deploy Agent Desktop as a thick client, you must consider the administrative tasks required due to the limitations of this type of deployment.

- You must manually install all required prerequisites on each client computer. Install the Agent Desktop prerequisites using the `setup.exe` file located in the `Avaya\Contact Center\Multimedia Server\Agent Desktop\` folder.
- All Contact Center client computers must contain the `Avaya\Contact Center\Multimedia Server\Agent Desktop\client` folder. Use, for example, a Systems Management Server (SMS) to allow client computers to access this folder.
- All agents must launch Agent Desktop using the `CCAD.exe` file located in the local copy of the `Avaya\Contact Center\Multimedia Server\Agent Desktop\client` folder. Agents must not launch Agent Desktop from within a Web browser or from a shortcut on the client computer, as this initiates a click-once install from the Contact Center server.
- If you make configuration changes to the `CCADAppSettings.xml` file, client computers must use the latest version of this file. For example, in High Availability solutions, you must launch Agent Desktop using the Managed name or IP address of Contact Center Multimedia. This requires editing the `CCADAppSettings.xml` file. All client computers must have the latest version of the `CCADAppSettings.xml` file after configuration changes are made.
- After an Avaya Aura® Contact Center service pack upgrade or patch application., all agents must have access to the updated version of the `Avaya\Contact Center\Multimedia Server\Agent Desktop\client` folder. For example, following the application of a service pack, you must once again manually copy the folder from your Contact Center server to each client computer.

Third-party software requirements

This section describes the third-party software requirements for Agent Desktop client computers.

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 v4.0, 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*.

Chapter 40: 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 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, might impact performance or might cause damage to your contact center solution.

Receiving email messages originating from a Web page

If your Web site generates email messages destined for a Contact Center Multimedia 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

Contact Center Multimedia supports hosted email providers that permit a POP3 or IMAP & SMTP connection. Contact Center Multimedia supports hosted email providers that require SSL or TLS 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, might impact performance or might cause damage to your contact center solution. Do not use Contact Center Multimedia 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 SSL, POP3 or IMAP/SMTP over TLS, and the use of nonstandard ports for these protocols. For more information, see *Avaya Aura® Contact Center Installation* (44400-311).

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 be 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* (44400-610).

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 Commissioning* (44400-312).

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 41: Microsoft Lync

Server requirements

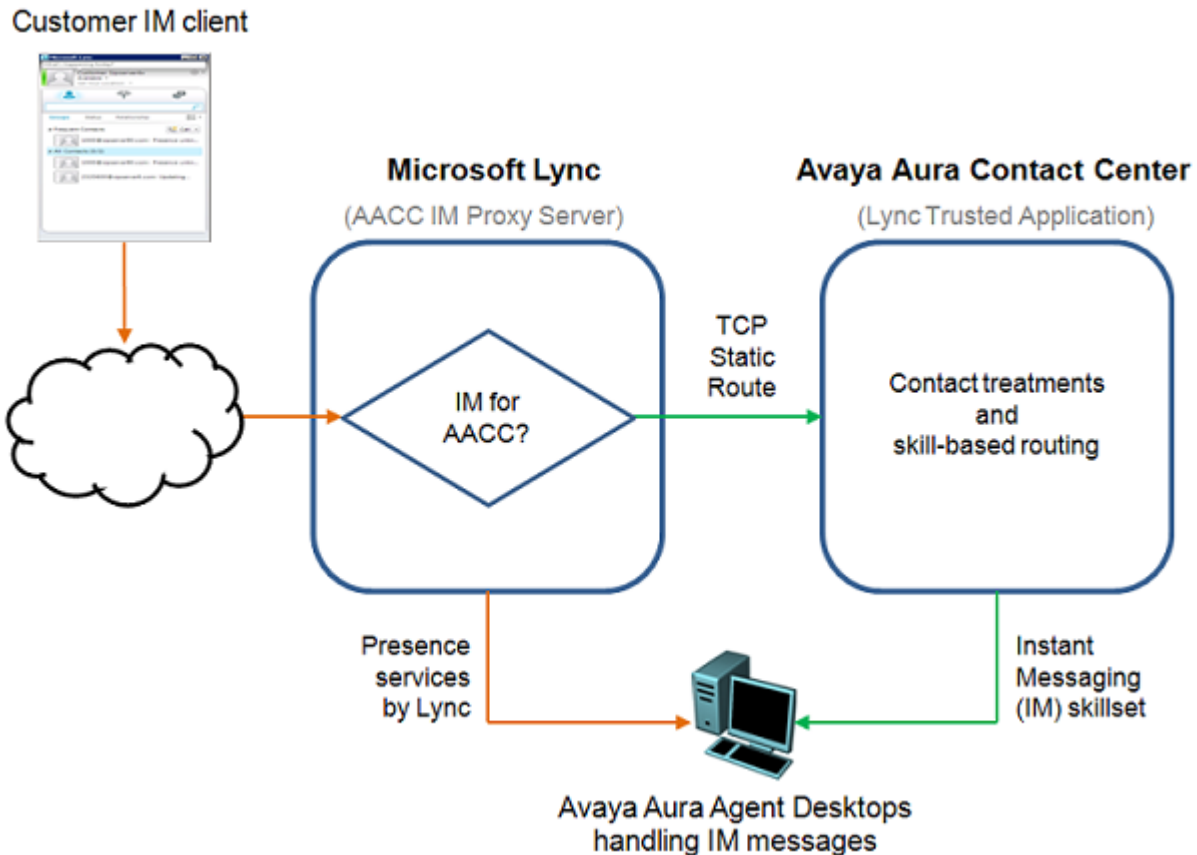
SIP-enabled Avaya Aura® Contact Center supports Microsoft Lync Server as an Instant Messaging (IM) and Presence services provider. Avaya Aura® Contact Center can process the IM messages it receives from Microsoft Lync Server and then route the messages to available Agent Desktop agents.

Avaya Aura® Contact Center supports Microsoft Lync Server Release 2010 and Release 2013.

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

 Important:

Agent Desktop does not support co-resident installation of Microsoft Office Communicator or Microsoft Lync client software.



Avaya Aura® Contact Center uses TCP transport to communicate with Microsoft Lync Server. Avaya Aura® Agent Desktop uses TLS transport to communicate with Microsoft Lync Server.

Avaya Aura® Contact Center supports Microsoft Office Communications Server (OCS) and Microsoft Lync Server. Agent Desktop supports Microsoft Lync to the same degree as it supports Microsoft OCS; with feature parity between both platforms. Customer IM messages are handled the same and exhibit the same flow in peer-to-peer and Avaya Aura® Contact Center routed contacts.

*** Note:**

Microsoft Lync Server requires a dedicated server. Microsoft Lync Server is not supported co-resident with Avaya Aura® Contact Center or Avaya Media Server. For more information about Microsoft Lync Server, refer to the Microsoft Lync Server product documentation.

Overview of integration

The following is a short overview of how to integrate Avaya Aura® Contact Center and Microsoft Lync Server. For more detailed information about the commissioning tasks, see *Avaya Aura® Contact Center Commissioning* (44400-312) and *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611).

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

Microsoft Lync Server requirements

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

Licensing requirements

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

Chapter 42: Avaya Aura® Presence Services requirements

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

Avaya Aura® Presence Services overview

Avaya Aura® Contact Center allows customers to use Avaya Aura® Presence Services to provide instant messaging services to support the Instant Message contact type. Customers also have the option of using Microsoft OCS 2007 for the same purpose.

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

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

Integration with Avaya Aura® Presence Services is available only in a SIP-enabled contact center based on the Avaya Aura® Release 6.1 or 6.2 platforms.

Important:

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

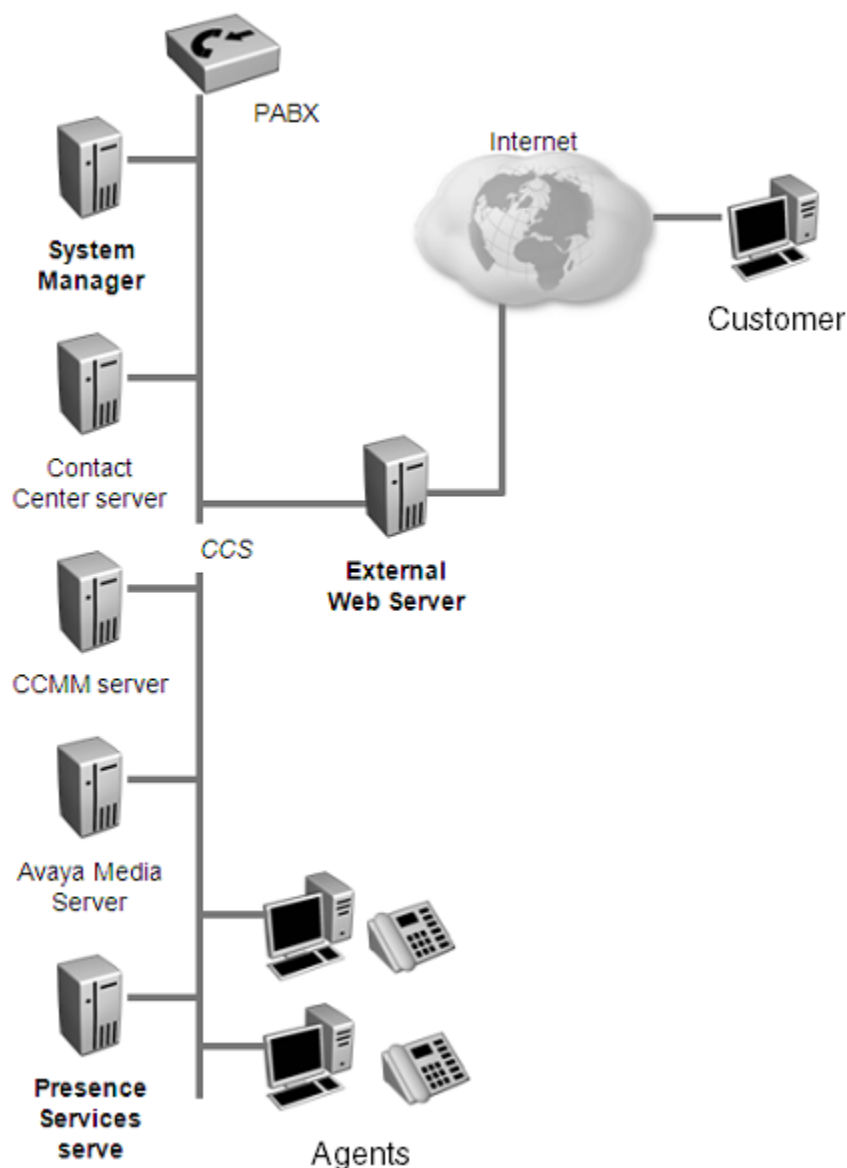


Figure 40: Avaya Aura® Presence Services server deployment

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

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

To assist with understanding this development, Avaya DevConnect supplies a sample Instant Messaging chat server component that you can install on your external Web server. The Instant

Messaging chat server allows customers to start Instant Messaging chat sessions with the contact center.

For full details of the interface specifications, browse www.avaya.com/devconnect.

The sample web-based client application from DevConnect does not cover integrating with Avaya Aura® Presence Services Release 6.2.2 or later. Contact DevConnect for more detail on how to achieve this integration.

To integrate with Contact Center, Avaya Aura® Presence Services requires the following:

- A Contact Center Multimedia server installed and commissioned, with the IM contact type licensed.
- An Avaya Aura® Presence Services server.

For information on installing the Avaya Aura® Presence Services server, see documentation on implementing Avaya Aura® releases 6.1 or 6.2.

- Avaya Aura® System Manager, which provides centralized management of all Avaya Aura® components including Avaya Aura® Presence Services.

You create routepoints and agent user accounts in System Manager for each routepoint and agent that is configured for Instant Messaging in CCMA, see documentation on installing and upgrading Avaya Aura® System Manager.

Hardware requirements

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

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

Operating system requirements

Avaya Aura® Presence Services requires the Linux operating system. See documentation on implementing Avaya Aura® releases 6.1 or 6.2.

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

Licensing requirements

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

High Availability

The Avaya Aura® Presence Services Release 6.1 product does not have a High Availability feature.

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

Chapter 43: 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* (44400-610).

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.

On the Call Complexity input page, enter the average number of Send Info and Send Request/Get Response commands issued for each call.

This is the average value taken over all incoming calls.

Example

Suppose that the call rate is 20 000 CPH during the peak hour. If 40 percent of incoming calls are treated with the HDX service, and of these calls

- 20 percent use one Send Info command
- 20 percent use two Send Info commands
- 30 percent use one Send Info and one Send Request/Get Response command
- 30 percent use one Send Request/Get Response command

The average number of Send Info commands issued per incoming call is

$$0.4 \times (0.2 + 0.2 \times 2 + 0.3) = 0.36$$

The average number of Send Request/Get Response commands issued per incoming call is

$$0.4 \times 0.3 \times 2 = 0.24$$

Enter these values into the appropriate boxes on the Call Complexity property sheet.

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 1:100 (or 1 customer record per 100 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 Web sites 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 +35387555555@sms.company.com instead of gateway@sms.company.com must be recorded under +35387555555@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 50: 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 44: 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.

Table continues...

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.

Avaya Security Advisories

Avaya Security Advisories are posted on the Avaya Security Support web site at <https://support.avaya.com/security>. From the Avaya Support web site, 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 www.avaya.com/support.

Secure RTP in Contact Center

In Release 6.4, 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 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 recognise 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 same Certificate Authority (CA). You can use the Contact Center default certificates, but Avaya recommends this only for testing, because the AACC default certificate is a widely available certificate.

! Important:

AACC Release 6.4 does not support SRTP for SIP call recording by Avaya Contact Recorder (ACR). DMCC call recording through an interface directly to the Communication Manager does support SRTP.

! 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 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 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 Aura® 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 *Avaya Aura® Contact Center Installation* (44400-311).

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 51: 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.
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
8444	Local WebLM Port
9080–9083	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

Table continues...

CCMS port number	Functionality
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
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 52: 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 SSL is enabled for secure Internet Information Services (IIS) communication).
TCP Ports 389 and 636	For Active Directory Lightweight Directory Services (AD-LDS) functionality. Port 389 is for LDAP, and port 636 is for SSL. When you install CCMA on a server that runs Window Server 2008, these ports usually appear by default in the Port Configuration for AD-LDS installation window. If the values 50 000 and 50 001 appear instead, port numbers 389 and 636 are already taken. In this case, you can either accept the new values, or choose other ports for security reasons. These ports are also used for AD-LDS replication in High Availability solutions.
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.

Table continues...

CCMA port number	Functionality
3899, 6366	For AD-LDS when CCMA is co-resident with Avaya Media Server or with an upgraded legacy Security Framework server. These ports are also used for AD-LDS replication in High Availability solutions.
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 ports

The following table lists the configurable Multimedia ports.

Table 53: 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

Table continues...

Port	Host	Client	Network interface	Functionality
				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 SSL (optional)	Receiving secure email (optional)
993	Email server	Email Manager	IMAP over SSL (optional)	Receiving secure email (optional)
110	Email server	Email Manager	POP3 over TLS (optional)	Receiving secure email (optional)
143	Email server	Email Manager	IMAP over TLS (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 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 54: 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 (CCMA 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	Default 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.
8888	For the TAPI switch connection using direct-connect. This port is required only for the ELAN subnet.
8087	For CCT CMF component.
9000	For CCT WebAdmin component.
9010	For CCT CMF component.
11110	Used by the CCT Server service for the CMF Web Service - Callback port.
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 Media Server port requirements

The following table shows the port numbers required for Avaya Media Server on Windows Server 2008.

Table 55: Avaya Media Server port usage—Windows Server 2008

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
5060	TCP	Yes	SIP over TCP
5060	UDP	No	SIP over UDP
5061	TCP	Yes	SIP over TLS
6080	TCP	No	Agent Greeting
7080	TCP	No	ConfMP MSLink
7410	TCP	Yes	SoapServer
7411	TCP	Yes	SoapServer TLS
8080	TCP	Yes	EM/UCM HTTP
8443	TCP	Yes	EM/UCM HTTP(s)
11004	TCP	No	DiamC MSLink
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 Media Server on Linux.

Table 56: Avaya 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
6080	TCP	No	Agent Greeting
7080	TCP	No	ConfMP MSLink
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
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 57: Required UDP Port Range

Operating System	UDP Port Range
Windows Server 2008	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
HTTP (Web services)	CCMM	443 (if SSL is enabled on the CCMM server)
CCT	CCT	29373
Web Reporting P2P IMs	CCMS	7080
Voice History	CCMS	57772
Aura Presence	Aura Presence Server	5222 (fixed, jabber protocol)
Web Statistics	CCMS	9086
CC Offsite Agent	CC Offsite Agent	8080 (fixed, web service)
CC Offsite Agent	CC Offsite Agent	20000 (fixed, service call)
Spark – embedded phone	Communication Manager	6225 – 106275 range
MS Office Communicator	MS Office Communicator server	5060 and 5061 (fixed, TCP and TLS)
SER	Predictive server	40000

Avaya Aura® Presence Services port requirements

The following table shows the port numbers required for Avaya Aura® Presence Services.

Table 58: 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

AACC firewall considerations	45
AACC-M	330
about Contact Center client components	39
about Contact Center components	38
about multimedia components	107
about Presence Services	489
about Unified Communications platform	55
Access Security Gateway	130
access to remote support	375
activity codes	
improvements	25
ACW codes	22
ADD	
Citrix	460
Administration Client	456
administration client operating system requirements	458
Agent Desktop	39
Citrix support	479
shortcut keys	29
thick client deployment	479
Agent Desktop client requirements	462
Agent Desktop thick client installation	479
Agent Greeting	268
agent limits	287
Alarm Monitor	97
aliases	484
AML and SIP capacities	288
AML and SIP cost per call	297
AML Contact Center on CS 1000	64
AML features	248
announcements	271
antivirus software	398, 410, 416, 429, 438, 446, 449, 453
Antivirus software	433
antivirus software guidelines	374
application intrinsics	295
application migrations	49
application sequencing	218
application variables	295
ASG	130
assignment parameter limits	288
attached call data for CCT	302
attachments for email	483
attachments in email storage	300
Automatic Call Distribution	69
Automatic phrases	111
availability highest level	377
availability standby level	380
availability warm standby level	381
Avaya Aura Experience Portal	213, 250
Avaya Media Server	130, 431, 432
zoning	144

Avaya Media Server licensing	268, 432
Avaya Media Server network configurations	134
Avaya Media Server port requirements	511
Avaya Media Server Zoning	
licensed feature	268
Avaya MS	
server specifications	330
Avaya Security Advisory	370, 505
Avaya Voice Portal compability	252
average call rate	299

B

backup software requirements CCMS	
.....	398, 409, 415, 428, 438, 445
binding order for network cards	396, 408, 454
BIOS	326
blended agents	235

C

Call Center Elite	
commissioning overview	236
call complexity	297
Call Control XML	216
call data attached for CCT	302
Call Join	23
call load	297
CallPilot compatibility	252
Call Recording	57
call resources limits	288
calls per hour limits	287
campus network requirements	385
capacity, hardware appliance	332
capacity CCT	301
capacity maximum	287
capacity outbound contact centers	304
capacity SIP and AML	288
capacity steady state operation	495
CCMA	
Citrix	460
CCMA client performance	498
CCMA network performance	496
CCMA performance	496
CCMA port requirements	508
CCMM	
database files	300
CCMM external email server requirements	483
CCMM outgoing email	485
CCMM performance	499, 500
CCMM port requirements	509
CCMS backup software requirements	
.....	398, 409, 415, 428, 438, 445

CCMS call load	297	Controlled Directory Number	68
CCMS hardware requirements	308	Conversation log	111
CCMS performance	493	converting protocols	338
CCMS port requirements	507	corporate enterprise licensing	257
CCT and CS 1000 on ELAN subnet	454	Corporate NCC licensing	258
CCT call attached data	302	cost of call services	297
CCT capacity	301	critical high availability	377
CCT components	389 , 402	CSTA interfaces	55
CCT network interface card order	396 , 408 , 454	customer contact ratio	499
CCT network performance	501		
CCT performance	500	D	
CCT port requirements	511	data attached to CCT calls	302
CCT supported functionality	389 , 403 , 422	database files	
CCXML	216	CCMM	300
CDN	68	database parameter limits	288
Citrix support		database restoration	46
Agent Desktop	479	data limits for Open Interfaces Web service	304
Click-to-Dial	57	data management, Multimedia	125
client hardware requirements	463	Data transfer	215
Client hardware requirements	456	decrease hardware	345
Client operating system requirements	465	default attachment files	483
client terminals	393 , 407	Default conversation text	111
commissioning Contact Center on VMware	357	DHCP	371
commissioning overview		dialogs	271
Call Center Elite	236	digital signal processors	338
common server requirements	366	direct switch telephony connections	455
Communication Control Toolkit		disk caching	327
installation configuration	99	disk partitioning	367
Communication Server 1000 phones	247	disk storage requirements for multimedia	299
Communication Server 1000 platform compatibility	245	distributing licenses	257
compatibility	242	DNIS	340 , 343
compatibility for Communication Server 1000 platform	245	domain	43
compatibility for switches in SIP	336	domain security deployments	52
compatibility for Unified Communications platform	242	DVD Controller	45
compatibility License Manager server	285		
compatibility with voice services	252	E	
compatible phones	244 , 247	ELAN subnet CCT and CS 1000	454
component clients of Contact Center	39	email	296
components of CCT	389 , 402	email aliases	484
components of Contact Center	38	email attachment storage	300
Computer Telephony Integration	66	email message memory requirements	
consolidate hardware resources	345		394 , 412 , 426 , 435 , 442
Contact Center commissioning VMware	357	email messages	
Contact Center Manager Administration		supervisor approval	30
installation configuration	84	email outgoing configuration	485
Contact Center Manager Server		email server requirements	483
installation configuration	73	email settings	483
Contact Center maximum capacities	287	Emergency Help	91
Contact Center migration paths	49	emergency licensing	283
Contact Center Multimedia		Enterprise licensing	257
installation configuration	105	entry-level licensing	259
contact handling	73	Entry-level server	305
contact modeling	397 , 408	Entry-level solution	305 , 308
contact presentation	73	Essential licensing	259
contact processing	73	evaluating limitations	305
contact queuing	70		
contact treatment	73		

expected resource consumption	297
Experience Portal	225 , 228
external server interactions	108

F

features	21 , 22 , 27 , 30
extended email capacity	24
features licensed	274
filtering email	484
firewall considerations	
AACC	45
firmware	326
functions of telephony server	389 , 403 , 422

G

generation for licenses	273
geographic network requirements	386
Geographic Node	143
Geographic redundancy	149
geographic resiliency	194
global requirements server name	367
grace period for licensing	283
Grace Period Reset	47
guidelines for antivirus software	374
guidelines for Java Runtime Environment	371
guidelines for RAID	375
guidelines for SAN	375
guidelines for service packs	371
guidelines for service updates	370
guidelines for UPS	376
guidelines for utility software	373

H

H.323	219
hardware appliance	24 , 333
hardware appliance, capacity	332
hardware-assisted virtualization	355
hardware RAID guidelines	375
hardware requirements	
.....	317 , 388 , 402 , 412 , 418 , 432 , 435 , 442 , 451
hardware requirements CCMS	308
hardware requirements Office Communications Server 2007	343
hardware requirements Presence Services	491
hardware requirements remote geographic node server	384
hardware requirements standby servers	384
hardware requirements virtual machine	364
hardware SAN guidelines	375
hardware UPS guidelines	376
high availability	274
High Availability	149
Machine Preserving	191
switchover	199 , 208

high availability critical	377
High Availability overview	
Midsize Enterprise	193
high availability standby	380
high availability warm standby	381
High-end server	305
.....	305 , 317
historical tracking license statistics	284
host considerations vmware	355
Host Data Exchange	493
Hot patching	166
hyper-threading	329

I

identifiers for licensing	274
increase	
email backlog capacity	24
installation	41 – 43
installation configuration	
Communication Control Toolkit	99
Contact Center Manager Administration	84
Contact Center Manager Server	73
Contact Center Multimedia	105
License Manager	79
Server Utility	94
instance licensing	23
Instant Messaging	486
interactions with external multimedia servers	108
interoperability	242
IOPS	356
IP voice protocol	337

J

Java Runtime Environment guidelines	371

K

knowledge worker environment	455
Knowledge Worker server	451
Knowledge Worker Server	451
KRS	259

L

LACP	164
licensed feature	
Avaya Media Server Zoning	268
TLS SRTP Signaling and Media Encryption	271
Licensed packages	268
license features	274
license identifiers	274
License Manager	
installation configuration	79
License Manager location	267

License Manager server support	285	multiple AACC instances	243
licensing	277	multiple server licensing	257
Licensing	488		
licensing Avaya Media Server	268 , 432	N	
licensing enterprise solutions	257	naming server requirements	367
licensing essential voice solutions	259	NCC	448 , 449
licensing generation	273	network Avaya Media Server	134
licensing historical tracking	284	network CCT performance	501
licensing locks	283	Network Control Center	71 , 448 , 449
licensing mechanisms	259	networked campus requirements	385
licensing multiple servers	257	networked geographic requirements	386
Licensing requirements	256	network environment contact modeling	397 , 408
licensing single server	257	networking parameter limits	288
limitations evaluation	305	network interface cards binding	396 , 408 , 454
limitations for contact modeling	397 , 408	network outage	182 , 203 , 212
localized languages	462	network performance for CCMA	496
locked licenses	283	Network requirements	466
		New in this release	20
M		nodal enterprise licensing	257
Machine Preserving High Availability	191	Nodal NCC	258
managed name	209	No Switch Configured	441
managing prompts	91	No Switch Configured Multimedia Only	442
maximum capacities	287	NUMA	328
maximum capacity	287		
mean holding time	299	O	
media management	130 , 419	obtaining a license	261
memory requirements for email messages	394 , 412 , 426 , 435 , 442	OCS 2007 for SIP	343
Meridian Link Services	66	Offsite Agent	269
Message timers	111	open interfaces	
Microsoft Hyper-V	345	email	128
Microsoft Lync	26 , 486	open interfaces data limits	304
Mid-range server	305	open queue	274
Mid-range solution	305 , 311	Open Queue	71
Midsize Enterprise		Open Queue Route Points	68
High Availability overview	193	Open Virtual Appliance	26
Midsize Enterprise compatibility	242	operating system Java Runtime Environment guidelines	371
migration		operating system packs guidelines	371
migration process	48	operating system requirements	368
migration paths	49	operating system requirements Presence Services	491
Mission Critical	177	operating system service update guidelines	370
Mission Critical HA with Midsize Enterprise	170	operational state	495
Mission Critical HA without platform resiliency	171	optional configuration tools	
Mission Critical HA with platform resiliency	168	email open interfaces	128
Mission Critical High Availability	168	outbound	274
overview	175	outbound capacity	304
Mission Critical High Availability configuration utilities	178	outbound Contact Center	107
MPS compatibility	252	outgoing email configuration	485
Multimedia Complement for Elite	434 , 435	OVA	26
multimedia components	107	overview client components	39
Multimedia Contact Server	411 , 412	overview components	38
multimedia disk storage	299		
multimedia email attachment storage	300	P	
multimedia external server interactions	108	performance	326
multimedia only	266		
multimedia terminals	393 , 407		

performance for CCMA	496	requirements port CCMS	507
performance for CCMA client	498	requirements port CCT	511
performance for CCMA network	496	requirements Presence Services hardware	491
performance for CCMM	499 , 500	requirements Presence Services operating system	491
performance for CCMS	493	requirements Presence Services port	514
performance for CCT	500	requirements RAID	375
performance for CCT networking	501	requirements remote geographic node server	384
performance management	327	requirements SAN	375
P-header	217	requirements server name	367
phonebook enhancements	27	requirements service packs	371
adding custom contacts	27	requirements service updates	370
tagging contacts	27	requirements standby server	384
phone compability	244 , 247	requirements UPS	376
P-Intrinsics	217	requirements utility software	373
port requirements Avaya Media Server	511	requirements virtual machine hardware	364
port requirements CCMA	508	RGN	204 , 205
port requirements CCMM	509	Route Point	68
port requirements CCMS	507	Route points	111
port requirements CCT	511		
port requirements Presence Services	514	S	
ports	514	SAN guidelines	375
Presence Services	489	Screen Pop	217
Presence Services hardware requirements	491	screen pops	21
Presence Services operating system requirements	491	security	370 , 505
Presence Services port requirements	514	stand-alone server	504
Private Header	217	Security	504
Proactive Outreach Manager	28	security deployments	52
progressive outbound	274	server name requirements	367
		Server specification	305
R		server support virtual	345
RAID	327	Server types	305
RAID guidelines	375	Server Utility	
ratio of customers to contacts	499	installation options	94
real-time display parameter limits	288	Service-Oriented Architecture	219
Remote Geographic Node	151 , 182 , 183 , 204	service packs guidelines	371
remote geographic node server requirements	384	service updates guidelines	370
remote support access tool	375	Session Initiation Protocol	217
report creation wizard	274	Session Manager	343
requirements antivirus software	374	SGM	217
requirements backup software CCMS	398 , 409 , 415 , 428 , 438 , 445	shortcut keys	
requirements campus network	385	Agent Desktop	29
requirements CCMM disk storage	299	sign-on deployments	52
requirements email message memory	394 , 412 , 426 , 435 , 442	single server licensing	257
requirements external email server	483	SIP	217
requirements geographic network	386	SIP and AML capacities	288
requirements hardware	317	SIP and AML cost per call	297
requirements hardware CCMS	308	SIP contact center service	268
requirements Java Runtime Environments	371	SIP Domain	62
requirements knowledge worker environment	455	SIP Enablement Services	57
requirements Office Communications Server 2007	343	SIP feature limitations	335
requirements operating system	368	SIP Gateway Manager	217
requirements port Avaya Media Server	511	SIP high availability	377 , 381
requirements port CCMA	508	SIP in Unified Communications platform	55
requirements port CCMM	509	SIP Network Components	60
		SIP OCS2007 requirements	343
		SIP Route Point	68

Index

SIP signaling	218	user permissions	
SIP standby availability	380	maintain	95
SIP switch compatibility	336	monitor	95
skill-based routing	69	using call data in scripts	493
snapshot considerations	361	utility software guidelines	373
Social Media Analytics	116	UII	218 , 219
social network, contact type	113		
software antivirus guidelines	374	V	
software requirements remote geographic node server	384	VDI	477
software requirements standby servers	384	VDI support	23
software utility guidelines	373	VE	173
SRTP	505	videos	18
standby high availability	380	virtualization	328
standby server	274	Virtualization	362
standby server requirements	384	virtual machine hardware requirements	364
steady state operation	495	virtual server support	345
supervisor approval		VMware	305 , 328
email messages	30	VMware commissioning Contact Center	357
supervisor approval of email messages	30	VMware Horizon View	477
support	19	vmware host	355
support access tool	375	VMware vSphere	345
supported License Manager servers	285	VMXNET	361
Survivable Core	195	Voice and Multimedia Contact Server	387 , 388 , 418
switch compatibility SIP	336	Voice Contact Server	401 , 402
switchover	204	voice only licensing	259
reinstate High Availability resiliency	181 , 202 , 211	voice services compatibility	252
Switchover	177	Voice XML	216
Switchover Handling Script	185	VoIP	337
switch processing	338	VRRP	164
		VXML	216
T			
telephony server functions	389 , 403 , 422	W	
telephony subnet with CCT and CS 1000	454	warm standby high availability	381
terminals	393 , 407	Web communications limits	288
third call appearance button	30	WebLM	259 , 260
third line appearance	30	Web Service data limits	304
third-party interface limits	288	whisper skillset	31
third-party software		workgroup	43
.....	397 , 408 , 414 , 428 , 432 , 437 , 444 , 449 , 453 , 461		
Third-party software requirements	480		
TLS SRTP Signaling and Media Encryption		Z	
licensed feature	271	zoning	
Toll Free Queuing	31	Avaya Media Server	144
Trusted IP	153		
U			
Unified Communications phones	244		
Unified Communications platform compatibility	242		
Uninterruptible Power Supply guidelines	376		
Universal Call Identifier	219		
universal networking	274		
unused hardware	329		
upgrade	48		
upgrading Contact Center	49		
usage of licensing	284		