AVAYA

Avaya Aura® Contact Center Fundamentals

Release 6.2
NN44400-110
03.05
30 July 2012

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 generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by 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 Web sites 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 its Hardware and Software (“Product(s)”). 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 Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation 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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: New in this release

The following sections describe the new features and changes documented in *Avaya Aura® Contact Center Fundamentals* (NN44400-110).

Features

See the following sections for information about feature changes:

- Avaya Aura® Call Center Elite support on page 12
- Agent Greeting on page 12
- Agent Templates on page 12
- Call Routing Enhancement on page 13
- Avaya Media Server on Linux on page 13
- Support for Avaya Aura® Presence Services on page 13
- Supported operating systems on page 14
- Supported PBXs on page 14
- Essential licensing on page 15
- High Availability on page 15
- Contact Center Manager Administration installation changes on page 15
- Contact Center Multimedia media type changes on page 16
- Support for inline attachments in auto suggestions and auto responses on page 16
- Support for a LDAP server for Voice contacts on page 16
- Support for Web on hold and Web communications comfort groups on page 16
- Supervisor observe and barge-in on page 17
- Screen Pops on page 17
- Customer History on Voice Contact on page 17
- Avaya Aura® Agent Desktop user interface on page 17
- Communication Control Toolkit client and server administration on page 18
- Multiplicity on page 18
- Multimedia only installation on page 18
- Avaya Aura® Agent Desktop on page 18

- Avaya Secure Access Link support on page 19
- Call Force Answer Zip Tone on page 19
- Support for Web Communications transfer to a skillset on page 19

Avaya Aura® Call Center Elite support

Avaya Aura® Contact Center Release 6.2 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 a unified voice and multimedia Agent Desktop, and unified reporting.

You can install Avaya Aura® Contact Center to add multimedia-enabled capabilities to new or existing Avaya Aura® Call Center Elite contact center solutions. For more information about Avaya Aura® Call Center Elite integration, see Avaya Aura® Call Center Elite integration on page 191.

Agent Greeting

The Agent Greeting feature allows agents to pre-record greetings. The system plays the greeting automatically when an agent answers a call.

The Agent Greeting feature is supported only in SIP-enabled contact centers. In AML-based contact centers, use the Avaya Communication Server 1000-based Agent Greeting product.

Agent Templates

Only on Avaya Aura® Call Center Elite when an agent logs into Avaya Aura® Agent Desktop, templates apply a group of settings to the Agent Desktop. Agent templates provide flexibility since you can have specialized settings for each individual agent. Administrators must enable the Contact Center Multimedia server to work with Call Center Elite to use agent templates.

A default template contains the basic settings for agents. Agent templates inherit properties from the default template. Inheritance in templates follows a tree structure. Child templates inherit properties from all their parents. You can set inheritance only up to five levels.

Assigning a template to an agent creates the agent's profile. You can then customize profiles based on agent requirements and the changes made to a profile are specific to an agent.

Administrators can assign multiple profiles to agents and then select a preferred profile for an agent. The agent logs into the Agent Desktop using the preferred profile.

Call Routing Enhancements

Avaya Aura® Contact Center Release 6.2 includes three call routing enhancements. The Enhanced Expected Wait Time enhancement provides a more accurate measure of wait time in the Expected Wait Time (EWT) script intrinsic. The administrator can select the existing NES EWT or the Enhanced EWT in Global Settings.

The Service Level Routing (SLR) and Service Level Management (SLM) enhancements reduce the wait time that a caller experiences. These enhancements allow contact center administrators to easily set and meet the service level thresholds on skillsets. These enhancements provide functionality similar to the Business Advocate product used with Call Center Elite.

Service Level Routing is an enhanced routing strategy. It minimises the number of callers that experience a wait time that exceeds the target for the skillset. It considers the Target Service Level threshold for the skillset when selecting the next queued contact to route to an available agent.

Service Level Management (SLM) reduces callers' wait time further by automatically assigning standby priority skillsets to reserved agents, which makes them available for pending contacts. This skillset assignment is activated when the skillset's Expected Wait Time (EWT) exceeds its Target Service Level (TSL). When the EWT of the skillset falls below its TSL, the skillset is removed from the reserved agent. The administrator can assign the agents to the standby skillset with SLM enabled. These agents do not appear on the Real-Time Display (RTD). In a normal routing situation, these agents do not receive any calls on their standby skillsets, even if they are idle. However, SLM routes calls to the agent only on a call-by-call basis, and the agent's skillset assignment does not change.

Avaya Media Server on Linux

Avaya Aura® Contact Center Release 6.2 provides support for installing Avaya Media Server (Avaya MS) on Linux.

Support for Avaya Aura® Presence Services

Avaya Aura® Contact Center Release 6.2 provides integration with Avaya Aura® Presence Services.

Integration with Presence Services enables Contact Center Agent Desktop to display presence information for the Agent, Supervisor, and Expert. Knowing an Expert's availability allows an Agent to instantly consult the appropriate Expert if necessary.

Integration with Presence Services is available only in a SIP-enabled contact center.

You must install and configure the following Avaya Aura® components to work with Contact Center:

- Avaya Aura® System Manager: Avaya Aura® System Manager provides centralized management of all Avaya Aura® components.

  You must create routepoints and agent user accounts in System Manager for each routepoint and agent that is configured for Instant Messaging through Contact Center Manager Administration (CCMA).
- Avaya Aura® Presence Services: For sending an Instant Message into the Contact Center, you must create customer accounts on the Presence Services server.

Supported operating systems

Avaya Aura® Contact Center Release 6.2 server applications are supported only on the Windows Server 2008 Release 2 64-bit operating system.

Contact Center Release 6.2 does not run on Microsoft Windows Server 2003. Installation and upgrade processes to Contact Center cannot use the same server as previous releases.

For more information, see the following sections

- Domains and Windows Server 2008 Release 2 security policies on page 26
- Supported server operating systems on page 29
- Installation process on page 103
- Upgrades versus migrations on page 229

On Windows Server 2008 Release 2, the ADAM database is now referred to as Active Directory Lightweight Directory Services (AD-LDS).

Supported PBXs

Contact Center Release 6.2 supports the Avaya Aura® Unified Communications platform in addition to the Avaya Communication Server 1000 (Avaya CS1000) and Microsoft Office Communications Server (OCS) configurations. For more information about the new switch, see Avaya Aura® Unified Communications platform on page 45.

A Session Initiated Protocol (SIP)-enabled environment offers features that enrich customer interaction with the Contact Center. These features include inbound voice contacts, instant messaging, and buddy lists. The following sections include information about SIP:

- Installation configurations on page 106
- Modes of operation on page 142

The OCS configuration is supported with Avaya Communication Server 1000, so you can have voice and instant messaging with presence.

Avaya Aura® Presence Services is supported with Avaya Aura® Unified Communications platform Releases 6.1 and 6.2, so you can have voice and instant messaging with presence.

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 coresident License Manager.

For more information, see the following sections:

- Co-resident installations on page 103
- Installation configurations on page 106

WebLM

SIP-enabled Avaya Aura® Contact Center supports WebLM. Avaya Aura® Contact Center can use WebLM to license the contact center features and to control the number of agents in your system.

For more information about the WebLM license, see Licensing mechanisms on page 121.

High Availability

Contact Center supports High Availability (HA) resiliency for Contact Center Manager Server, Communication Control Toolkit (CCT), Contact Center Multimedia (CCMM), Avaya Media Server and Contact Center Manager Administration.

For more information about high availability, see High Availability fundamentals on page 53.

Contact Center Manager Administration installation changes

The prerequisites and user configuration for CCMA are more streamlined. Components external to Contact Center such as Crystal Reports are not required.

For more information about CCMA installations, see Contact Center Manager Administration on page 151.

Contact Center Multimedia media type changes

If you are licensed to use multimedia, you can route Standard Message Stream (SMS) text, faxed documents, scanned documents, and voice mail and handle them as e-mail messages in your contact center.

The administration for details related to all multimedia contact types occurs within the Contact Center Manager Administration client.

For more information, see Contact Center Multimedia on page 163.

Support for an LDAP server for Voice contacts

Administrators can configure a Lightweight Directory Access Protocol (LDAP) server to provide agents using Agent Desktop with a list of contacts during a voice call.

Support for inline attachments in auto suggestions and auto responses

Administrators can add inline attachments (only as images), such as company logos, to auto suggestions and auto responses. Both standard and inline attachments are supported for auto suggestions and auto responses.

Agents can also place inline attachments (only as images) in e-mail messages.

Inline attachments display complete information within the body of the e-mail. This makes the information easily accessible to customers, even without explicitly opening the attachment.

Support for Web on hold and Web communications comfort groups

A Web on hold comfort group creates a list of messages that are sent to the customer's desktop, while the customer waits for an agent to respond.

A Web communications comfort group creates a list of messages that are sent to the customer's desktop while they wait for an agent to respond.

Administrators need to add both the Web on hold and Web communications comfort groups to the Web communications skillset.

Administrators can also set the time for which messages display on the customer's desktop.

Avaya recommends that you use no more than five messages in each Web on hold or Web communications comfort group and one Web on hold or Web communications comfort group for each Web communications skillset.

Supervisor observe and barge-in

An agent-supervisor can observe or participate in any currently active agent-customer Web communications chat session, provided the agent is under the supervision of that particular agent-supervisor. Agent-supervisors using Avaya Aura® Agent Desktop can see a display of all such applicable Web communications and Voice contacts currently active. This display can also flag any Web communications contacts where certain intrinsic values exceed the defined threshold.

Screen Pops

Administrators can use the Screen Pops page in CCMM Administrator to configure application shortcuts and intrinsics, that agents can use while running Agent Desktop.

Voice Contact Screen Pop is supported in SIP-enabled contact centers and in Contact Center as a Multimedia complement to Call Center Elite.

Customer History on Voice Contact

You can search for customer history based on the calling line ID for voice contacts.

Customer History on Voice Contacts is supported only in contact centers that include Contact Center Multimedia.

Avaya Aura® Agent Desktop user interface

Avaya Aura® Agent Desktop is a new user interface is based on a work item paradigm. Each agent-to-customer interaction is a work item. Work items appear on the Agent Desktop work list. If you perform another interaction associated with that work item (for example an IM consultation with an expert), then that interaction is displayed as part of the original work item. The work list window contains work items and buttons corresponding to the work item. The buttons and functions change depending on the items in the work list window. When a new contact arrives, Agent Desktop adds the new contact to the work list.

The Agent Desktop e-mail editor supports the HTML format for e-mail messages.

Agent Desktop displays skillset-related statistics. Agents can view statistics for their skillsets in pie chart or bar chart format. Supervisors can display statistics for all skillsets in pie chart or bar chart format.

For more information, see Components on page 166.

Communication Control Toolkit client and server administration

The CCT Snap-in includes server-side and bulk configuration tasks only. CCT Administration occurs by using the CCT Web Administration client, which is accessible from CCMA.

The bulk provisioning tool is updated to replace the Import Configuration and Export Configuration tools. Use this tool to export any or all data in the CCT database to an XML file using one of two possible XML schema definitions: a standard data schema definition and a flat schema definition.

For more information, see Communication Control Toolkit on page 141.

Multiplicity

Multiplicity ensures an agent can handle multiple concurrent contacts. At any one time an agent can be active on a voice and multimedia contact; only one of these can be active, the others automatically are on hold.

See the following sections for information about multiplicity:

- Handle contacts on page 179
- Report multimedia data on page 181

Multimedia only installation

The Contact Center DVD supports installing a non-voice multimedia-only set of Contact Center applications. You use a non-voice multimedia-only Avaya Aura® Contact Center to handle e-mail based customer contacts or to add multimedia capabilities to an existing voice-based Contact Center such as Avaya Aura® Call Center Elite. A multimedia-only installation of Avaya Aura® Contact Center handles e-mail messages, scanned documents, SMS text messages, FAX messages, and voice mail messages.

Avaya Aura® Agent Desktop

Avaya Aura® Agent Desktop has an embedded softphone, eliminating the need for an agent deskphone. Agents can use a suitable computer headset with their Avaya Aura® Agent Desktop softphone, or they can continue to use Avaya Aura® Agent Desktop to control their deskphone.

Agent Desktop controls the softphone and the deskphone using one set of user interface buttons.

Avaya Secure Access Link support

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. Secure Access Link (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.

Call Force Answer Zip Tone

In a SIP-enabled Contact Center, Avaya Aura® Contact Center 6.2 supports an optional configuration to give Call Force Answer (CFA) Zip Tone to all agents who answer a voice call. A zip tone is a tone or beep that a contact center agent hears before they are connected to a customer call. The restricted CFA Zip Tone Feature provides a global system wide setting that turns CFA Zip Tone on or off for all agents. This is a restricted version of the Call Force Answer Zip Tone feature, as it is not connected with the Call Force option in the call presentation class of your Contact Center Manager Administration (CCMA) configuration.

Support for Web Communications transfer to a skillset

Agents can transfer a Web Communications (WC) contact to a skillset.

> ❗ **Important:**
>
> Agents cannot transfer a contact to a skillset that does not have active agents.

The agent who answers the transferred contact, views all the messages that were previously sent by the customer and the previous agent. The agent can also view the transfer details such as:

- the agent who transferred the contact
- the skillset from which the contact is transferred
- the skillset to which the contact is transferred
- the reason for transferring (if the agent who transferred the contact provides the reason)

For more information on performing a Web Communications transfer to a skillset, see *Avaya Aura® Agent Desktop User Guide* (NN44400-114).

Other changes

There are no other changes in this document.

Chapter 2: Introduction

This document describes the general background information to help you understand the planning and engineering, installation, commissioning, and upgrade concepts for Avaya Aura® Contact Center Release 6.2.

Related resources

Support

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

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit http://www.youtube.com/AvayaMentor and do one of the following:

- Enter a key word or key words in the Search channel to search for a specific product or topic.
- Click the name of a playlist to scroll through the posted videos.

Chapter 3: Server preparation

This chapter describes the background information you need before you begin installing Avaya Aura® Contact Center software on your servers. It contains information for planning your hardware, software, and network setup.

Hardware setup

Use the following sections to understand the requirements for configuring your hardware:

- Hardware requirement on page 23
- Partitions on the server on page 23
- Uninterruptible Power Supply on page 24
- Recovery using RAID backups or third-party backups on page 24

Hardware requirement

To determine the platform size required for a contact center configuration and to analyze in detail your contact center capacity requirements, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210). This information is necessary to decide on the specifications for your platform-vendor independent (PVI) server for such items as CPU speed, RAM size, and disk space.

For small or entry-level contact centers, you must use server hardware that meets the recommended minimum hardware specification. For more information on the minimum hardware specification, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Partitions on the server

The actual requirements for how to partition a server you prepare for a Contact Center installation depends on the number of agents, call rate, and other factors.

The minimum partition sizes are based on the following information:

- 1 KB = 1024 bytes
- 1 MB = 1024KB = 1 048 576 bytes
- 1 GB = 1024MB = 1 048 576 KB = 1 073 741 824 bytes

If you work with a server that you plan to upgrade, and a partition is smaller on the existing server than specified by the new requirements, you must rebuild the platform to increase the partition size and reinstall the operating system.

The operating system resides on the C partition. This must be the only primary partition. The application partition usually resides on D. The database partition is a separate partition.

For detailed information about the minimum partition sizes for your Contact Center server configuration, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Uninterruptible Power Supply

Avaya recommends that you use of an Uninterruptible Power Supply (UPS) with your servers. A UPS provides the following benefits:

- Reduction in data loss—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 that occur at the time of a power dip or spike can be unusable.

The UPS must adhere to the following requirements:

- Provide at least 10 minutes of power, which is required for the server to stop all services and shut down the server.
- Fit physically within the workplace.
- Apply power to the server when line voltage reaches a stable state.
- Recharge before powering up the server if the server is down for a long time.
- Be 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.
- Have hot-swappable batteries. Replacement or capacity upgrades of the batteries must not interrupt service.
- Not affect the Contact Center application software.

Recovery using RAID backups

Avaya Aura® Contact Center supports 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-1 controller. RAID-1 and RAID-5 are the only levels and types of RAID supported.

Network setup

Use the following sections to understand the requirements to configure your network.

- Network configuration on page 25
- Computer name and DNS configuration on page 26
- Domains and Windows Server 2008 Release 2 security policies on page 26

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.

Computer name and DNS configuration

Contact Center includes many server software applications that control routing, handling, and reporting contacts. If you change the name or IP address of one server software application, you must update the other server applications in your Contact Center with the new information.

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. FQDNs must not exceed 255 characters.

Server names must adhere to RFC1123 (Requirements for Internet Hosts) which specifies that a host name must adhere to the following guidelines:

- Use only characters a to z, A to Z, and 1 to 9 in a host name.
- Do not use the an underscore (_) or a period (.).
- Do not use spaces.
- Host names must be 6 to 15 characters in length.
- You can use a hyphen, but not to start or end the host name.

If all servers are on a network, you can use the Domain Name Service (DNS) server to resolve name and IP address translations for your servers. If you do not use a DNS in your network, you must manually update the HOSTS file on every server in your network. You must ensure your server computer name and Domain Naming Server (DNS) host name match, including uppercase and lowercase letters. If these names do not match, you cannot install the Contact Center software.

A mismatch in these names can occur, for example, if you perform a new installation of the operating system and enter the computer name in uppercase letters. Windows uses your entry to configure both the computer name and the DNS host name. However, after the installation, you can find that Windows configured the DNS host name in uppercase letters as you entered it, but that the computer name is configured in lowercase letters. Check the names, and if necessary, change them.

Domains and Windows Server 2008 Release 2 security policies

Avaya recommends that you add the Contact Center Manager Server, Communication Control Toolkit and Contact Center Multimedia servers to your domain.

If the Communication Control Toolkit server is not on a domain, you cannot use the High Availability features for the server.

If the Contact Center Multimedia/Outbound server 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 the Contact Center Multimedia/Outbound server is not part of a Windows Server 2008 domain, additional configuration is required. You can add the Contact Center Multimedia server as a member server and all agent network logon accounts to a domain. Immediate access is then on the shared network drives that you configured on the Multimedia Server. If the Contact Center Multimedia/Outbound server 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 the Contact Center Multimedia/Outbound server 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.

Software setup

This section describes the software that is not part of the Contact Center suite. It includes all supporting and third-party software guidelines.

- Third-party software requirements on page 27
- Supported server operating systems on page 29
- Operating system updates on page 30
- Preinstallation check on page 31

Third-party software requirements

Due to the mission-critical, real-time processing performed by Contact Center applications, you must not install other application class software on the server. You can install certain utility class software on the server if it conforms to the guidelines in this section.

Application class software generally requires a certain amount of system resources and is not 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 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.

Anti-virus software is classified as a utility and is subject to the generic guidelines listed in the following section.

Utility-class software

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 reduce 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.
- You cannot use disk compression utilities.
- You cannot use memory-tweaking utilities (for example, WinRAM Turbo, Memory Zipper) that are used to reclaim memory that is unused by Microsoft.
- The installation or removal of the third-party software must not affect or conflict with the Contact Center application (for example, it must not cause DLL conflicts). If a conflict occurs, you can be required to rebuild the server.
- You must perform tests to ensure these conditions and recommendations are met before you place the Contact Center application into production. Avaya support can ask for the results of the testing during fault diagnosis. As fault diagnosis, the distributor or end user can be asked to remove third-party software.
- You cannot install HyperTerminal on the CCT Server as it interferes with the operation of the CCT Telephony Server.

Anti-virus software

Avaya acknowledges that user's security policies can require the installation of antivirus software on the application server.

Avaya selected a representative sample of anti-virus software packages and has a policy validating these products to ensure co-residency with Contact Center server application products. The currently accepted anti-virus products are as follows:

- Symantec AntiVirus 11.0.5, 11.0.6, or 12
- McAfee 8.8
- Microsoft ForeFront 2010

The following are additional generic guidelines for the use of antivirus software:

- You can configure antivirus software to automatically clean the detected virus and quarantine files if they cannot be cleaned. Contact Avaya to verify if the quarantine file is part of the product files or a 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. You must not use a Contact Center application 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 procedure to download Contact Center application patches. This method limits access to the Internet and thus reduces the risk of downloading infected files.
- You must scan all patches, service packs, DVD ROMs, and floppy disks before you install or upload to the server. This practice minimizes exposure to infected files from outside sources.
- With respect to capacity considerations, running virus scan software can place an additional load on a Contact Center platform. You can 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, do not load the antivirus software onto the Contact Center platform.
- Avaya does not support antivirus software configuration, but offers guidance where possible. Direct questions or problems about antivirus software to the appropriate vendor.
- If you raise performance or functionality issues to Avaya support as part of fault diagnosis, you can be asked to remove third-party utility software or antivirus software.

Supported server operating systems

You can use all Contact Center servers software only on the following platforms:

- Windows Server 2008 Release 2 64-bit Standard edition
- Windows Server 2008 Release 2 64-bit Enterprise edition

The following table lists the operating system settings for Contact Center Servers. For more information about configuring Microsoft Windows Server 2008, see *Avaya Aura® Contact Center Installation* (NN44400-311).

Setting	Value required for Contact Center
Automatically adjust clock for Daylight savings time	If you use an Avaya Communication Server 1000 switch, clear the check box. If you use Network Skill-Based Routing in a Network Control Center server, select the check box if your area uses daylight savings time.
Computer name	Do not use spaces or underscores or exceed 15 characters. The name must start with an alphabetic character.

Setting	Value required for Contact Center
Date and Time window	Configure as required for your site.
Disk drives	Format to partitions as required for the Contact Center server. See *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
Domain/workgroup name	Configure as required for your site.
Licensing modes	Select Per server licensing mode. Accept the default five concurrent connections.
Modem dialing	Configure as required for your site. Do not install a modem on the CCT server.
Network components	Configure IP Address, WINS and DNS for one or two network cards for the server configuration.
Network connections	Ensure Contact Center subnet is first.
Network settings	Choose Custom.
Partitions	Configure C to be the only primary drive. Configure the other drives on your server to meet the requirements according to *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210) for the server.
Regional settings window	Configure as required for your site.
SNMP	Configure for all servers.

Operating system updates

Operating system updates include both patches and service packs.

Given the number of operating system security patches and the complexity inherent in a network, you must create a systematic and accountable process to identify and apply Windows operating system service packs. Avaya implements 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 customers wait until compatibility testing is complete before the you apply the service pack. Operating system service packs are typically tested with the most recent Contact Center application patch; therefore, an upgrade to a new service pack necessitates an upgrade to the most recent Contact Center application patch.

To help create 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 patches into a library, then system administrators or the Contact Center Administrator must fulfill this role.

Whenever possible, Avaya incorporates the most recent operating system security recommendations and patches in an integrated solutions testing strategy during each test cycle. However, due to the urgent nature of security patches when vulnerabilities are discovered, you must follow Microsoft guidelines as they are issued, including Microsoft installation and security patch rollback procedures that can be in place.

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 pack, you must remove the service pack and revert to the previous version of the application (from the backup you made before you applied the service pack). For added security, always check to see if Avaya verified the Microsoft service pack for compatibility with Contact Center Manager.

For more information about updating, see Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Compatibility List on Avaya (www.avaya.com).

Preinstallation check

Before you begin installing software, make sure that the server meets all requirements according to *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Ensure that each server meets the basic requirements for Platform Vendor Independence. After you install the operating system, the Pre-installation Compliancy Checker utility reviews the server performance, selects the Contact Center software, and partitions the drives as per specifications. This utility is on the server application DVD. It generates warnings and suggestions when the server does not satisfy the minimum or suggested requirement.

The Contact Center installer reviews automatically several software packages when the installation starts. The DVD for Contact Center automatically installs the following packages:

- Microsoft .NET Framework Version 3.5
- Visual C++ run-time libraries on the server

For more information about installing the other required software on the server, see *Avaya Aura® Contact Center Installation* (NN44400-311).

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.
AML	No specific network security mechanism is used. Because it is a proprietary protocol, exposure is limited as it runs over the ELAN subnet.

Server verification

Avaya provides technical support for the Contact Center suite of products and required third-party applications only. The hardware vendor performs all hardware diagnostics. Check with the manufacturer instructions and recommendations before you perform any hardware-related procedure.

You must verify the selected server before you install Contact Center software:

- Ensure the platform vendor independent system conforms to specifications.
- Install the operating system.
- Ensure the server is functional and can connect to the network.

You must rule out hardware faults before you escalate issues into Avaya. During problem diagnosis, Avaya can ask for test reports for platform vendor-independent hardware or request that you remove certain software utilities if it is deemed necessary as part of the investigation process.

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, such as:

- Secure Access Link for remote support on page 33
- Microsoft Remote Desktop Connection on page 33
- Virtual Private Network (VPN) on page 34
- Direct-connect modem on page 35

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* (NN44400-610).

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

For more information about setting up remote support with a VPN, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Virtual Private Network (VPN)

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.

Chapter 4: Routing options

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

Contact routing at the switch

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

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

ACD routing

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

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

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

Skill-based routing

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

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

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

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

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

Contact queuing and presentation

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

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

customer group with a lower service level agreement (such as small business accounts).

- Priority by agent: The agent has a priority for every skillset. Agents with high priorities for the skillset receive contacts for the skillset before agents with low priorities. Agent priorities range from 1 to 48, indicating the level of skill in the skillset. For example, an agent assigned a skillset priority 1 is likely highly proficient in the skill required to effectively handle a customer. An agent assigned a priority of 48 for a skillset can be a new employee learning how to handle customer inquiries for that skillset.

Multiple skillsets

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

Open Queue

Open Queue is a licensed feature on Contact Center Manager Server. The primary use of Open Queue is to enable the multimedia Contact Center to receive e-mail 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 5: Client preparation

Clients in Avaya Aura® Contact Center perform agent or supervisor duties such as handling contacts (Avaya Aura® Agent Desktop) or monitor real-time statistics (Agent Desktop Displays). Clients also create applications off-line before you install and configure servers (Orchestration Designer).

Operating system requirements

All clients associated with Contact Center Release 6.2 must use one of the following operating systems:

- Windows Vista Business SP1 or later
- Windows Vista Enterprise SP1 or later
- Windows 7
- Windows XP Professional Service Pack 2 or later

If Windows Vista is on a client on which you plan to run the Agent Desktop Displays, you must download a patch from the Microsoft Web site to view the online Help.

Citrix environment

All end user clients, except Contact Center Multimedia and Outbound Campaign Management Tool, in the Avaya NES Contact Center Release 7.0 fully support a Citrix Presentation server environment.

Avaya Aura® Contact Center Release 6.2 user clients support the current and previous Citrix Presentation server and Microsoft Terminal Services except for Contact Center Outbound Campaign Management Tool.

Other required software

The following sections describe other software that is compatible with or required for Contact Center clients.

Office suites

Contact Center Release 6.2 supports co-resident clients such as the following office suites:

- Microsoft Office
- IBM Lotus Smartsuite
- Openview

You may need to upgrade to the most recent software if you find issues with the previous release of software.

Other Avaya software

The following clients for other products are supported co-resident with Contact Center clients. If issues occur with a previous release of software, upgrade the software before you contact support.

- Avaya CallPilot®
- Avaya MPS
- OTM
- MCS5100
- i2050
- All Avaya Communication Server 1000 (Avaya CS 1000) Administration clients

Internet Explorer

To access the Contact Center Manager Administration software or Agent Desktop, all clients must have Internet Explorer 7.0 (32–bit) or later with the most recent supported service pack.

When you configure Internet Explorer, you configure the Contact Center server as a Trusted Site, and you disable or block cookies for your required level of security.

ActiveX control security

Security issues related to ActiveX controls are addressed by the following features:

- digital signatures
- code signing certificates (for digital signatures)
- Trusted Sites zone and Safe for Scripting

Digital signatures

All controls provided with Contact Center Manager Administration are in .cab files that are digitally signed either by Avaya or by the third-party vendor of origin. Signing the .cab file verifies that the software originated from a trusted source. You cannot alter the signed .cab file without invalidating the signature, which validates that the contents of the .cab file (including the control) also originated from a trusted source.

If the browser security settings stipulate that a control must be signed before you download it to the client, Internet Explorer checks whether the .cab file containing the control is signed. If the signature is valid, the control is downloaded to the client.

Code signing certificates (for digital signatures)

Software publishers use a code signing certificate to sign code that they develop and distribute. A signature given by a code signing certificate validates that the file originates from a trusted source and was not altered since it was originally published.

This type of certificate is valid for a specified period of time (usually one year) during which time software developers can use it to sign binary files with their digital signature. The code signing certificate can expire (usually after one year) without invalidating the signature. Provided the digital signature includes a timestamp, the only other requirement for the validity of the digital signature is that the code signing certificate be valid when the code is digitally signed. The digital signature includes a timestamp from a trusted server to prove the date on which the code was signed.

Secure Sockets Layer (SSL) certificates are different in that they are not useful after they expire.

For Contact Center, Avaya uses a code signing certificate purchased from VeriSign that is renewed each year. The digital signatures for Contact Center are timestamped against VeriSign servers. For information about VeriSign code signing certificates, see www.verisign.com.

Chapter 6: Supported switches

Contact Center Manager Server routes, manages, and supports voice calls coming from the following switches:

- Avaya Aura® Unified Communications platform
- Avaya Communication Server 1000
- SIP-initiated family of compatible switches

Avaya Aura® Unified Communications platform

Avaya Aura® Contact Center Release 6.2 supports integration with the Avaya Aura® Unified Communications platform.

Contact Center uses industry-standard SIP and CSTA (TR/87 over SIP) interfaces to communicate with the outside world. The Avaya Aura® Unified Communications platform supports these SIP-enabled interfaces. Integrating the Contact Center with the Avaya Aura® Unified Communications platform using SIP infrastructure supports multi-nodal communication between customers and Contact Center agents. This integration gives Contact Center access to and control of Avaya Aura® Unified Communications platform phones. The Avaya Aura® Unified Communications platform benefits from Contact Center skill-based routing, call treatments, reporting, and the graphical Orchestration Designer. Contact Center Agent Desktop supports Avaya Aura® Unified Communications platform phones and continues to support voice, e-mail, and Web chat contact types.

Avaya Aura® Contact Center supports the following Avaya Aura® components:

Avaya Aura® Midsize Business Template 5.2.1.3.6, System Platform 1.1.1.0.2:

- Avaya Aura® Communication Manager 5.2.1
- Avaya Aura® SIP Enablement Services 5.2.1
- Avaya Aura® Application Enablement Services 5.2.1

Avaya Aura® 5.2.1 Standalone server deployment:

- Avaya Aura® Communication Manager 5.2.1
- Avaya Aura® SIP Enablement Services 5.2.1
- Avaya Aura® Application Enablement Services 5.2.2

Avaya Aura® 6.1 Standalone server deployment:

- Avaya Aura® Communication Manager 6.0.1
- Avaya Aura® Session Manager 6.1
- Avaya Aura® Application Enablement Services 6.1

Avaya Aura® 6.2 Standalone server deployment:

- Avaya Aura® Communication Manager 6.2
- Avaya Aura® Session Manager 6.2
- Avaya Aura® Application Enablement Services 6.1.2.0.32 or 6.2

Avaya Aura® Solution for Midsize Enterprise 6.1:

- Avaya Aura® Communication Manager 6.0.1
- Avaya Aura® Session Manager 6.1
- Avaya Aura® Application Enablement Services 6.1

Avaya Aura® Solution for Midsize Enterprise 6.2:

- Avaya Aura® Communication Manager 6.2
- Avaya Aura® Session Manager 6.2
- Avaya Aura® Application Enablement Services 6.1.2.0.32

You must configure the following Avaya Aura® Unified Communications components to work with Contact Center:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager

  Or

  Avaya Aura® SIP Enablement Services server
- Avaya Aura® Application Enablement Services server

You use Avaya Aura® System Manager to configure Avaya Aura® Session Manager.

Avaya Aura® Communication Manager

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

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

- Stations to be used by Avaya Aura® Contact Center agents must be configured appropriately.
- Communication Manager must be configured to route calls to and from Avaya Aura® Contact Center using SIP Enablement Services (SIP Trunks to SES) or Avaya Aura® Session Manager.
- Communication Manager must also be configured for communication with Application Enablement Services (AES) in order to facilitate the station control and monitoring.

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

Avaya Aura® SIP Enablement Services

The Avaya Aura® SIP Enablement Services (SES) application provides connectivity, integration, and a smooth migration path to SIP-based communications. SES is used to deploy SIP telephony alongside existing analog, digital, and IP telephones. Multi vendor telephony can be integrated for enhanced collaboration and productivity. The software is centrally managed and supports SIP trunking, SIP stations, presence, instant messaging, and other SIP-based applications.

SIP calls to the Avaya Aura® Unified Communications platform can be redirected to Contact Center for processing, treatments and routing to appropriate skillsets. To achieve this you must configure the Avaya Aura® SES server to trust the Contact Center Manager Server. To determine which calls to the Avaya Aura® Unified Communications platform are be redirected to the Contact Center Manager Server for processing you must configure a routing entry and contact details for the Contact Center Manager Server in SES.

Avaya Aura® Application Enablement Services

Avaya Aura® Application Enablement Services (AES) are a set of enhanced telephony APIs, protocols, and Web services. These support access to the call processing, media, and administrative features available in Communication Manager. They enable off-the-shelf and custom integration with communications and business applications such as Microsoft Office Communicator, as well as a broad range of Contact Center, Call Recording and Click-to-Dial applications.

The Avaya Device, Media and Call Control (DMCC) APIs provided by Application Enablement Services enable applications to access the physical device, media and basic third-party call control capabilities of Avaya Aura® 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 helps provide privacy and safety. With public key cryptography, two keys are created, one public, one private. Information encrypted with either key can be decrypted only with the corresponding key. Thus, if a message is encrypted with the server private key, it can be decrypted only using the corresponding public key, ensuring that the data can only be from the server.

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 it 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 use by 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 it to create a signed client certificate for the Contact Center side of the secure TLS SIP link. The AES and Contact Center can then communicate securely using a TLS SIP connection.

Avaya Aura® Contact Center Release 6.2 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 your 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.

Avaya Aura® Session Manager

Avaya Aura® Contact Center Release 6.2 supports integration with the Avaya Aura® Session Manager 6.1 and 6.2.

Avaya Aura® Session Manager is a SIP routing and integration tool. It integrates all the SIP entities across the entire enterprise network within a company. Session Manager offers a core communication service that builds on existing equipment but adds a SIP-based architecture. Session Manager connects to and acts as a system-wide dial plan for call processing applications such as:

- Avaya Aura® Communication Manager using direct SIP connections.
- Avaya Communication Server 1000 Release 7.5 SIP-enabled PBX.

Avaya Aura® System Manager

Avaya Aura® System Manager delivers a set of shared, secure management services and a common console across multiple products. You 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.

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 does not support the NRS.

Avaya Communication Server 1000 Release 7.5 uses Session Manager as the SIP Voice Proxy. For more information about configuring Session Manager to support Avaya Communication Server 1000 Release 7.5, see *Avaya Aura® Contact Center Configuration – Avaya CS 1000 Integration* (NN44400-512).

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 CS 1000 Integration* (NN44400-512).

Voice paths are connections that carry speech (phone calls). They are configured as Terminal Numbers (TN) on the switch. The following table shows the voice paths types used for various voice-processing systems.

Voice type path	Voice processing system
virtual ACD (Automatic Call Distribution) agent phones	Avaya CallPilot®
2500 phone TNs	Usually third-party voice-processing systems
2500 phone ACD agent TNs	Usually third-party voice-processing systems
T1 TNs	Usually third-party voice-processing systems
E1 TNs	Usually third-party voice-processing systems

Signaling links are connections that carry auxiliary information, such as treatment directory numbers (DN) between the switch and a voice-processing system. Signaling links are optional, but they ensure maximum cooperation and control between the switch and the voice-processing system.

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).

For information about the supported switch platforms, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Communication with the Contact Center

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

The server runs applications and instructs the switch to 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. The 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 client both connect to the contact center subnet. Third-party applications that interact with the server also connect to this LAN.

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. For more information about the details, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Avaya CallPilot® communication

Avaya CallPilot® provides Voice/Fax Messaging as well as integrated Unified Messaging capabilities through the users' familiar desktop e-mail 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.

SIP and Office Communication Server

Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol to create, modify, and terminate sessions with one or more participants. SIP works with Contact Center to include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP invitations create session descriptions for participants to agree on compatible media types. SIP Contact Center uses elements called proxy servers to help route requests to the user's current location, to authenticate and authorize users for services, to implement provider call-routing policies, and to provide features to users. SIP also provides a registration function for users to upload their current locations for use by proxy servers. SIP uses several transport protocols.

Integration with Contact Center

In Contact Center, an application gateway mediates the SIP signaling from Contact Center Manager Server to Office Communication Server (OCS). This gateway is part of Contact Center Manager Server and is enhanced to add instant messages contact support and capacity improvements.

Avaya Media Server is the supported conferencing and announcement platform. Avaya Media Server also has increased capacity over the previous version so fewer servers are needed for a specified number of agents.

Avaya Aura® Contact Center uses the media processing capabilities of the Contact Center Services for Avaya Media Server (CCSM) component to support conferencing, announcements and dialogs in SIP-enabled Contact Centers.

- Conference–This service creates an Avaya Media Server conference and anchors customer calls, announcements, and agent calls to the Avaya Media Server conference.
- Announcement–This service plays treatments (ringback, announcements) into an Avaya Media Server conference.
- Dialog–This service plays and collects DTMF digits entered in the Avaya Media Server conference.

Each Avaya Media Server in a Contact Center is configured in Contact Center Manager Administration as a Media Server and assigned to handle conference, announcement or/and dialogs Media Services.

In SIP-enabled Contact Centers Avaya Media Server provides default media for standard ringback and busy tones. Contact Center uses these default tones with SIP-based phone calls. Additional media for recorded announcements (RAN) and music must be provisioned in order for Avaya Media Server to provide meaningful media to the customer.

Features

For voice contacts, user interactions are the same. The agent uses Agent Desktop to control an Avaya Communication Server 1000 phone and the usual agent features such as transfer and conference. Instant message contacts are also supported for OCS.

Agents handle the IM contacts on the Agent Desktop the same as other contact types. The agent can also select a colleague in the enterprise (who may be a Contact Center agent or not) and use instant messaging in consultation mode. Presence is supported in Agent Desktop to ensure agents see the colleagues and their current status.

Supported switch platforms

Contact Center provides support for the Avaya Communication Server 1000 software releases and switching platforms for a converged OCS CS 1000 with SIP. For more information, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Chapter 7: High Availability fundamentals

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.

Mission Critical High Availability requirements

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

- Two co-resident Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), License Manager, and Contact Center Manager Administration (CCMA) servers configured as a High Availability pair.
- 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. Avaya Media Server High Availability is supported only 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.
- Optionally, Two Contact Center Multimedia (CCMM) servers configured as a High Availability pair. High Availability also supports CCMM coresident with CCMS, CCT, and CCMA.
- 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, 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.

The following diagram shows a typical Mission Critical High Availability solution.

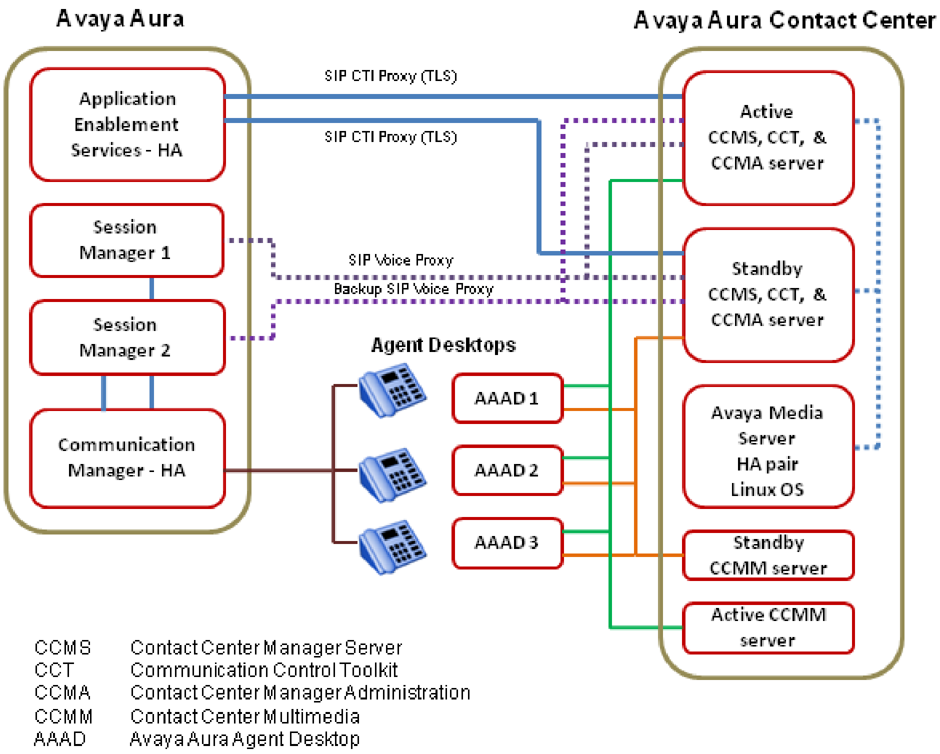
Avaya Aura
Avaya Aura Contact Center
Application Enablement Services - HA
Session Manager 1
Session Manager 2
Communication Manager - HA
SIP CTI Proxy (TLS)
SIP CTI Proxy (TLS)
SIP Voice Proxy
Backup SIP Voice Proxy
Agent Desktops
AAAD 1
AAAD 2
AAAD 3
Active CCMS, CCT, & CCMA server
Standby CCMS, CCT, & CCMA server
Avaya Media Server HA pair Linux OS
Standby CCMM server
Active CCMM server
CCMS Contact Center Manager Server
CCT Communication Control Toolkit
CCMA Contact Center Manager Administration
CCMM Contact Center Multimedia
AAAD Avaya Aura Agent Desktop

Figure 1: Example of a typical Mission Critical High Availability solution

Mission Critical High Availability

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 near real time.

Switchover

In a Mission Critical High Availability campus co-resident 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 (AAAD) 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.

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 co-resident 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 should inform IT staff, who receive an automatic e-mail/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 should 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.

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 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.

Hot-standby High Availability requirements

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

- Two co-resident Contact Center Manager Server (CCMS) and Contact Center Manager Administration (CCMA) servers configured as a High Availability pair.
- Two Communication Control Toolkit (CCT) servers configured as a High Availability pair. High Availability also supports CCT co-resident with CCMS and CCMA.
- Avaya Communication Server 1000 High Availability PBX, Release 6.0 or later.
- Optionally, two Contact Center Multimedia (CCMM) servers configured as a High Availability pair. High Availability also supports CCMM coresident with CCMS, CCT, and CCMA.
- Redundant Ethernet switches.

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.

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

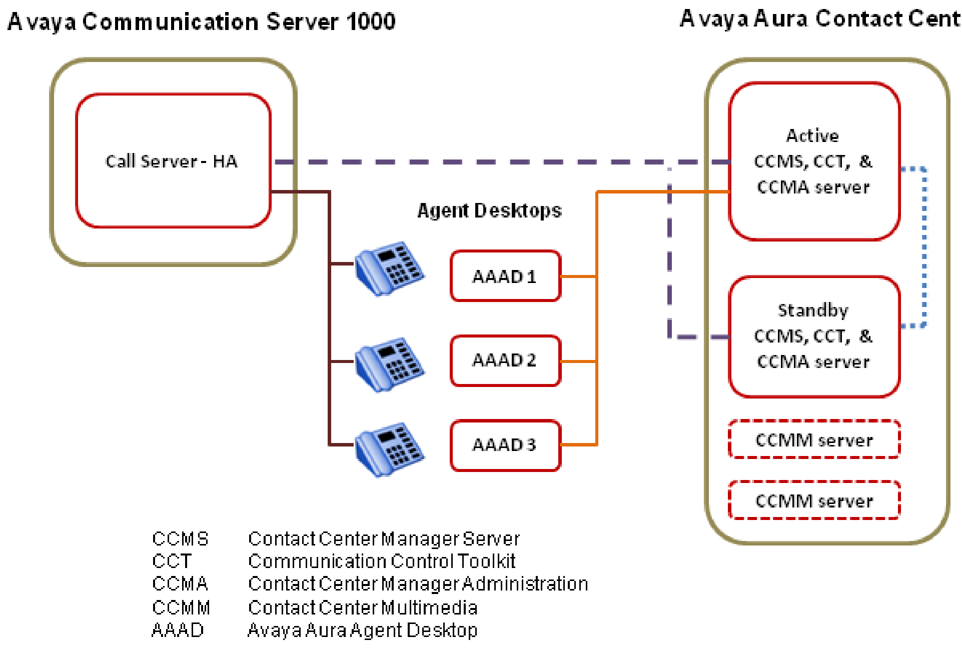
Avaya Communication Server 1000
Avaya Aura Contact Center
Call Server - HA
Agent Desktops
AAAD 1
AAAD 2
AAAD 3
Active CCMS, CCT, & CCMA server
Standby CCMS, CCT, & CCMA server
CCMM server
CCMM server
CCMS Contact Center Manager Server
CCT Communication Control Toolkit
CCMA Contact Center Manager Administration
CCMM Contact Center Multimedia
AAAD Avaya Aura Agent Desktop

Figure 2: Example of a typical hot-standby High Availability solution

Hot-standby High Availability

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.

Agent experience during a switchover

If any Avaya Aura® Contact Center application or server fails, this 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 may 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 (AAAD) 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 switchover multimedia enabled-agents may notice a short delay in receiving new contacts.

Administrator experience during a switchover

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

Warm standby High Availability requirements

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

Avaya Communication Server 1000 based:

- Two co-resident Contact Center Manager Server (CCMS) and Contact Center Manager Administration (CCMA) servers configured as a High Availability pair.
- Two Communication Control Toolkit (CCT) servers configured as a High Availability pair. High Availability also supports CCT co-resident with CCMS and CCMA.
- One or more Avaya Media Server servers. In Contact Center Warm Standby HA solutions, the Avaya Media Server High Availability feature is not supported. In Contact Center Warm Standby HA solutions Avaya Media Server is supported on Windows 2008 Release 2 and Linux. For improved media processing redundancy Contact Center can use an Avaya Media Server cluster. In Contact Center High Availability solutions, Avaya Media Server is not supported co-resident with other Contact Center applications.
- Avaya Communication Server 1000 High Availability PBX.
- Avaya Communication Server 1000 —NES Network Routing Services [SIP Redirect Server (SRS) or SIP Proxy Server (SPS)].
- Optionally, Two Contact Center Multimedia (CCMM) servers configured as a High Availability pair. High Availability also supports CCMM coresident with CCMS, CCT, and CCMA.
- Redundant Ethernet switches.
- This configuration is supported only for Campus High Availability.

Avaya Aura® Communication Manager based:

- Two co-resident Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Manager Administration (CCMA) servers configured as a High Availability pair.
- One or more Avaya Media Server servers. In Contact Center Warm Standby HA solutions, the Avaya Media Server High Availability feature is not supported. In Contact Center Warm Standby HA solutions Avaya Media Server is supported on Windows 2008 Release 2 and Linux. For improved media processing redundancy Contact Center can use an Avaya Media Server cluster. In Contact Center High Availability solutions, Avaya Media Server is not supported co-resident with other Contact Center applications.
- Avaya Aura® Communication Manager (CM).
- Avaya Aura® SIP Enablement Services (SES).
- Avaya Aura® Application Enablement Services (AES).

- Optionally, two Contact Center Multimedia (CCMM) servers configured as a High Availability pair. High Availability also supports CCMM coresident with CCMS, CCT, and CCMA.
- Redundant Ethernet switches.
- This configuration is supported only for Campus High Availability.

Avaya Aura® Midsize Business Template based:

- Two co-resident Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Manager Administration (CCMA) servers configured as a High Availability pair.
- One or more Avaya Media Server servers. In Contact Center Warm Standby HA solutions, the Avaya Media Server High Availability feature is not supported. In Contact Center Warm Standby HA solutions Avaya Media Server is supported on Windows 2008 Release 2 and Linux. For improved media processing redundancy Contact Center can use an Avaya Media Server cluster. In Contact Center High Availability solutions, Avaya Media Server is not supported co-resident with other Contact Center applications.
- Avaya Aura® Midsize Business Template.
- Optionally, two Contact Center Multimedia (CCMM) servers configured as a High Availability pair. High Availability also supports CCMM coresident with CCMS, CCT, and CCMA.
- Redundant Ethernet switches.
- This configuration is supported only for Campus High Availability.

Contact Center Multimedia in standalone configuration:

- Two co-resident Contact Center Manager Server (CCMS) and Contact Center Manager Administration (CCMA) servers configured as a High Availability pair.
- Two Communication Control Toolkit (CCT) servers, configured as a High Availability pair. High Availability also supports CCT co-resident with CCMS and CCMA.
- Two Contact Center Multimedia (CCMM) servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA.
- Redundant Ethernet switches.
- This configuration is supported only for Campus High Availability.

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

- Two co-resident Contact Center Manager Server (CCMS) and Contact Center Manager Administration (CCMA) servers configured as a High Availability pair.
- Two Communication Control Toolkit (CCT) servers, configured as a High Availability pair. High Availability also supports CCT co-resident with CCMS and CCMA.
- Two Contact Center Multimedia (CCMM) servers configured as a High Availability pair. High Availability also supports CCMM co-resident with CCMS, CCT, and CCMA.

- 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, and Avaya Media Server) 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.

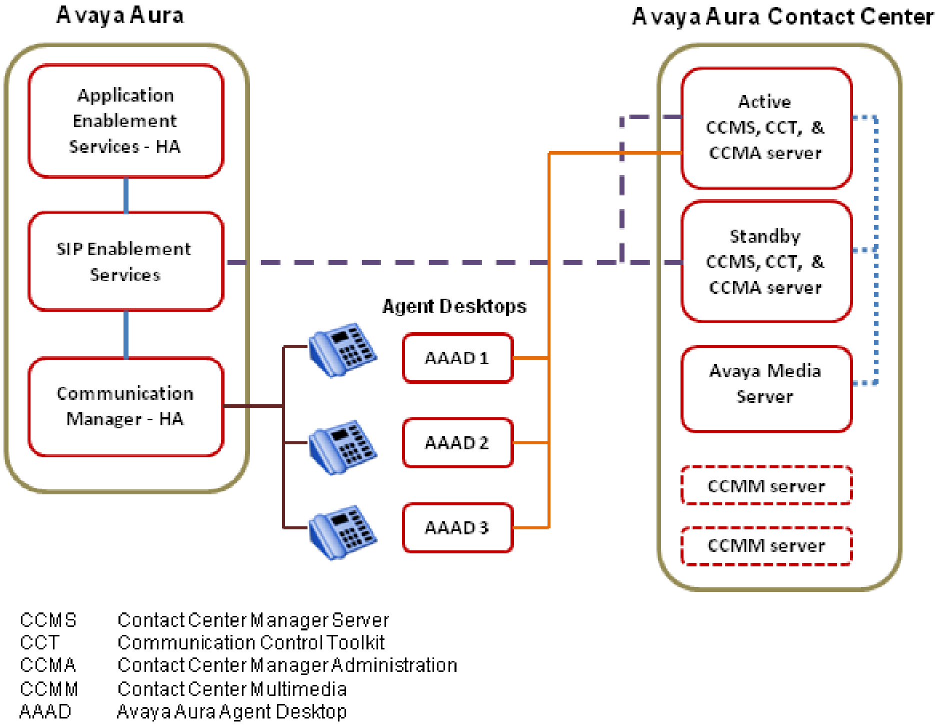
Avaya Aura
Application Enablement Services - HA
SIP Enablement Services
Communication Manager - HA
Agent Desktops
AAAD 1
AAAD 2
AAAD 3
Avaya Aura Contact Center
Active CCMS, CCT, & CCMA server
Standby CCMS, CCT, & CCMA server
Avaya Media Server
CCMM server
CCMM server
CCMS Contact Center Manager Server
CCT Communication Control Toolkit
CCMA Contact Center Manager Administration
CCMM Contact Center Multimedia
AAAD Avaya Aura Agent Desktop

Figure 3: Example of a typical warm standby High Availability solution

Warm standby High Availability

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.

Agent experience during a switchover

If any CCMS or CCT application or server fails, calls in progress between a customer and an agent are maintained, but call control is lost and agents must use their deskphone to complete the customer phone call. The switchover time is approximately five minutes in warm-standby High Availability contact centers. If an Avaya Media Server application or server fails, the media associated with the calls it was handling is lost. If you are using an Avaya Media Server cluster, and if one of the Avaya Media Servers fails, calls in progress on the remaining functional Avaya Media Server(s) are maintained. During the switchover, incoming calls are not processed. Multimedia enabled-agents may notice a short delay in receiving new contacts.

During a CCMS switchover, newly incoming calls are not processed. During an Avaya Media Server, CCMM, or CCT switchover, newly incoming calls are queued and routed in CCMS as usual. Following an Avaya Media Server outage, CCMS continues to anchor newly incoming calls on the remaining Avaya Media Servers in the Avaya Media Server cluster. Engineer the Avaya Media Server cluster to cope with the number of Avaya Media Server outages that you wish to cater.

In a warm-standby High Availability solution Agent Desktop clients are registered with the managed IP address of the CCT High Availability server pair. In multimedia-enabled High Availability solutions Agent Desktop clients are registered with the managed IP address of the active Contact Center Multimedia server.

In the event of a CCMM or CCT switchover, once the standby CCMM or CCT server has transitioned to the active mode and taken over the Managed IP, Agent Desktop clients automatically reconnect to the newly active CCMM or CCT server.

Administrator experience during a switchover

In a warm-standby High Availability campus co-resident solution, the Contact Center Administrator launches Contact Center Manager Administration using the managed name of the co-resident 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.

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 it’s 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 may also be configured that maps to the Managed IP address. This Managed name may be configured on a Domain Name System (DNS) or in the hosts file on the servers that are connecting to the High Availability (CCMS, CCMA, CCT and CCMM) 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. For example, configure the CCT server to connect to the Managed Name of the standalone CCMS server so that the CCT server connects to the Managed IP or Server Name when a switchover of the CCMS occurs.

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. Contact Center applications do not require a restart when a switchover of another Contact Center application occurs. For example, if a Contact Center Manager Server switchover occurs, the Communication Control Toolkit server does not restart but automatically reconnects to the Contact Center Manager Server using the same managed IP address.

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.

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. If the Active server has CCMS and CCT installed then the RGN must have CCMS and CCT 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 co-resident server shadows the Active co-resident server. CCMA on the Standby server replicates CCMA on the Active server. The Standby CCMM server shadows the Active CCMM server. The Remote Geographic Node server, on the remote geographic site shadows the Active co-resident server on the campus site. CCMA on the Remote Geographic Node replicates the CCMA instance on the Active server. The Remote Geographic Node CCMM server shadows the Active CCMM server on the campus site.

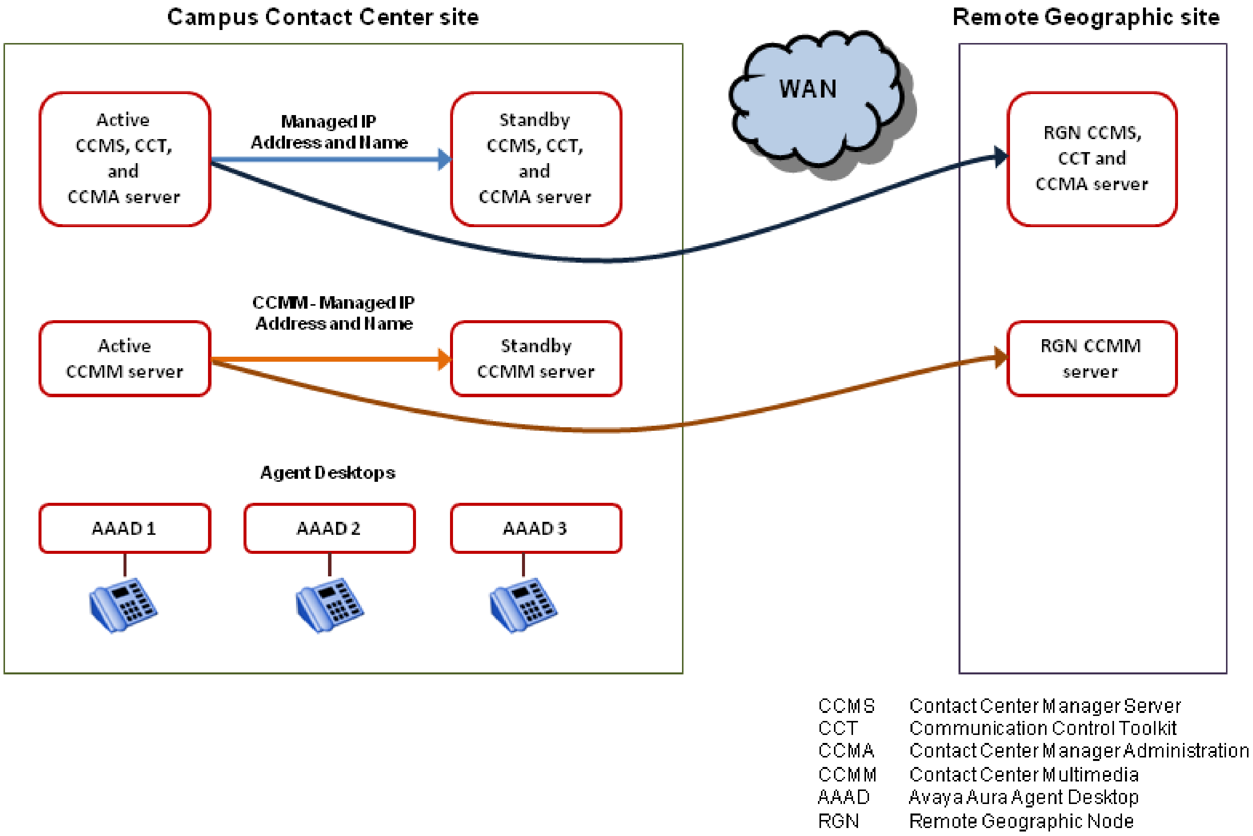
Campus Contact Center site
Remote Geographic site
WAN
Active CCMS, CCT, and CCMA server
Managed IP Address and Name
Standby CCMS, CCT, and CCMA server
RGN CCMS, CCT and CCMA server
CCMM - Managed IP Address and Name
Active CCMM server
Standby CCMM server
RGN CCMM server
Agent Desktops
AAAD 1
AAAD 2
AAAD 3
CCMS Contact Center Manager Server
CCT Communication Control Toolkit
CCMA Contact Center Manager Administration
CCMM Contact Center Multimedia
AAAD Avaya Aura Agent Desktop
RGN Remote Geographic Node

Figure 4: 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 Releases 6.1 or 6.2 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.

Contact Center solutions that use an Avaya Aura® SIP Enablement Services (SES) server or SIP-enabled Avaya Communication Server 1000 PABX do not support geographic High Availability.

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 may 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.

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 co-resident CCMS, CCMA, and CCT RGN server, and a CCMM RGN 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) server with CCMS, CCMA, and CCT installed co-resident.

- Use the HA utility to change the HA Server Mode Configuration from Standby to Active.
- Use the HA utility to disable High Availability. In the HA utility, on the System tab, select “Restore Configuration” to disable High Availability.
- Restore the most recent campus primary CCMA database (mdb) files to the RGN CCMA using selective restore.
- Use the CCMS Server Configuration utility to configure the CS1000 IP addresses for the local CS1000 Survivable Media Gateway.
- Use the CCMS Server Configuration utility to configure the CallPilot IP addresses for the local CallPilot.
- Use the System Control and Monitor Utility (SCMU) to start all services.
- Log on to the RGN CCMA Web administration, use CCMA Configuration to:
    - Edit the configured CCMS properties to point to the RGN CCMS server.
    - Edit the configured CCT properties to point to the RGN CCT server.
    - Edit the configured CCMM properties to point to the RGN CCMM server.
    - Acquire the ACCESS Voice ports for the CS1000 Survivable Media Gateway CallPilot system.
    - In Global Settings, set the Default Access DN to the RGN CallPilot Queue.
- On the CCMS RGN server, use SCMU to restart the CCMS Voice Services VSM service (CCMS VSM_Service).

Remote Geographic Node CCMM configuration

Perform the following steps on the Remote Geographic Node (RGN) server with CCMM installed.

- Launch the CCMM Dashboard and change the CCMA server name to be the RGN CCMA server name.
- Launch Internet Explorer and login to CCMA (using the RGN CCMA server name).

- Under the Launchpad, select “Multimedia” from the drop down list.
- Select the RGN CCMM server and “Launch Multimedia Client”.
- Under General Administration, select Server Settings. Edit the following CCMM settings:
    - Contact Center Manager Server: change to CCMS RGN IP address or name.
    - Contact Center Manager Administration: CCMA RGN IP address or name as edited in CCMM Dashboard.
    - Communication Control Toolkit Server: change to the RGN IP address or name.
    - Standby CCT Server: click Delete to remove.
    - Geographic Alternate CCT server: click Delete to remove.
    - Contact Center Multimedia Server: change to the RGN IP address or name.
    - Contact Center Multimedia Standby Server: click Delete to remove.
    - CC Web Stats: Configure the Contact Center Web Statistics server details.
    - Under Email, select General Settings. The Inbound and Outbound URLs must point to the RGN IP address or name.
    - Click Save to save changes.

The Remote Geographic Node servers are now commissioned to handle voice and multimedia contacts.

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

If the Mission Critical 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 co-resident CCMS, CCMA, LM and CCT RGN server, a standalone CCMM RGN server, and a local standalone Avaya Media Server.

- Stop the High Availability system on the Remote Geographic Node (RGN). Ensure the Remote Geographic Node servers are not shadowing data from the campus site. On the RGN server, using the High Availability configuration utility, configure the HA Server Mode to be “Non HA”.
- Use the RGN CCMS Server Configuration utility to configure the IP addresses for the local Avaya Aura® Session Manager, Avaya Aura® Application Enablement Services, and

IM Provider. Configure Contact Center Manager Server to use a RGN License Manager server.

- Restore the most recent campus primary CCMA database (mdb) files to the RGN CCMA using selective restore.
- From the SMMC System tray icon, select “Start System” to start Contact Center services.
- Log on to the RGN CCMA Web administration, use CCMA Configuration to:
    - Edit the configured CCMS properties to point to the RGN CCMS server.
    - Edit the configured CCT properties to point to the RGN CCT server.
    - Edit the configured CCMM properties to point to the RGN CCMM server.
    - In Global Settings, configure the Default DN as a local attendant console.
    - Configure a local Avaya Media Server as a Media Server.
- Launch the CCMM Dashboard and change the CCMA server name to be the RGN CCMA server name.
- Launch Internet Explorer and login to CCMA (using the RGN CCMA server name).
- Under the Launchpad, select “Multimedia” from the drop down list.
- Select the RGN CCMM server and “Launch Multimedia Client”.
- Under General Administration, select Server Settings. Edit the following CCMM settings:
    - Contact Center Manager Server: change to CCMS RGN IP address or name.
    - Contact Center Manager Administration: CCMA RGN IP address or name as edited in CCMM Dashboard.
    - Communication Control Toolkit Server: change to the RGN IP address or name.
    - Standby CCT Server: click Delete to remove.
    - Geographic Alternate CCT server: click Delete to remove.
    - Contact Center Multimedia Server: change to the RGN IP address or name.
    - Contact Center Multimedia Standby Server: click Delete to remove.
    - CC Web Stats: Configure the local Contact Center Web Statistics server details.
    - Under Email, select General Settings. The Inbound and Outbound URLs point to the RGN IP address or name.
    - Click Save to save changes.
- Reboot all Remote Geographic Node servers.
- Use the Contact Center Manager Server System Control and Monitor Utility (SCMU) to verify that all core Contact Center services started.

The Remote Geographic Node servers are now commissioned to handle voice and multimedia contacts. The Remote Geographic Node servers also support local reporting.

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

If a Mission Critical, Hot-standby or Warm 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 may not get restored on the new campus HA server.

In the following example the campus site has a co-resident CCMS, CCMA, LM and CCT server, a standalone CCMM 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.
- Restore the RGN database backups on the campus active servers.
- On this 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, configure IP addresses for the Active server, Standby server and RGN. Also configure a local Trusted IP address.
- On the CCMS Active server, use the Server Configuration utility to configure the IP addresses for the local Avaya Aura® Session Manager, Avaya Aura® Application Enablement Services, and IM Provider. Configure Contact Center Manager Server to use a local License Manager server.
- On the CCMA Active server, configure the campus CCMS, CCT, CCMM, and Avaya Media Server details.
- On the CCMM Active server, configure the CCMA details in the CCMM Dashboard.
- Using a CCMA Web client, launch the CCMM Administration utility and configure all Server Settings to use local campus resources and servers.
- Reboot all the active servers.
- After active server is up, take the database backup from the active server and restore the backup from the Active server to build the standby server and RGN server again.

High Availability configuration utilities

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

- High Availability Utility (Mission Critical High Availability version) on page 74
- High Availability Utility (Hot-standby and warm standby version) on page 75
- SMMC system tray (for Mission Critical High Availability only) on page 76

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 e-mail server for e-mail notifications
    - Configure where and how often to send e-mail notifications
    - Configure the e-mail character set
- System
    - Display information on the system status

  - Verify that database shadowing is running

High Availability Utility (Hot-standby and warm standby version)

Configure hot-standby and warm standby High Availability resiliency for CCMS, CCT and CCM 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 e-mail server for e-mail notifications
  - Configure where and how often to send e-mail notifications
  - Configure the e-mail 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.

SMMC system tray (for Mission Critical High Availability only)

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)

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.	A
Active HA server with no connection to remote system. This server is configured as a High Availability active server.	A
Active HA server running with connection to remote system, fully HA capable system. A switchover is possible.	A
Active HA server running, but switchovers disabled. A switchover is not possible.	A
Switchover in progress, the active system is switching over to become a Standby system. After the switchover, this server becomes a standby server.	A S
Standby HA server in stopped state. This server is configured as a High Availability standby server.	S
Standby HA server with no connection to remote system. This server is configured as a High Availability standby server.	S
Standby HA server running with connection to remote system, fully HA capable system. A switchover is possible.	S
Standby HA server running, but switchovers disabled. A switchover is not possible.	S
Switchover in progress, the standby system is switching over to become an Active system. After the switchover, this server becomes an active server.	S A
The Geographic Standby server HA system is starting.	G ⇧
The Geographic Standby server HA system is stopping.	G ⇩

High Availability status	SMMC icon
The Geographic Standby server HA system is stopped.	G
The Geographic Standby server HA system is shadowing the Active server, but the Geographic Standby server is not yet synchronized with the Active server.	G
The Geographic Standby server HA system is shadowing and synchronized with the Active server.	G

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.

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

Avaya Aura® Contact Center supports High Availability (HA) resiliency using a pair of Contact Center Manager Server (CCMS) servers.

In a campus solution, one CCMS server actively processes scripts and contacts.This CCMS server is called the active CCMS server. Another CCMS server 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 server is installed on the remote geographic site. The CCMS 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* (NN44400-610).

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 stand-by 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. 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. As both the primary and backup servers are identical in functionality and configuration, the switchover is seamless.

Limitations:

- High Availability can be configured only in 1+1 configuration.
- High Availability is available only if the servers are installed on the Linux operating system.
- Once the backup server becomes active there is no automatic fallback to the primary server.

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

To restore the primary server the administrator must manually set the backup server status to “Failover”, using Avaya Media Server Element Manager.

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, announcement, and dialog 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.

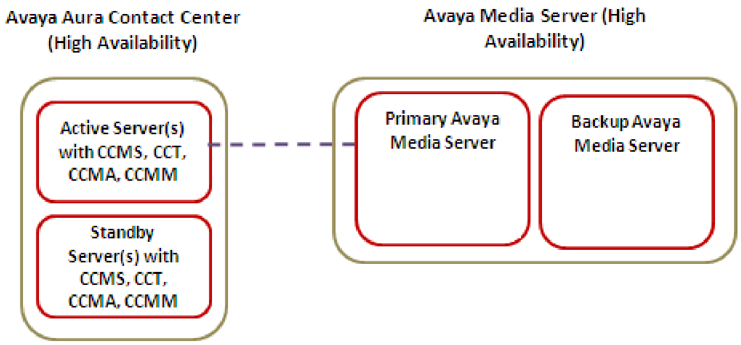
Avaya Aura Contact Center (High Availability)
Active Server(s) with CCMS, CCT, CCMA, CCMM
Standby Server(s) with CCMS, CCT, CCMA, CCMM
Avaya Media Server (High Availability)
Primary Avaya Media Server
Backup Avaya Media Server

Figure 5: 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.

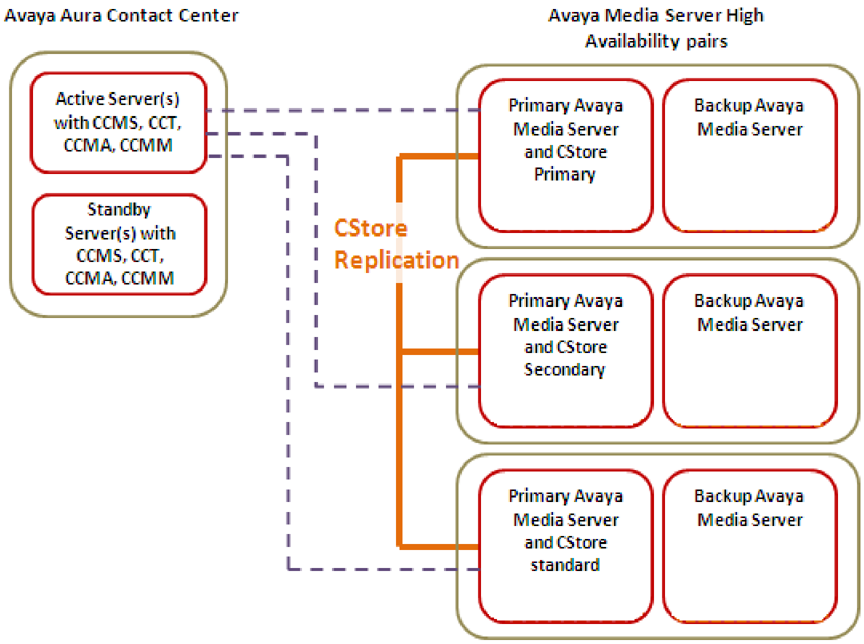
Avaya Aura Contact Center
Avaya Media Server High Availability pairs
Active Server(s) with CCMS, CCT, CCMA, CCMM
Standby Server(s) with CCMS, CCT, CCMA, CCMM
CStore Replication
Primary Avaya Media Server and CStore Primary
Backup Avaya Media Server
Primary Avaya Media Server and CStore Secondary
Backup Avaya Media Server
Primary Avaya Media Server and CStore standard
Backup Avaya Media Server

Figure 6: 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, announcement, and dialog media services.

In a High Availability deployment, when using more than one Avaya Media Server redundant pair, you license each redundant pair separately. On each pair, you install the license file on the primary server and the secondary Avaya Media Server replicates this license automatically.

Avaya Media Server Remote Geographic Node deployment

Where the contact center deploys High Availability with a Remote Geographic Node, implement a cluster of Avaya Media Server at the remote site. Configure one remote Avaya Media Server server in the cluster for each High Availability pair at the campus site. Configure licensing on the remote cluster in the same way as on the standard cluster.

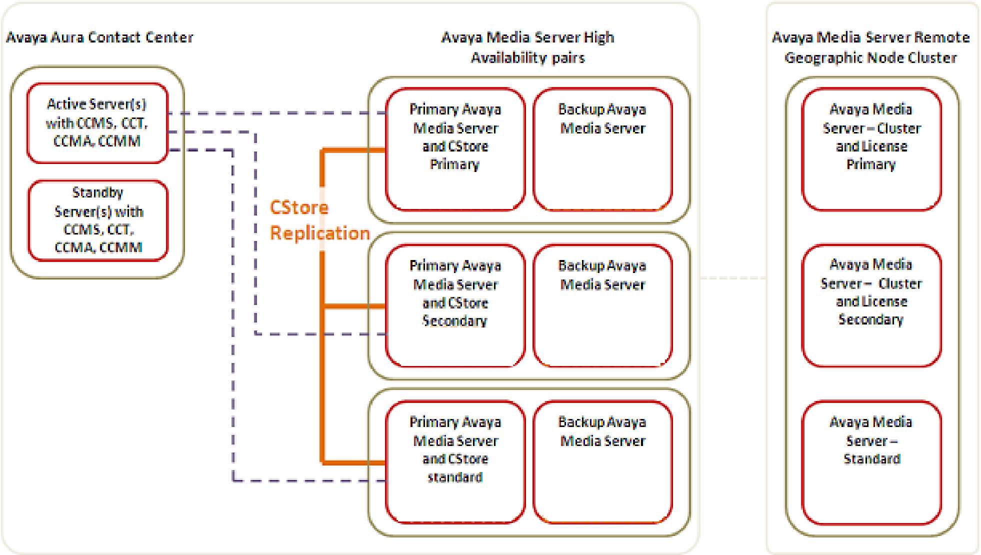
Avaya Aura Contact Center
Active Server(s) with CCMS, CCT, CCMA, CCMM
Standby Server(s) with CCMS, CCT, CCMA, CCMM
CStore Replication
Avaya Media Server High Availability pairs
Primary Avaya Media Server and CStore Primary
Backup Avaya Media Server
Primary Avaya Media Server and CStore Secondary
Backup Avaya Media Server
Primary Avaya Media Server and CStore standard
Backup Avaya Media Server
Avaya Media Server Remote Geographic Node Cluster
Avaya Media Server – Cluster and License Primary
Avaya Media Server – Cluster and License Secondary
Avaya Media Server – Standard

Figure 7: 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.

After switchover to the remote site, the administrator must manually configure each of the remote Avaya Media Server servers separately as a media server on CCMA, and assign it to handle conference, announcement, and dialog media services.

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 server, that the result is replicated to the other server. If the primary CCMA server fails, AD-LDS replication ensures the standby CCMA server is configured with the most recent data.

In a campus co-resident solution the Contact Center Administrator launches Contact Center Manager Administration using the managed name of the co-resident 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 server and a standby CCMA server. The primary CCMA server is installed with the Enable CCMA Replication option not selected. The standby CCMA server is installed with the Enable CCMA Replication option selected. The standby CCMA server replicates the primary CCMA 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.

The primary CCMA server and the standby replication CCMA 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 CCMA servers, to copy or replicate data from the primary CCMA AD-LDS to the standby CCMA AD-LDS.

The primary CCMA server is always the primary CCMA server. 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 CCMA server, or install a new primary CCMA 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 server using the CCMA Backup and Restore utility.

In a combined campus and geographic enterprise solution, a third CCMA server is installed on the remote geographic site. The CCMA 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* (NN44400-610).

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 reports and report definitions
- Audit Trail events

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.

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

In a co-resident 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, which may be required.

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 CCMA server. If the primary CCMA is offline and if you are using the standby CCMA, then regularly backup the standby CCMA server, because this contains the most recent data. Do not store the standby CCMA backup on the standby CCMA 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 co-resident 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* (NN44400-311). For more information about commissioning CCMA, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

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, select AD-LDS replication - Enable CCMA Replication.
- 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* (NN44400-311).

For more information about commissioning CCMA, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

For more information about removing obsolete CCMA replication entries, see *Avaya Aura® Contact Center Upgrade and Patches* (NN44400-410).

For more information about performing switchovers for continuity in the Contact Center, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Communication Control Toolkit

Avaya Aura® Contact Center supports High Availability (HA) resiliency using a pair of Communication Control Toolkit (CCT) servers.

One CCT server actively processes contacts. This CCT server is called the active CCT server. Another CCT server 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. In an AML-based solution where CCT is co-resident with CCMS, a CCT service failure does not initiate an automatic switchover; CCT simply restarts the service and dependant services. In a campus AML-based solution with a pair of standalone CCT servers, an active CCT service failure, hardware, network, or database failure can initiate a switchover. So for improved resiliency in an AML-based solution, use a pair of standalone CCT servers.

In a SIP-enabled solution an active 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 server is installed on the remote geographic site. The CCT 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* (NN44400-610).

Contact Center Multimedia

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

One CCMM server actively processes multimedia contacts. This CCMM server is called the active CCMM server. Another CCMM server 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 server is installed on the remote geographic site. The CCMM 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* (NN44400-610).

For more information about performing switchovers for continuity in the Contact Center or for maintenance, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

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 may 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 has useful data or intrinsics, queue it to the most appropriate skillset as normal. If the call does not have useful data, queue the call to the appropriate default skillset.

Note:

After a High Availability switchover, multimedia contacts may 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. E-mail contacts transferred to agents or Pulled Closed e-mail 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* (NN44400-510).

How to reinstate High Availability resiliency after a switchover

In a Mission Critical, 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 e-mail 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 may 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), stop High Availability shadowing.

  Use the Database Maintenance utility to restore each database application individually from the network share.

  In the High Availability 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* (NN44400-610).

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 update the Standby server details.
- 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* (NN44400-610).

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:

- Avaya Aura® Communication Manager survivability overview on page 93
- Avaya Aura® Session Manager redundancy overview on page 94
- Avaya Aura® Application Enablement Services high availability overview on page 95

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.

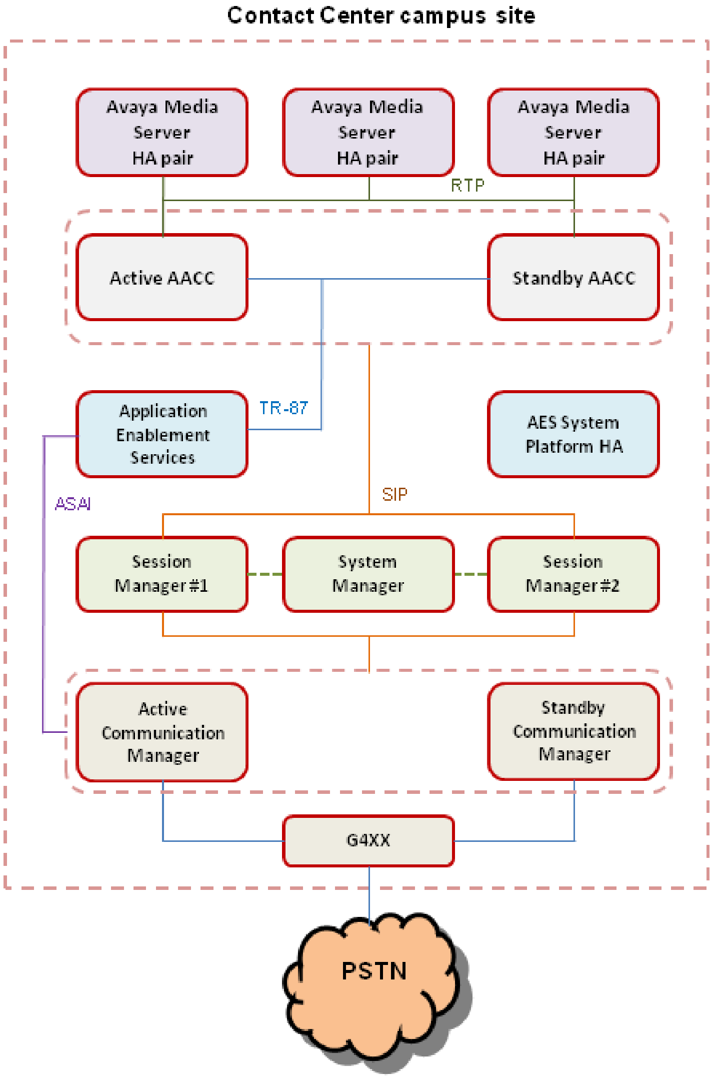
Contact Center campus site
Avaya Media Server HA pair
Avaya Media Server HA pair
Avaya Media Server HA pair
RTP
Active AACC
Standby AACC
Application Enablement Services
TR-87
AES System Platform HA
ASAI
SIP
Session Manager #1
System Manager
Session Manager #2
Active Communication Manager
Standby Communication Manager
G4XX
PSTN

Figure 8: Example of a campus voice-enabled site with platform resiliency

Avaya Aura® 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 must be in close proximity so that they can be connected with the crossover cable.
- The same version of System Platform must be installed on the active and standby nodes.
- Install the Communication Manager Duplex template on both System Platforms.
- Configure a Duplication Link between the pair of 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.

Avaya Aura® Session Manager redundancy overview

Avaya Aura® Session Manager Release 6.1 and Release 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 a CM signaling group to SM-1, you need to add a 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 may be impacted and the agent may have to complete the call using their phone.

Avaya Aura® Application Enablement Services high availability overview

Avaya Aura® System Platform (Releases 6.1 and 6.2) is a real-time virtualization technology that enables applications such as Application Enablement Services to be deployed on supported hardware platforms. System Platform provides a High Availability Failover feature that supports service continuity. System Platform High Availability Failover is a licensed feature and if required it must be purchased when ordering Application Enablement Services (AES) Release 6.1 or Release 6.2.

System Platform High Availability requires two identical servers, an Ethernet crossover cable, and a single license file for the two servers. The two identical System Platform High Availability servers can be addressed and administered as a single entity. If one server fails, the second server automatically becomes available to client applications. Only the active System Platform, called the “preferred node”, provides service. The standby System Platform server monitors the preferred node server. If the preferred node server fails the AES solution template is propagated from the preferred node to the standby node. The standby System Platform server then starts providing service.

System Platform High Availability Failover requirements

System Platform High Availability Failover requires the following:

- Two System Platform supported servers with exactly the same hardware configuration.
- Both servers must be in close proximity so that they can be connected with a crossover cable.
- The same version of System Platform must be installed on the active and standby nodes.
- Install the Application Enablement Services solution template on the active node.
- Do not install a template on the standby node.

The System Platform High Availability Failover feature is configured using the System Platform Web console on the preferred node.

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

AES System Platform switchover

If the standby System Platform node is unable to communicate with the preferred node for more than 30 seconds it declares the active node dead. The standby System Platform then attempts to propagate the AES solution template from the preferred node to the standby node. If the propagation is successful, the standby System Platform server then starts providing service. For a failover due to the total failure of the active node, the total time between the start of the outage and the time when all resources are running on the standby node – the longest switchover time is up to 5.5 minutes.

Contact Center experience during the AES System Platform switchover interval

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 e-mail 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.

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 may 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 97
- Session Manager geographical redundancy overview on page 98
- Application Enablement Services geographical redundancy overview on page 98

Campus site and remote geographic site

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

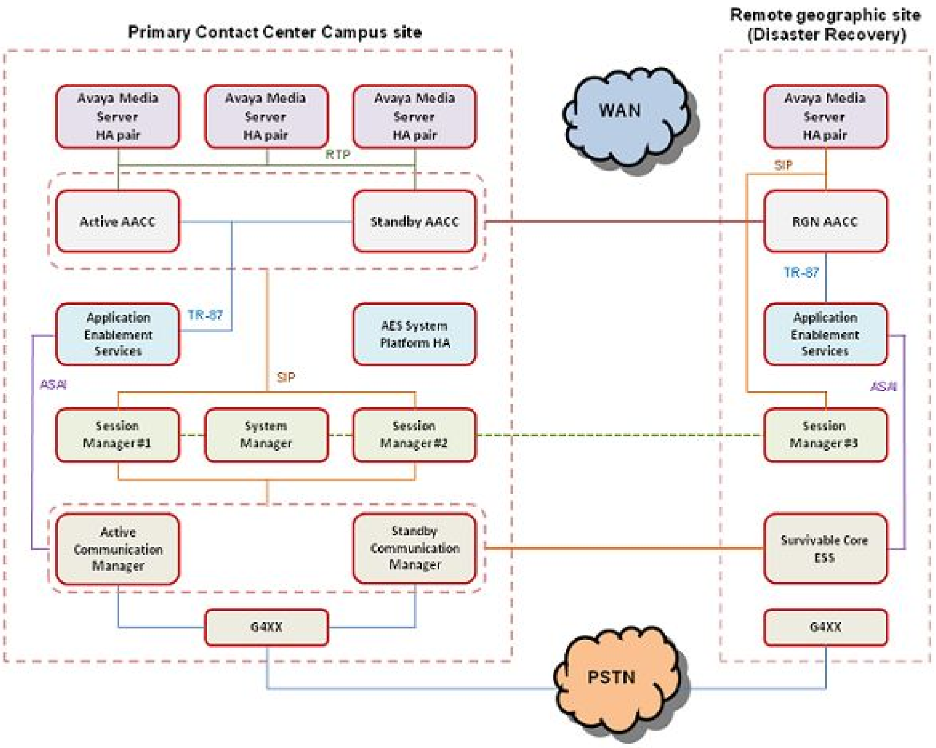
Primary Contact Center Campus site
Remote geographic site (Disaster Recovery)
Avaya Media Server HA pair
Avaya Media Server HA pair
Avaya Media Server HA pair
RTP
WAN
Avaya Media Server HA pair
SIP
Active AACC
Standby AACC
RGN AACC
TR-87
Application Enablement Services
TR-87
AES System Platform HA
Application Enablement Services
ASAI
SIP
ASAI
Session Manager #1
System Manager
Session Manager #2
Session Manager #3
Active Communication Manager
Standby Communication Manager
Survivable Core ESS
G4XX
G4XX
PSTN

Figure 9: 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 Application Enablement Services 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 may 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 Application Enablement Services server to control these calls.

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

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.

You must use Link Aggregation Control Protocol (LACP), NIC Teaming and Virtual Router Redundancy Protocol (VRRP) 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. Even if one NIC fails, the network connection does not cease and continues to operate on other NICs.

Virtual Router Redundancy Protocol (VRRP):

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. Two or more physical routers, such as Avaya ERS 5520, can be configured to stand for a virtual router. If one physical router fails, another physical router automatically replaces it.

Campus High Availability supports LAN environments where the round trip delay is less than 80ms, with less than 0.5% packet loss.

Geographic 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.

You must use Link Aggregation Control Protocol (LACP), NIC Teaming and Virtual Router Redundancy Protocol (VRRP) 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. 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 (SNMP)

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, SNMP alarms, and e-mail 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 may not support Hot Patching and these patches may require a maintenance window. Read the patch Readme file to determine if a patch supports Hot Patching.

If your Contact Center is licensed for active and standby servers, you can patch software to minimize down time during the patching process. You must ensure that you patch both the active and standby servers to the same level of patch.

For more information about Hot patching the active and standby servers, see *Avaya Aura® Contact Center Upgrade and Patches* (NN44400-410).

More information

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* (NN44400-311), *Avaya Aura® Contact Center Commissioning* (NN44400-312) and *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Chapter 8: Installation fundamentals

This chapter describes the concepts and configuration services that you must understand before you begin installation tasks.

Installation process

The installation process is standard across the portfolio into a single installation utility. The DVD Controller manages installation process of the Avaya Aura® Contact Center Release 6.2.

The Contact Center Installation Engine performs the following steps:

1. Back up, then remove existing Contact Center software.
2. Review server requirements and perform PVI checks to ensure the server has the correct partitions.
3. Install third-party applications.
4. Install Contact Center software with customer-specific installation interview.
5. Install Database software and databases with customer-designated location.
6. Configure the resources in the system.

The DVD Controller checks the server hardware, operating system, required third-party software, drive partition sizes before it installs software. For some issues, the Platform Vendor Independent (PVI) checker warns the installer about the problem. In other situations, the PVI Checker blocks the installation. The PVI check results are stored in the `pvicheck.log` file in the Contact Center SysOps log folder.

Use the DVD Controller to choose the platform and then install one or more of the required applications for the server on which you install the software.

Co-resident installations

In Contact Center, you can use multiple combinations of products and product releases to save money on your server resources.

You can install Contact Center Manager Server either on its own server or on a server with other Contact Center applications. When the Contact Center Manager Server is installed on its own server, it is called a stand-alone server. When the Contact Center Manager Administration is installed on a server containing the Contact Center Manager Server it is called a co-resident server. The following table lists the components that can be installed on the same server with the Contact Center Manager Server software.

Agent Desktop is installed automatically when Contact Center Multimedia is installed on the server. You need not install the two applications.

The following table shows which Contact Center applications can co-reside on the same server.

Table 1: Contact Center co-resident configurations

	CCMS	CCMA	CCT	CCMM	LM	Server Utility	Security Framework	Agent Desktop	OD	Avaya Media Server
CCMS	N/A	Yes	Yes (see Note 3)	Yes (see Note 4)	Yes (see Note 4)	Yes	Yes	Yes (see Note 2)	Yes	Yes
CCMA	Yes	N/A	Yes (see Note 1)	Yes (see Note 4)	Yes (see Note 1)	Yes	Yes	No	Yes	Yes
CCT	Yes (see Note 3)	Yes (see Note 1)	N/A	Yes (see Note 4)	Yes (see Note 1)	Yes	Yes	No	Yes	Yes
CCMM	Yes (see Note 4)	Yes (see Note 4)	Yes (see Note 4)	N/A	Yes (see Note 4)	Yes (see Note 4)	No	Yes	Yes	Yes (see Note 5)
License Manager	Yes	Yes (see Note 1)	Yes (see Note 1)	Yes (see Note 4)	N/A	Yes	Yes	No	Yes (see Note 1)	Yes
Server Utility	Yes	Yes	Yes	Yes (see Note 4)	Yes	N/A	Yes	No	Yes	Yes
Security Framework	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes	No
AAAD	Yes	No	Yes	Yes	No	No	Yes	N/A	No	Yes

	CCMS	CCMA	CCT	CCMM	LM	Server Utility	Security Framework	Agent Desktop	OD	Avaya Media Server
OD	Yes	Yes	Yes (see Note 1)	Yes	Yes (see Note 1)	Yes	Yes	Yes	N/A	Yes
Avaya Media Server	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	No	Yes (see Note 5)	Yes (see Note 5)	N/A

Note 1: These applications can co-reside only if CCMS is already installed.
Note 2: CCT must be installed for the Avaya Aura® Agent Desktop (AAAD) stand-alone application to co-reside.
Note 3: CCMA must be installed on the same server for CCT to co-reside with CCMS.
Note 4: CCMA and CCT must be installed on the same server for CCMM to co-reside with CCMS.
Note 5: CCMS, CCMA, CCT, and CCMM must be installed on the same server for Avaya Media Server to co-reside with CCMS. Avaya Media Server is supported only in SIP-enabled Contact Centers. If the agent limit is reached for a SIP-enabled single server install where Avaya Media Server and CCMM are both installed, Avaya Media Server and CCMM must be removed from the server at the same time. Avaya Media Server co-residency is not supported on an Active or Standby High Availability server. Standalone Avaya Media Server is supported in a High Availability solution.

- Any Contact Center applications in this release cannot co-reside with Contact Center applications from previous releases.
- Contact Center Manager Server can co-reside with Contact Center Manager Administration.
- Communication Control Toolkit can co-reside with Contact Center Manager Administration if Contact Center Manager Server is already installed on the same server.
- Contact Center Multimedia can co-reside with Contact Center Manager Server only when Contact Center Manager Administration and Communication Control Toolkit are installed on the same server.
- When Contact Center Manager Administration is co-resident it must only be used to administer the co-resident Contact Center Manager Server and not any other Contact Center Manager Server. Although multiple servers can exist in the same system as a co-resident Contact Center Manager Administration, the co-resident Contact Center Manager Administration server can only administer the Contact Center Manager Server with which it is co-resident.
- The Network Control Center must be administered by a stand-alone Contact Center Manager Administration server. A co-resident Network Control Center and Contact Center Manager Administration server is not supported.

Installation configurations

Contact Center supports the following configurations:

- single-node configuration on Avaya Communication Server 1000 includes the five main Contact Center server applications that work together to route voice contacts from the PABX to an agent telephone:
    - Contact Center Manager Server
    - Contact Center Manager Server Utility
    - Contact Center License Manager
    - Contact Center Manager Administration
    - Communication Control Toolkit

    Note:

    An additional server application, Contact Center Multimedia, can work with the other Contact Center servers to route outbound voice, e-mail messages, Web communications, and instant message contacts.
- direct-connect (Knowledge Worker) on Avaya Communication Server 1000—The Communication Control Toolkit server works with the Contact Center License Manager server to assign calls to agents directly from the PABX.
- network configuration on Avaya Communication Server 1000, a networked configuration of the five main Contact Center server applications that work together in a networked environment to route voice contacts from the PABX to an agent telephone in one of the following locations:
    - Network Control Center
    - one or more Contact Center Manager Servers
    - Contact Center Manager Server Utility
    - Contact Center License Manager
    - Contact Center Manager Administration
    - Communication Control Toolkit

  Note:

  An additional server application, Contact Center Multimedia, can work with the other Contact Center servers to route outbound voice, e-mail messages, Web communications, and instant message contacts for one site.

- universal networking—A deployment of virtual contact centers across all Avaya PABX platforms and Avaya Interactive Voice Response (IVR) systems.

  Your contact center must contain a complete Communication Control Toolkit installation for each PABX. The Open Queue feature must be enabled on Contact Center Manager Server, and CMF is configured on the Communication Control Toolkit servers.
- SIP configuration—A deployment of Contact Center using the session-initiation protocol to support the Office Communications Server from Microsoft. The OCS system allows additional functions in the Contact Center such as instant messaging and agent presence.

Common utilities

Several common utilities are installed with every Contact Center application.

- Patch viewer on page 107
- System Control and Monitor Utility on page 107
- Automated Log Archiver on page 108
- Contact Center Process Monitor on page 108
- Trace Control Utility on page 109
- Grace Period Reset on page 109
- Database Maintenance on page 109
- High Availability on page 110

Patch viewer

Use the Patch viewer to view the patches currently on a Contact Center server. You can use Patch viewer 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.

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.

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.

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.

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 122.

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 6.2 (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 53.

Security Framework deployments

If you plan to use a single security domain to allow single-sign on for multiple applications in your network, you must determine and configure all applications to access the primary security server. The following list describes where the primary security server must be hosted based on the applications that are deployed.

Consider the following applications in your network:

- Avaya Communication Server 1000 Release 7.0.

  If the Avaya Communication Server 1000 application is on your network, it must host the primary security server.
- Contact Center.

  If a Contact Center application is on your network with no Avaya Communication Server 1000 application, use the Contact Center application to host the primary security server.
- Avaya Media Server.

For example, if your network uses Avaya Communication Server 1000 and you want to enable the single-sign on feature for all applications including Contact Center and Avaya Media Server, you must configure Communication Server to host the primary security server, or security domain in your network.

If you do not want your application to be configured as part of the single security domain, follow the documentation for your specific application to configure the security server for the application.

If you configure a backup security server in your network configuration, use the same configuration as described for the primary security application.

Chapter 9: 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 licensing modes. For more detailed information to plan your Contact Center license file, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

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.

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.

Installation configuration

Use the DVD controller to install Contact Center Manager Server as a stand-alone server, with Server Utility and License Manager, or with all of the Contact Center components (Contact Center Manager Administration, Communication Control Toolkit, Server Utility, and License Manager).

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

- DVD controller on page 113
- User configuration on page 114
- Services on page 115
- Components on page 115

DVD controller

The DVD controller installs the following components on your server:

- .NET Framework 3.5 installation
- common components, including the server configuration utility and patch viewer
- available service packs and service pack supplements

User configuration

When installing Contact Center License Manager, you can choose the following items:

- software installation location
- patch installation location
- other options depend on other applications installed with the License Manager

When you install the License Manager for Contact Center, you use one of two license file types. You must ensure that you do not change the extensions for the file for the following mechanisms:

- Key Recovery System (KRS) for software on an Avaya Communication Server 1000 uses a .lic file to record and maintain the licenses for Nodal or Corporate Licensing and the features you use in your contact center.
- WebLM is a Web-based license manager for the SIP-enabled contact center on an Avaya switch. WebLM is hosted on the Apache Tomcat server and uses an .xml file to maintain the status of the licensed features.

Before installing Contact Center Manager Server, you must know whether you are going to use Essential, Nodal Enterprise, or Corporate Enterprise licensing. You must also decide which server is least affected by the real-time operation of the Contact Center License Manager.

You can install the License Manager on the Network Control Center (NCC) server or a Contact Center Manager Server, based on the following rules:

- If you install Contact Center components in a networked environment with a NCC server, and you use Corporate Licensing, you must install the License Manager on the NCC server.
- If you install Contact Center components in a networked environment with an NCC server, and you use Nodal Licensing, you must install the License Manager on Contact Center Manager Server. The NCC server must point to the Contact Center Manager Server node that has a license for the NCC server.
- If you install a single Contact Center Manager Server, install the License Manager on the same server.
- If you install Communication Control Toolkit in a Knowledge Worker environment, in which you have no Contact Center Manager Server, install the License Manager on the Communication Control Toolkit server.

Services

After you install the Contact Center License Manager, several Windows services are configured on the server. You can review the status of a service in the Windows Services, or in the System Control and Monitor Utility.

- CC License Manager—Controls the features licensed in the Contact Center suite.
- CC Log Archiver—Monitors and archives log files across the Contact Center portfolio.
- CC Process Monitor—Monitors and balances the CPU usage of Contact Center processes.

Components

Contact Center License Manager functions are distributed among various components:

- Server software—The server software provides licensing and monitoring of features such as the contact types, open queue, and resiliency.
- Common server utilities—The utilities common to all servers in the Contact Center that provide basic monitoring of the status of the software and the switch. The common server utilities include the Patch Viewer, Log Archiver, Process Monitor, System Control and Monitor Utility, and Trace Control. See Common utilities on page 107.
- Uninstallation—An application used to uninstall Contact Center License Manager components.

Operations performed on the server

The Contact Center Manager Server gathers and routes the contacts. This section contains the following topics:

- Configure and view licenses on page 116
- Understand optional packages on page 116
- Understand licensed features on page 117
- Configure license alarms on page 118
- Choose licensing types on page 119
- Manage standby license manager on page 119
- Maintain switch considerations on page 120

- Licensing mechanisms on page 121
- Update licensing grace period on page 122

Configure and view licenses

The License Manager Configuration utility provides the license name, the maximum number of licenses available, the current number of licenses issues, 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.

Understand optional packages

During the installation of the License Manager, you can apply one or more optional packages based on your license. The following list describes each optional package.

Open Queue

With Open Queue, you can queue voice and multimedia contacts in Contact Center and then route the contacts to agents using the Agent Desktop.

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

Multiplicity

Multiplicity is the ability of an agent to handle multiple concurrent 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 contacts that an agent can be assigned is five.

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.

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.

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.

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.

Understand licensed features

This section describes some of the licensed features in Contact Center. You must use License Manager for Contact Center Release 6.2 applications.

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.

Report Creation Wizard

Report Creation Wizard provides a method to customize historical reports within Contact Center.

Standby Server High Availability

One set of Contact Center applications (a CCMS, a CCT, a CCMA, and an optional CCMM) actively processes scripts and contacts. This set 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 Avaya Contact Center applications monitors and shadows 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 active application fails the standby applications, running in hot standby mode, recognize this failure and start processing. You must configure the standby applications exactly the same as the active applications. Configuration changes to the active system during normal operation are automatically copied to the standby applications. The standby applications are therefore configured correctly if they need to take over processing from the active systems. Statistical data is also automatically copied to the standby applications.

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.

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 Manager servers: 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 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 installation:

- Install 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.
- You must not install the standby License Manager on the standby Contact Center Manager Server because the License Manager cannot run as the active License Manager independently of the Contact Center Manager Server. The active License Manager attempts to write statistics to the standby Contact Center Manager Server and not the primary Contact Center Manager Server which can terminate database shadowing.

Maintain switch considerations

Depending on installation, consider the issues described in the following sections when you configure a Contact Center licensing serial ID.

Avaya Communication Server 1000

The serial ID of the Avaya Communication Server 1000 is the identifier for Nodal Avaya Communication Server 1000 installations.

You can use the MAC addresses, but the license file is shipped with a serial ID rather than the MAC address.

You must enter the serial ID correctly during the installation. If the serial ID does not match the ID used to generate the license file, the Contact Center License Manager cannot start.

Note:

A corporate license file can be generated only from the Contact Center subnet NIC MAC address. The nodal license file can be generated from either the Contact Center subnet NIC MAC address or the Avaya Communication Server 1000 serial ID.

Communication Control Toolkit server

If you use Communication Control Toolkit as part of the Contact Center solution, use the License Manager on the Contact Center Manager Server.

If you plan to use the Communication Control Toolkit server as a stand-alone server (without Contact Center Manager Server), the license identifier is the MAC address of the server.

The MAC address can be MAC address of the NICs; however, you must use the Contact Center subnet MAC address. If the MAC address does not match the MAC address in the license file, the Contact Center License Service cannot start.

SIP server

The only identifier required for SIP installations, including Avaya Aura® Unified Communications platform integrations, is the MAC address of the Contact Center Manager running License Manager.

The MAC address can be any MAC address of the NICs; however, you must use the Contact Center subnet MAC address. If the MAC address does not match the MAC address in the license file, the Contact Center License Service cannot start.

Mixed Corporate node

In all Corporate installations, even if all servers connect to an Avaya Communication Server 1000, servers use the MAC address as the identifier.

The MAC address can be any MAC address of the NICs; however, you must use the Contact Center subnet MAC address. If the MAC address does not match the MAC address in the license file, the Contact Center License Service cannot start.

Licensing mechanisms

When you install the License Manager for Contact Center, you use one of two licensing mechanisms depending on your system configuration: Key recovery system (KRS) or Web LM. You can view the licensed features for both licensing mechanisms using the License Manager Configuration Utility.

At startup, Contact Center identifies the license mechanism and releases the licenses to use.

Key recovery system

If you have an Avaya Communication Server 1000 PBAX, the license mechanism uses a .lic file to record and maintain the licenses for Nodal or Corporate Licensing and the features you use in your contact center.

WebLM

WebLM is a Web-based license manager for the SIP-enabled Contact Center on an Avaya switch. WebLM uses an .xml file to assign and monitor the status of the licensed features.

WebLM supports only a nodal contact center.

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. For more information about the licensing requirements for Avaya Media Server, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Chapter 10: 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.

Each contact type is a licensed feature. See License Manager on page 113.

Installation configuration

Use the DVD controller to install Contact Center Manager Server server as a stand-alone server, with Server Utility and License Manager, or with all of the Contact Center components (Contact Center Manager Administration, Communication Control Toolkit, Server Utility, and License Manager).

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

- DVD controller on page 123
- Default users on page 124
- Services on page 124
- User configuration on page 126
- Components on page 127
- Possible co-resident components on page 128

DVD controller

Use the DVD controller to install the following components on your server:

- .NET Framework 3.5 installation
- Caché database
- CCMS MSI installation

- common components, including the server configuration utility and patch viewer
- database migration tool to convert CCMS 6.0 Sybase database to Caché for Contact Center Release 6.2
- Available service packs and service pack supplements

Default users

The installation adds default users to the Windows operating system when you install Contact Center Manager Server. You must change your passwords for the Avaya user accounts to protect your system from unauthorized access. The local Administrator account is used to configure default users.

Services

After you install the Contact Center Manager Server the following services are created on the server. You can review the status of a service in the Windows Services or in the System Control and Monitor Utility.

Service	Description
Caché Controller for CCDSInstance	Caché controller
CC Log Archiver	Monitors and archives log files across the Contact Center portfolio
CC Process Monitor	Monitors and balances the CPU usage of Contact Center processes
CCMS ASM_Service	Performs agent management and skillset queuing
CCMS AUDIT_Service	Processes all notifications created by the local OA&M service and generates appropriate actions
CCMS Control Service	CCMS Service Controller
CCMS EB_Service	Distributes internal CCMS agent workflow and contact processing events to the reporting services
CCMS ES_Service	Common Object Request Broker Architecture (CORBA) Service for third-party applications to receive Agent related events
CCMS HDC_Service	Calculates CCMS historical reporting statistics from agent workflow and contact processing events
CCMS HDM_Service	Manages the bulk loading of CCMS historical reporting data into the database and consolidates statistics into daily, weekly, and monthly summaries

Service	Description
CCMS Host Application Integration	Integrates CCMS with Telephony Application Program Interface (TAPI) and ODBC databases
CCMS IS_Service	Provides contact intrinsic statistics data to the CCMS task flow engine for application writing
CCMS Avaya Media Server Configuration Manager	Provides wide-ranging data services to components about the state of the local CCMS
CCMS Avaya Media Server Event Scheduler	Schedules and executes CCMS-related service requests to remote clients
CCMS Avaya Media Server Fault Manager	Provides report and event log and alarm processing services
CCMS Avaya Media Server LinkHandler Port #2	Messaging interface between TSM and Avaya CallPilot®
CCMS Avaya Media Server OM Server	Provides monitoring services of local CCMS-related resources
CCMS Avaya Media Server Security	Provides access control, password encryption, and administrative and audit services to the local CCMS
CCMS Avaya Media Server Service Daemon	Starts and restarts Avaya Media Server Service Manager when required
CCMS Avaya Media Server Service Manager	Ensures safe and continued operations of all registered CCMS services
CCMS Avaya Media Server Time Service	Provides CCMS server time to continuously synchronize with the switch
CCMS MLSM_Service	Provides third-party CTI applications call control ability
CCMS NBMSM_Service	Multimedia Services manager
CCMS NBNM_Service	Resolves logical CCMS addresses into physical IP addresses
CCMS NBTSM_Service	Implements the Service Provider Abstraction Layer to the rest of CCMS components
CCMS NCCOAM_Service	Processes messages to and from satellite NDL CCMS
CCMS NDLOAM_Service	Processes messages to and from a dedicated NCC
CCMS NINCCAudit_Service	NCC polling of database connectivity to Nodal servers
CCMS NITSM_Service	Depends on NBTSM service
CCMS OAM_Service	Provides data, controls and communicates changes made to core CCMS data

Service	Description
CCMS OAMCMF_Service	OAM to CMF bridge
CCMS RDC_Service	Calculates CCMS real-time reporting statistics from agent workflow and contact processing events
CCMS RSM_Service	CORBA/IP Multicast to provide basic status reporting capability to third-party application
CCMS SDMCA_Service	Cache of CCMS agent and skillset IDs and assignments and other data used by the Statistical Data Manager components
CCMS SDP_Service	Propagates CCMS real-time statistical data to reporting clients
CCMS SIP_Service	SIP Gateway
CCMS TFA_Service	Third-party applications register for call data
CCMS TFABRIDGE_Service	Win32 Proxy server for RPC calls to CORBA
CCMS TFE Bridge Connector	Bridge Connector for Cisco integration
CCMS TFE_Service	Routes Telephone Calls and Multimedia contacts
CCMS UNE_Service	Universal Networking Engine
CCMS VSM_Service	Play Voice Services to calls placed in the Contact Center

User configuration

When you install Contact Center Manager Server, you can choose the following items:

- switch: either Avaya Communication Server 1000, Microsoft Office Communication Server, or the Avaya Aura® Unified Communications platform
- type of contact center: nodal or networked
- export existing database to migrate to the Contact Center installation
- database installation location
- patch installation location
- customer and site information
- host address for Real-Time statistics multicast (if applicable)
- server and ELAN subnet addresses
- Avaya CS 1000 switch data location

The software installation location, by default, is on Drive D of your server in the Avaya folder.

The SysOps Event log (`D:\sysops.log`) tracks events associated with an installation, reinstallation, upgrade, or uninstallation. It also tracks fatal errors that interrupt these operations. Use a text editor (for example, Notepad) to view the SysOps log.

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. This server runs with Windows Server 2008 Release 2 (Enterprise or Standard).

  For more information about the following utilities on the CCMS server, see *Avaya Aura® Contact Center Server Administration* (NN44400-610):

  - 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).
- The switch—The switch (either an Avaya Communication Server 1000 switch or a Microsoft Office Communication Server) provides telephony services and voice network connectivity.
- 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 Patch Viewer, Log Archiver, Process Monitor, System Control and Monitor Utility, and Trace Control. See Common utilities on page 107.
- 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. See Common utilities on page 107.

- Uninstallation—An application used to uninstall Contact Center Manager Server components.

Possible co-resident components

You can install other components on the Contact Center Manager Server:

- The License Manager—The License Manager software that provides access to features within Contact Center. The License Manager is installed with the Contact Center Manager Server software. Fields and commands for features that you did not purchase are not available.
- Server Utility—See Contact Center Server Utility on page 133.
- Contact Center Manager Administration—See Contact Center Manager Administration on page 151.
- Communication Control Toolkit—See Communication Control Toolkit on page 141. If you plan to install Communication Control Toolkit on the server co-resident with Contact Center Manager Server, you must also install Contact Center Manager Administration on the server.
- Contact Center Multimedia—See Contact Center Multimedia on page 163. If you plan to install Contact Center Multimedia on the server co-resident with Contact Center Manager Server, you must also install Contact Center Manager Administration and Communication Control Toolkit on the server. If you install Contact Center Multimedia co-resident, then you must also install Avaya Media Server. The Avaya Media Server platform is supported only in SIP-enabled contact centers.

For the full list of supported co-residency options, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Operations performed on the server

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

- Gather voice and multimedia contacts on page 129
- Contact routing and queuing on page 129
- Multicast communication on page 129
- Network routing on page 131

Gather voice and multimedia contacts

Contact Center Manager Server connects to a switch 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 e-mail 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.
- 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 may 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* (NN44400-510).

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* (NN44400-311) and *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Optional configuration tools

Two programming tools are available with Contact Center Manager Server:

- Programming units on page 131
- Web services on page 132

Programming units

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. The MLSM interface is typically used to implement softphone features.

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 11: 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 configuration

Use the DVD controller to install Server Utility stand-alone, with Contact Center Manager Server and License Manager, or with all of the voice contact components (Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, and License Manager).

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

- DVD controller on page 133
- User configuration on page 133
- Supported operating systems on page 134
- Components on page 134
- Possible co-resident components on page 134

DVD controller

The DVD controller installs the following components on your server:

- .NET Framework 3.5 installation
- common components, including the server configuration utility and patch viewer
- Available service packs and service pack supplements

User configuration

When installing Contact Center Server Utility, you can choose application installation location.

You must ensure sufficient space exists on the drive for the application or patches on the selected drive.

Supported operating systems

For more information about Server Utility, see the Server Utility Help.

Components

Contact Center Server Utility contains major components of Contact Center Server Utility:

- 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
  - Server Backup—Backup scheduler
  - 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.
- Common server utilities—The utilities that are common to all servers in the Contact Center that provide basic status monitoring of the software and the switch. The common server utilities include the Patch Viewer, Log Archiver, Process Monitor, System Control and Monitor Utility, and Trace Control. See Common utilities on page 107.
- Common database utilities—The utilities that are common to all servers in the Contact Center related to database functions such as backups and restores and the warm standby. The common database utilities are Database Maintenance and High Availability. See Common utilities on page 107.
- Uninstallation—An application used to uninstall Contact Center Manager Server Utility components.

Possible co-resident components

You can install the following components on the Contact Center Manager Server:

- Contact Center Manager Server—See Contact Center Manager Server on page 123.
- License Manager—The License Manager software that provides access to features within Contact Center Release 6.2. Install the License Manager with the Contact Center Manager Server software. Fields and commands for features that you did not purchase are not available.
- Contact Center Manager Administration—See Contact Center Manager Administration on page 151.
- Communication Control Toolkit—See Communication Control Toolkit on page 141. If you plan to install Communication Control Toolkit on the server co-resident with Contact Center Manager Administration, you must also install Contact Center Manager Server on the server.

For the full list of supported co-residency options, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

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 135
- Configure access classes on page 136
- Reset passwords on page 136
- Monitor system configuration settings and performance on page 136
- Manage alarms and events on page 137
- Schedule backups on page 139

Monitor and maintain user permissions

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

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

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

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

Configure access classes

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

Three default access classes are available:

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

Reset passwords

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

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

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

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

The sysadmin password does not expire.

Monitor system configuration settings and performance

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

- serial ports

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

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

- switch resources

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

  The Switch Resources option is not available when you connect to an Avaya 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 2: 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

Feature	In PC Event Browser?	In Alarm monitor?
Automatically show the graphical user interface in the foreground when an event occurs	No	Yes
Clear an event	No	Yes

Schedule backups

You can use the Server Utility Backup Scheduler to schedule backups for the server. To ensure that you can restore system information after a hardware failure or data corruption, schedule regular backups. For more information about scheduling, backup options, and recovery procedures, see *Avaya Aura® Contact Center Server Administration* (NN44400-610). You can schedule a backup at the following times:

- before and after major system operations occur, such as an upgrade or the application of an Emergency Customer Solution
- after major modifications, such as the addition of a large number of users or custom prompts
- after the server is installed and operational

You can schedule backups to run online while calls are handled. (Restores occur offline.) However, because backups compete with services for system resources, schedule backups to run only during off-peak hours when little or no system activity occurs.

Server Utility performs an automatic audit hour (3:00 to 4:00 a.m. server time) to review the content. Avoid scheduling backups during the audit hour; they do not successfully complete.

When you schedule a backup, it appears in the Backup Scheduler window. You must log on as an administrator or ensure that you have administrative privileges to schedule a backup.

You can back up your database to either a local tape drive or a remote directory on a network computer.

Chapter 12: Communication Control Toolkit

The Communication Control Toolkit server 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 configuration

Use the DVD controller to install Communication Control Toolkit stand-alone, with License Manager for a Knowledge Worker configuration, or with all of the contact components (Contact Center Manager Server, Contact Center Manager Administration, Server Utility, and License Manager). If you plan to install Communication Control Toolkit with Contact Center Manager Server, you must also install Contact Center Manager Administration on the server.

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

- DVD controller on page 141
- Modes of operation on page 142
- User configuration on page 143
- User accounts on page 143
- Services on page 144
- Components on page 144
- Possible co-resident components on page 145

DVD controller

The DVD controller installs the following components on your server:

- .NET Framework 3.5 installation
- Caché database
- common components, including the server configuration utility and patch viewer

- database migration tool to convert CCT database to Caché
- available service packs and service pack supplements
- CCT-IVR
- TAPI connector

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, the Communication Control Toolkit server connects to the Contact Center subnet. Avaya recommends that this subnet be 10/100 Mb/s Ethernet. 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 1 ELAN TCP/IP link. If the ELAN subnet is not already connected to the Contact Center subnet through a router. The proprietary protocol Application Module Link (AML) communicates between the Avaya Communication Server 1000 and the TAPI Service Provider.

If you use Communication Control Toolkit as a TAPI server, a direct-connect configuration is used. The Communication Control Toolkit server requires an ELAN subnet with a minimum 10/100 Mb/s Ethernet if the ELAN subnet is not already connected to the Contact Center subnet through a router. Avaya recommends that the Contact Center subnet be a 100 Mb/s ethernet call capacity.

User configuration

When you install Communication Control Toolkit, you can choose the following options:

- application installation location
- database installation location
- patch installation location
- select the primary or secondary server for the configuration

You choose the software installation location when you perform the installation. You must ensure that sufficient space is available on the drive for the application, database, or patches on the selected drive.

The SysOps Event log (`D:\sysops.log`) tracks events associated with any installation, reinstallation, upgrade, or uninstallation. It also tracks fatal errors that interrupt these operations. Use a text editor (for example, Notepad) to view the SysOps log.

User accounts

No default user accounts are configured on the Communication Control Toolkit.

To test Communication Control Toolkit connections with the Contact Center Manager Server, you must create at least one Windows user who can log on and receive voice contacts.

Services

After you install Communication Control Toolkit, the following services are created on the server. You can review the status of a service in the Windows Services, or in the System Control and Monitor Utility.

- Caché Service
- NCCT SMON
- NCCT Logging Service
- ACD Proxy (for Avaya Communication Server 1000)
- Telephony (for Avaya Communication Server 1000)
- NCCT Data Access Layer
- NCCT TAPI Connector (for Avaya Communication Server 1000)
- NCCT Server
- NCCT OI Service (for SIP Office Communication Server)

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. This server runs with Windows Server 2008 Release 2 (Enterprise or Standard).

  For more information about the following utilities on the CCT server, see *Avaya Aura® Contact Center Server Administration* (NN44400-610):
- 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 the 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 Patch Viewer, Log Archiver, Process Monitor, System Control and Monitor Utility, and Trace Control. See Common utilities on page 107.

- 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. See Common utilities on page 107.
- Uninstallation—An application used to uninstall Communication Control Toolkit components.

Possible co-resident components

You can install other components on the Communication Control Toolkit server:

- Contact Center Manager Server and Contact Center Manager Administration—See Contact Center Manager Server on page 123 and Contact Center Manager Administration on page 151. You must install both software applications with Communication Control Toolkit on the same server.
- License Manager—You can install the License Manager software co-resident in a Contact Center environment. If you use Communication Control Toolkit in a Knowledge Worker environment, you must install the License Manager on the Communication Control Toolkit server because no Contact Center Manager Servers are available. The License Manager provides access to features within Contact Center Release 6.2.
- Avaya Aura® Agent Desktop—If your Contact Center is not multimedia-enabled, you can install the Agent Desktop to access the telephone functions from the switch on the softphone.

For the full list of supported co-residency options, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

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 146
- Configure resources on page 146
- Route and queue contacts on page 148
- Connect with switches on page 149
- Verify connection with switch on page 149

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:

- 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 e-mail 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 e-mail 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:

- In this release CCT the manually enabled automatic mapping feature is updated to an automatic mapping feature. When a terminal is assigned to an agent, CCT automatically assigns the addresses associated with a terminal to the respective 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. In the previous release, the automatic mapping feature was manually enabled in the CCT Snap-in; however the administrator had to enable this feature. Now this feature is automatic.
- 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 assign 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 3: Possible 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* (NN44400-610).

Route and queue contacts

The Contact Management Framework manages the states of contacts, agents, terminals, and addresses.

The Contact Management Framework (CMF) is a central repository for objects representing communications, including endpoints (terminals and addresses), transactions (contacts), and the relationships between them. The CMF includes the contact, resource, and agent managers. The CMF is also an abstraction or unification layer for various communications switch interfaces. The Communication Control Toolkit API objects have a one-to-one mapping with the objects in the CMF.

The CMF is driven by one or more switch interface service providers (for example, a connector for Avaya Communication Server 1000 communications or a SIP provider for SIP-enabled Contact Center). The switch interface service provider updates the CMF objects to reflect the status of the switch and to monitor the objects in the CMF for requests, which the objects pass to the switch.

The Contact Management Framework is configured in Communication Control Toolkit Snap-in under Deployment Type.

Connect with switches

The Telephony Application Program Interface (TAPI) Connector is a connector that converts Communication Control Toolkit requests to TAPI calls, and TAPI events to Communication Control Toolkit events. The TAPI Connector is between the Avaya TAPI Service Provider and the Contact Management Framework. The TAPI Connector is not used in SIP-enabled contact centers.

A SIP Connector is a SIP-enabled contact center that uses a Communication Control Toolkit connector to accommodate Contact Center Manager Server agent logons from the Agent Desktop application and other CTI interactions.

Verify connection with switch

The Reference Client is installed automatically on the Communication Control Toolkit server and mimics a telephone device. You can use the Reference Client to simulate telephone calls, to transfer telephone calls, and to handle other telephone events to test the functionality of the Communication Control Toolkit database.

Use the Reference Client to verify calls on one switch or calls transferred between switches.

Optional configuration tools

You can use the additional configuration tools installed with Communication Control Toolkit.

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. Two abstraction layers are also available:

- the Lite Communication Control Toolkit API
- the Graphical Communication Control Toolkit API

You can implement these layers using the Full Communication Control Toolkit API. These layers provide 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:

- 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.

One example of a Communication Control Toolkit client application is the Agent Desktop. If your Contact Center is licensed to handle only telephony calls, you can install the Agent Desktop telephony toolbar on the Communication Control Toolkit server to provide agents with a softphone on their desktop. The Agent Desktop telephony toolbar is a component on the Contact Center Multimedia server software.

Chapter 13: 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 configuration

Use the DVD controller to install Contact Center Manager Administration stand-alone; or with Contact Center Manager Server, Server Utility and License Manager; or with all Contact Center components of Avaya Aura® Contact Center (Contact Center Manager Administration, Communication Control Toolkit, Server Utility, and License Manager).

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

- Prerequisites on page 152
- Requirements on page 152
- DVD controller on page 152
- User configuration on page 152
- Default users on page 153
- Services on page 153
- Components on page 154
- Possible co-resident components on page 155

Prerequisites

Before you install Contact Center Manager Administration, you must install the following applications. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).

- configure Internet Information Service (IIS)
- configure proxy settings in Internet Explorer

If you plan to report on data from a Contact Center Manager Server from Release 6.0 or earlier, you must also install the following applications. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).

- install Sybase Open Client 12.5
- update the Sybase ODBC driver

Requirements

Windows Server 2008 Release 2.0 supports Contact Center server software. Information about hardware and software requirements for stand-alone and co-resident servers and Windows Server 2008 requirements are described in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

DVD controller

The DVD controller installs the following components on your server:

- .NET Framework 3.5 installation
- Active Directory Lightweight Directory Services (AD-LDS) database (formerly known as ADAM)
- common components, including the server configuration utility and patch viewer
- available service packs and service pack supplements

User configuration

When installing Contact Center Manager Administration, you can choose the following items:

- application installation location
- database installation location
- patch installation location

- enable or disable Active Directory Lightweight Directory Services (AD-LDS) replication
- LDAP port number
- SSL port number

You choose the software installation location during the installation. You must ensure that enough space exists on the drive for the application, database, or patches on the selected drive.

The SysOps Event log (`D:\sysops.log`) tracks events associated with any installation, reinstallation, upgrade, or uninstallation operation. It also tracks fatal errors that interrupt these operations. Use a text editor (for example, Notepad) to view the SysOps log.

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.
- 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 who log on to the CCMA application as a new user (NOT the webadmin account) to perform configuration.

Services

After you install the Contact Center Manager Administration the following services are created on the server. You can review the status of any service in the Windows Services or in the System Control and Monitor Utility.

- CC Log Archiver—Monitors and archives log files across the Contact Center portfolio
- CC Process Monitor—Monitors and balances the CPU usage of Contact Center processes
- CCMA ICEEMHLPService—CCMA Emergency Help Service

- CCMA IceRTDService—CCMA Real Time Display Service
- CCMA LMService—CCMA License Manager Service

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. This server runs with Windows Server 2008 Release 2 (Enterprise or Standard).

  For more information about the following utilities on the CCMA server, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611):

  - 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* (NN44400-611))
  - Configuration (see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611))
  - Scripting (see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510))
  - Real-Time Reporting (see *Avaya Aura® Contact Center Performance Management* (NN44400-710))
  - Historical Reporting (see *Avaya Aura® Contact Center Performance Management* (NN44400-710))
  - Report Creation Wizard (see *Avaya Aura® Contact Center Performance Management* (NN44400-710))
  - Emergency Help (see *Avaya Aura® Contact Center Performance Management* (NN44400-710))

  - Audit Trail (see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611))
  - Agent Desktop Displays (see Agent Desktop Displays online Help)
  - Outbound (see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611))

- CCMA database—The CCMA database is configured using the Contact Center Manager Administration application. The CCMA database stores reports, report schedules, and report statistics.
- Common server utilities—The utilities common to all servers in the Contact Center that provide basic status monitoring for the software and the switch. The common server utilities include the Patch Viewer, Log Archiver, Process Monitor, System Control and Monitor Utility, and Trace Control. See Common utilities on page 107.
- Common database utilities—The utilities that are common to all servers in the Contact Center related to database functions such as backups and restores and the warm standby. The common database utilities are Database Maintenance and High Availability. See Common utilities on page 107.
- Uninstallation—An application used to uninstall Contact Center Manager Administration components.

Possible co-resident components

The DVD controller installs several components on the Contact Center Manager Server:

- Contact Center Manager Server —See Contact Center Manager Server on page 123.
- License Manager—The License Manager software that provides access to features within Contact Center. The License Manager is installed with the Contact Center Manager Server software. Fields and commands for features that you did not purchase are not available. See License Manager on page 113.
- Server Utility—See Contact Center Server Utility on page 133.
- Communication Control Toolkit—See Communication Control Toolkit on page 141. If you plan to install Communication Control Toolkit on the server co-resident with Contact Center Manager Administration, you must also install Contact Center Manager Server on the server.
- Security Framework—The Security Framework provides identity management for integration with the customer's directory services infrastructure (for example, Active Directory) for authentication and authorization of application users.

For the full list of supported co-residency options, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

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 156
- Perform off-line configuration on page 156
- Manage users and skillsets for users on page 157
- Create script or flow applications on page 157
- Report real-time data on page 158
- Review real-time reports in Agent Desktop Display on page 158
- Report historical data on page 159
- Configure emergency support for agents on page 160
- Monitor configuration changes on page 160
- Create outbound campaigns on page 160

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* (NN44400-611).

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* (NN44400-610). 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* (NN44400-611).

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

For information and procedures to manage users and skillsets in your Contact Center, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

Create script or flow applications

Contact Center Manager Administration 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 offsite configuring a customer Contact Center, you can upload your Contact Center Manager applications by using the Orchestration Designer component on a client.

For more information about creating applications in the Orchestration Designer, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

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

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* (NN44400-710). To understand the fields in the real-time reports, see *Avaya Aura® Contact Center Performance Management Data Dictionary* (NN44400-117).

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) 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 e-mail 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* (NN44400-710). To understand the fields in the historical reports, see *Avaya Aura® Contact Center Performance Management Data Dictionary* (NN44400-117).

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* (NN44400-611).

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 (NN44400-611)*.

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* (NN44400-610). For information and procedures to create outbound campaigns in your Contact Center, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

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 161
- AD-LDS replication on page 161
- Logon warning message on page 162
- Security Framework on page 162

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 server fails, AD-LDS replication ensures the standby CCMA server 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 the 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 enable the Security Framework, the error message on the domain server overrides the logon message.

Security Framework

The Security Framework provides identity management, which enables integration with the customer's directory services infrastructure (for example Active Directory) for authentication and authorization of application users. The identify framework helps to reduce the administrative costs and eliminates the redundant user information associated with application 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.

If you plan to use the Security Framework for your Contact Center, Avaya recommends that you do not use the Contact Center Manager Administration security.

Chapter 14: Contact Center Multimedia

The Contact Center Multimedia server applications expand the Contact Center to allow agents to view, respond to, and track requests over the Internet. 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:

- E-mail
- Web communications
- Outbound
- SMS text
- Faxed document
- Scanned document
- Voice mail

Where Contact Center Multimedia connects to an OCS Contact Center, it supports Instant Message (IM) contacts. In addition, the Agent Desktop supports call control of voice contacts from the Avaya Aura® Agent Desktop toolbar.

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 configuration

Use the DVD controller to install Contact Center Multimedia. For large Contact Center deployments, Contact Center Multimedia must be installed on a stand-alone server. The following sections provide the information you need to install Contact Center Multimedia:

- DVD controller on page 164
- User configuration on page 164
- Default users on page 165

- Services on page 165
- Folder structure on page 165
- Components on page 166
- Co-resident components on page 166

DVD controller

Use the DVD controller to install the following Contact Center Multimedia components and supporting software on your server:

- .NET Framework 3.5 installation
- Caché database
- Multimedia server applications
- common components, including the server configuration utility and patch viewer
- available service packs and service pack supplements

User configuration

You can choose a range of installation options when you install Contact Center Multimedia. Certain options depend on the types of contacts for which you have licenses.

- application installation location
- database installation location
- patch installation location
- Contact Center Manager Server name
- Contact Center Manager Administration server name
- Communication Control Toolkit server name
- inbound mail server (if applicable)
- outbound mail server (if applicable)
- predictive reporting server (if applicable)
- predictive server (if applicable)
- Web server (if applicable)
- license server name

You must ensure that you have enough space for the application, database, or patches on the server hard disk selected. The SysOps Event log (`D:\sysops.log`) tracks events associated with any installation, reinstallation, upgrade, or uninstallation. It also tracks fatal errors that interrupt these operations. Use a text editor (for example, Microsoft Notepad) to view the SysOps log.

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.

Services

After you install Contact Center Multimedia, the following services are created on the server. You can review the status of a service in the Windows Services, or in the System Control and Monitor Utility.

- CC Log Archiver: Monitors and archives log files across the Contact Center portfolio.
- CC Process Monitor: Monitors and balances the CPU usage of Contact Center processes.
- Multimedia Contact Manager: Provides management services to configure the Multimedia server through Contact Center Manager Administration (CCMA).
- CCMM OAM service: Monitors the connections between Contact Center Multimedia and external servers.
- Campaign Scheduler service: Schedules outbound campaigns in the appropriate time zones and within regulatory times for each country to perform outgoing voice contacts.

Folder structure

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

- `Avaya/Contact Center/E-mail Attachments/inbound`
- `Avaya/Contact Center/E-mail 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* (NN44400-312).

Components

Contact Center Multimedia contains several major components:

- Server software: The server software handles multimedia contacts. This server runs with Windows Server 2008 Release 2. For more information about the following utilities on the CCMS server, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).
- 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 Patch Viewer, Log Archiver, Process Monitor, System Control and Monitor Utility, and Trace Control. See Common utilities on page 107.
- 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. See Common utilities on page 107.
- Uninstallation: An application used to uninstall Contact Center Multimedia components.
- 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).

Co-resident components

If you plan to install Contact Center Multimedia on the server co-resident with Contact Center Manager Server, you must also install Contact Center Manager Administration and Communication Control Toolkit on the server. If you install Contact Center Multimedia co-resident, then you must also install Avaya Media Server.

Operations performed on the server

In a multimedia Contact Center, the Contact Center Multimedia server gathers Internet 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 the CCMS and CCMM servers.

For more detail about the relevant procedures, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

This section contains the following topics:

- Configure e-mail settings on page 167
- Configure IM settings on page 169
- Configure Web communications settings on page 170
- Configure outbound settings on page 171
- Configure Predictive Outbound settings on page 172
- Configure voice mail settings on page 173
- Configure scanned document settings on page 174
- Configure SMS text settings on page 175
- Configure faxed document settings on page 176
- Configure Agent Desktop settings on page 177
- Configure General settings on page 178
- Handle contacts on page 179
- View and update customer information on page 180
- Create callbacks on page 180
- Report multimedia data on page 181
- Archive multimedia database content on page 181

Configure e-mail settings

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

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

E-mail is a text-based communication with clients using an e-mail client such as Microsoft Exchange.

To configure e-mail routing, you must create or configure the following items:

- Route points: Assign a route point to each e-mail 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 e-mail servers: Configure the names and e-mail transfer protocol for the e-mail servers in your organization.
- Inbound e-mail settings: Configure how frequently your Multimedia server scans the corporate server for new messages, and where e-mail attachments are stored.
- Outbound e-mail settings: Configure the outgoing e-mail address or contact information when an e-mail 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 e-mail 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 e-mail server that you use to receive inbound e-mail messages intended for the Contact Center.
- E-mail rules and rule groups: E-mail rules determine how an e-mail contact is routed based on information in or about the e-mail 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 e-mail (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 e-mail rules to send automatic responses based on the information in the e-mail contact. The E-mail Manager automatically sends the response to the customer without routing the contact to an agent.
- Suggested message responses: You can configure e-mail 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 e-mail that satisfies one rule, you can promote the suggested response to an automatic response for the rule.

- Barred addresses: Configure e-mail addresses to which your Contact Center environment does not respond.
- Automatic phrases: You can create templates containing text that agents commonly use in e-mail 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 e-mail contacts, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

If you use Microsoft Exchange 2007 on your e-mail server, configure authentication settings. For more information, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Configure IM settings

In a SIP OCS 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 e-mail 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* (NN44400-610).

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 e-mail 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* (NN44400-610).

Web communications customer interface

If you enable Web communications in your Contact Center, you can use the Sample Customer Interface (CI) Web site to help you develop Web pages for your corporate Web site. The Web services architecture is a platform-independent interface that can be accessed by customers from both Microsoft .NET and Java applications. Customer Web sites or third-party applications use the open interface for integration with the Avaya Contact Center Multimedia system.

In development, you can access the Web services from either ASP.NET or JSP Web applications.

The Customer Interface Web services provide several methods to perform the following functions:

- register new customers in the Contact Center Multimedia database
- log on or log off existing customers
- update customer logon credentials
- create customer contacts
- update customer details
- read customer information
- review a customer contact history
- request immediate or scheduled callback requests
- read a contact
- create and maintain a Web communications chat session

For developers who want to integrate with the Avaya Contact Center Multimedia system using Web Services, the following items are available on the Avaya Developer Partner Program Web site:

- Web Service documentation including an API reference in HTML format
- an installation package for the Sample Customer Interface Web site

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 you can contact the customer.

For information about configuring the administration settings for outbound contacts, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

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* (NN44400-611).

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. Avaya strongly recommends that agents use Agent Desktop for all 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 (e-mail 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* (NN44400-106).

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 e-mail 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 e-mail messages generated by the voice mail system arrive in a mailbox monitored by the E-mail 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, e-mail 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 e-mail transfer protocol for the mailbox from which E-mail 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* (NN44400-610).

If you use Microsoft Exchange 2007 on your e-mail server, configure authentication settings. For more information, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Configure scanned document settings

Combined with Contact Center Multimedia, the e-mail messages generated by the document imaging servers arrive in a mailbox monitored by the E-mail 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, e-mail response, Web chat, or a response through the document imaging server. To respond through the document imaging server, the agent uses an e-mail editor to compose the response, and the E-mail 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 e-mail transfer protocol for the mailbox from which the E-mail 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 e-mail 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* (NN44400-610).

If you use Microsoft Exchange 2007 on your e-mail server, configure authentication settings. For more information, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Configure SMS text settings

To handle SMS text contacts, Contact Center Multimedia operates with an SMS-E-mail gateway. The gateway converts SMS messages into e-mail messages and forwards these to a mailbox. The E-mail Manager monitors the mailbox and picks up the e-mail 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, e-mail response, web chat, or SMS response. For an SMS message, the agent uses an e-mail editor to compose the text, and the E-mail 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 e-mail transfer protocol for the mailbox from which E-mail 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 e-mail 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* (NN44400-610).

If you use Microsoft Exchange 2007 on your e-mail server, configure authentication settings. For more information, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

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 e-mail 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 e-mail messages generated by the fax server arrive in a mailbox monitored by the E-mail 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, e-mail response, Web chat, or fax. If they respond with a fax, the agent uses an e-mail editor to compose the fax message, and the E-mail 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 e-mail transfer protocol for the mailbox from which E-mail 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 e-mail response to the fax contact. The fax server picks up this e-mail response and converts it to a fax. The fax server must be configured to monitor this mailbox for e-mail messages to convert.

For information about configuring the administration settings for faxed document contacts, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

If you use Microsoft Exchange 2007 on your e-mail server, configure authentication settings. For more information, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Configure Agent Desktop settings

Use the CCMM Administration component of Contact Center Manager Administration to configure how the 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, the contact is placed into the pending state automatically. The default time is 1 hour (60 minutes).
- 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 the Agent Desktop. With hot desking enabled and properly configured, when agents start the 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 e-mail 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.
- 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 the Agent Desktop for multimedia contacts, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

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 e-mail (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 e-mail 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* (NN44400-610).

Handle contacts

Agents use the Agent Desktop application to process e-mail, 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* (NN44400-114).

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
- E-mail
- Fax
- Instant Message, supported on an OCS SIP system and Avaya Presence Services
- OpenQ, contact centermultimedia generic contact
- Scanned Document
- SMS
- 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 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 contacts that an agent can be assigned is five. The consumption of agent licenses in not affected by multiplicity. An agent continues to consume agent licenses at logon for each contact type assigned to the agent. The maximum number of contacts processed simultaneously is limited to 3000 to ensure agent engineering limits are not exceeded.

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* (NN44400-114).

Create callbacks

By using the Agent Desktop, agents can create a callback record to a 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* (NN44400-114).

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 (see Review real-time reports in Agent Desktop Display on page 158 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. See Report historical data on page 159. 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.

Archive multimedia database content

Data from the Contact Center Multimedia database is archived to tab-delimited text files that you can view in third-party applications such as Microsoft Excel. You must archive the Multimedia database regularly to clear space in the database partition of your server. The archive schedule must reflect your Contact Center volume to prevent large archive files.

You can archive contacts associated with the following elements:

- outbound campaigns
- e-mail rules
- skillsets
- closed reasons

For example, if you know that no action is expected for a particular skillset, you can archive the contacts associated with that skillset.

When you archive data, you can archive the customer data with the contact data. During an archive, the data is stored in a flat file and then deleted from the database. The only way to retrieve this data is to restore the archive. Before you archive your contacts, you must determine which type of archive or restore you want to use.

The following information is archived:

- contact details (and associated answer and custom fields)
- action details (and associated custom fields)
- attachment files
- campaign details and associated script questions, disposition codes, and custom fields (for outbound campaigns)
- customer details (if requested, including all phone numbers, e-mail addresses, and customer field records that are attached to the customer)

If you archive the customer data as well, records associated with the customer data are not deleted if other contacts associated with the customer exist in the database after the archive is complete. The records appear in the archived file.

Note:

If you manually modify the data generated from an archive, the data can become corrupt resulting in the failure of future restores. For this reason, Avaya cannot support issues with the application arising from manually modified archive data.

A log file of the archive, `ArchiveLogFile.txt`, is stored in the archive folder you choose.

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 182
- Web services on page 183

Contact Center Standby server

You can install a warm standby server, or redundancy 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 53.

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.

Chapter 15: Avaya Media Server

Avaya Media Server is a software-based media processing platform. All media processing is performed in software on the host CPUs. The Avaya Media Server architecture is uniquely scalable for all core functions of the platform, including media processing, signaling, application execution, and content management.

Avaya Media Server is IP-enabled with a strong focus on Web services and industry standards. The platform is designed for generic multimedia processing and is based on open standards protocols. Avaya Media Server uses standard Session Initiation Protocol (SIP) for signaling and Real-time Transport Protocol (RTP) to transport audio and video (in Contact Center, Avaya Media Server does not support Secure Real-time Transport Protocol (SRTP)). This enables it to work with a wide variety of clients and gateways. Avaya Media Server programmability is available using industry standards such as VXML and CCXML.

The Avaya Aura® Contact Center DVD contains an enhanced version of Avaya Media Server which contains an additional component—Contact Center Services for Avaya Media Server (CCSM). CCSM provides three services required by SIP-enabled Contact Center:

- Conference–This service is used to create an Avaya Media Server conference and anchor customer calls, announcements, and agent calls to the Avaya Media Server conference.
- Announcement–This service is used to play treatment (ringback, announcements) into the Avaya Media Server conference.
- Dialog–This service is used to play and collect DTMF digits entered in the Avaya Media Server conference.

In SIP-enabled Contact Centers the Avaya Aura® Contact Center DVD version of Avaya Media Server software may be installed co-resident with Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, and Contact Center Multimedia.

Avaya Media Server requires licenses for the CCSM conference, announcement, and dialog features. When installed co-resident with Contact Center Manager Server, Avaya Media Server uses the Contact Center License Manager, otherwise Avaya Media Server uses the Avaya Media Server License Server.

Media processing features

Avaya Media Server supports text, audio, and video for most multimedia processing features. The system is capable of streaming audio and video in a variety of codecs and formats, fully synchronized from the server, unbuffered and in real-time. The system can deliver text through both instant messaging and Web push methods.

Avaya Aura® Contact Center uses Avaya Media Server media processing capabilities to support conferencing, announcements and dialogs. Each Avaya Media Server in a Contact Center is configured in Contact Center Manager Administration as a Media Server and assigned to handle conference, announcement, or/and dialogs Media Services.

In SIP-enabled contact centers Avaya Media Server provides some default media for standard ringback and busy tones. Contact Center uses these default tones with SIP-based phone calls. Additional media for RAN (recorded announcements) and Music must be provisioned in order for Avaya Media Server to provide meaningful media to the customer. When adding this additional media, the Media Content Name in Avaya Media Server must match the Local SIP Subscriber Domain Name in Contact Center Manager Server–Server Configuration.

DVD controller

The Avaya Aura® Contact Center DVD controller installs the following Avaya Media Server components:

- Avaya Media Server
- Contact Center Services for Avaya Media Server (CCSM)

Supported platform

The Avaya Media Server software can be installed on Commercial off-the-shelf (COTS) servers or blades. A Platform Vendor Independence (PVI) is available to confirm if your platforms supports Avaya Media Server.

Avaya provides a tool (`mapvichecker.exe`) that confirms if your platform meets the minimum requirements.

For more information about the minimum hardware requirements for Avaya Media Server, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Network deployment options

Your Avaya Media Server network can be configured as a standalone system or as a cluster of multiple servers.

Standalone

You can deploy Avaya Media Server in a standalone configuration where it has no external dependencies and all network related resources are configured on a single Avaya Media

Server node. A standalone configuration includes only a primary server to configure. No secondary or standard servers require configuration.

Cluster

An Avaya Media Server cluster is a collection of Avaya Media Server nodes that work closely together and essentially can be viewed as one node. This configuration offers good redundancy, improved performance and can be configured to support load balancing. An Avaya Media Server cluster shares the following resources:

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

The cluster is based on system replication, so you must configure the same applications on all Avaya Media Server servers in the same cluster and you must configure any application data (such as subscriber information) for that cluster. To achieve scalability, the SIP proxy must support load balancing across all Avaya Media Server nodes in that cluster.

License requirements

Your maximum number of simultaneous active sessions is determined by the number of purchased licenses. Avaya Media Server supports the following licensing models:

- Nodal licenses
- Server licenses with redundant license servers and floating licenses

When installed co-resident with Contact Center Manager Server, Avaya Media Server uses the Contact Center License Manager and the license server on Avaya Media Server is disabled. When not co-resident with Contact Center Manager Server, Avaya Media Server uses the Avaya Media Server License Server and the Contact Center Services for Avaya Media Server (CCSM) licenses must be applied using the Avaya Media Server Element Manager.

Web based configuration and management features

Element Manager (EM) is a Web-based administration tool used to configure and manage Avaya Media Server. Element Manager allows control of the following:

- Licensing configuration (Stand-alone Avaya Media Server)
- System operational state management
- Gateway configuration
- Web services configuration
- Alarm and event log viewer

- Alarm and event log configuration and filtering
- Clustering configuration
- Backup and restore

Session Initiation Protocol features

The Avaya Media Server platform supports Session Initiation Protocol (SIP) for call and session signaling. SIP provides a standard means to establish sessions, negotiate capabilities, invoke applications, and exchange data with Avaya Media Server. SIP signaling provides generic session establishment.

The Avaya Media Server platform uses SIP Transport Layer Security (TLS) for securing SIP signaling. Avaya Media Server manages a list of trusted network sources, and signaling from non-trusted sources route to a network proxy for authentication. Avaya Media Server supports a SIP trunking mode that allows reuse of connections to and from network proxies for subsequent calls to reduce the overhead of TLS signaling. SIP routes define all SIP proxy and SIP registrar servers an Avaya Media Server node can communicate with. Avaya Media Server uses SIP routes designated as a SIP proxy server for routing outbound SIP requests for outbound traffic load sharing and switchover. Avaya Media Server registers applications with all configured SIP registrars. Registration is optional based on your Avaya Media Server configuration and digest authentication support.

Playing and recording audio

Avaya Media Server can stream media files (also called prompts or announcements) in all supported codecs. These files are not limited to audio.

Media files are cached locally on the system and are transcoded into temporary files. Subsequent requests for the media file use the transcoded file and are packetized without further processing. Files that surpass a configurable “hit” rate are pulled into memory in their post transcoded form and packetized directly. An uncached file that is not eligible for caching, is transcoded in real-time.

Conferencing

Avaya Media Server supports multimedia conferencing for audio and video streams in large and small conferences.

The conferencing algorithm uses mixing, which means that you can hear up to four parties simultaneously. Each channel runs a voice activity detector (to determine speech and background noise), an automatic gain control algorithm, and a dynamic jitter buffer with compaction and packet loss concealment.

Chapter 16: Avaya Aura® Call Center Elite integration

Avaya Aura® Contact Center Release 6.2 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 Release 6.2 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.

Avaya Aura® Contact Center supports the following multimedia contact types:

- E-mail
- SMS text messages
- Fax messages
- Scanned documents
- Voice mail messages
- Web Communications

You can install Avaya Aura® Contact Center to add multimedia-enabled capabilities to new or existing Avaya Aura® Call Center Elite contact center solutions.

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.

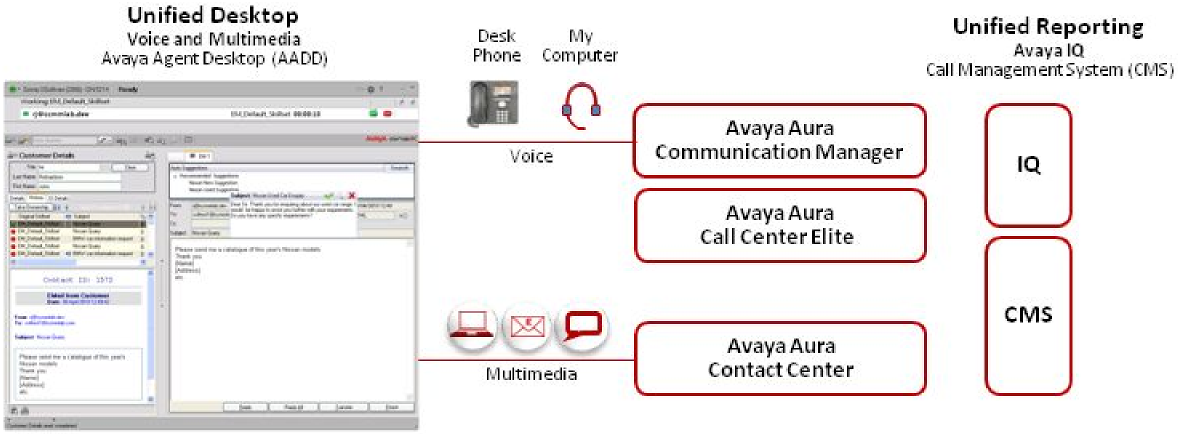
Unified Desktop
Voice and Multimedia
Avaya Agent Desktop (AADD)
Desk Phone
My Computer
Voice
Multimedia
Avaya Aura Communication Manager
Avaya Aura Call Center Elite
Avaya Aura Contact Center
Unified Reporting
Avaya IQ
Call Management System (CMS)
IQ
CMS

Figure 10: 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 e-mail 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-only installation and commissioning when using Contact Center as a multimedia addition to Avaya Aura® Call Center Elite. Multimedia-only 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. To end phantom calls on the soft client in Avaya Aura® Call Center Elite when it is integrated with Avaya Aura® Contact Center, configure the On hook dialing, n.

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 e-mail 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, e-mail, 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 Reporting and Performance management

Avaya IQ supports real-time and historical reports for Avaya Aura® Contact Center and Avaya Aura® Call Center Elite resources. This includes reporting on multimedia contacts, such as e-mail messages and scanned documents.

Avaya Performance Center (APC) real-time reports integrate Avaya Aura® Contact Center agents and queues with Avaya Aura® Communication Manager 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 Avaya Aura® Contact Center agents and queues as well, but the queue-based measure % in Service Level is not supported for multimedia channels such as e-mail. Avaya Aura® Contact Center agents and Avaya Aura® 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 the Avaya Aura® Contact Center 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 Avaya Aura® Contact Center, in Avaya IQ add a “Data Source Association” of type “AACC” for the Contact Center Manager Server. If you are using the Avaya Aura® Contact Center High Availability feature, use the Managed IP address for the active Contact Center Manager Server 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.

Unified Agent Administration

Avaya Aura® Call Center 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 Avaya Aura® Contact Center.

Control Manager supports:

- Adding agents simultaneously to both Call Center Elite and Avaya Aura® Contact Center
- Configuring agents to support voice calls using Call Center Elite.

- Configuring agent voice skills level assignments.
- Configuring agents to support multimedia contacts using Avaya Aura® Contact Center.
- Configuring agent multimedia skillsets.
- Moving Call Center Elite agents to work only on Avaya Aura® Contact Center multimedia contacts.
- Scheduling agents to move between skills and skillsets.

  For more information about using Control Manager to configure Avaya Aura® Contact Center, see Avaya Aura® Call Center Control Manager User's Guide on www.avaya.com/support.

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 Release 6.2 documentation to plan and engineer your multimedia addition.

   For more information about planning and engineering an Avaya Aura® Contact Center, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
2. Install and configure the necessary e-mail, document scanning, and/or SMS text handling infrastructure as required.

   For more information about the required infrastructure, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
3. Obtain an Avaya Aura® Contact Center Release 6.2 multimedia license and software DVD.
4. Download the most recent Avaya Aura® Contact Center Release 6.2 Service Packs.
5. Obtain a suitably engineered Windows Server 2008 Release 2 64-bit server. For more information about engineering a compliant server to host Avaya Aura® Contact Center, or to determine the number of servers required, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
6. Complete the *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).

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 “No Switch Configured” switch option. Install Contact Center Manager Server (CCMS), Contact Center License Manager, Contact Center Manager Administration (CCMA), Communication Control Toolkit (CCT), and Contact Center Multimedia (CCMM). For more information about installing Avaya Aura® Contact Center, see *Avaya Aura® Contact Center Installation* (NN44400-311).
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* (NN44400-312).
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” 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* (NN44400-611).
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* (NN44400-611).
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* (NN44400-114).

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* (NN44400-114).
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* (NN44400-514).

The contact center agents are now ready to handle voice and multimedia communications with customers.

Chapter 17: Avaya Voice Portal

Avaya Voice 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 Voice Portal (AVP) software is deployed on standard Linux servers and it supports integration with SIP-enabled communications infrastructures, including Communication Manager-based gateways and Avaya Aura® Contact Center.

The Avaya Voice Portal system consists of a Voice Portal Management System (VPMS), which controls the Voice Portal system and Media Processing Platform (MPP) servers, which process all calls. The Voice 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 Voice Portal:

- Front-end Avaya Voice Portal with SIP-enabled Contact Center
- Back-end Avaya Voice Portal with SIP-enabled Contact Center
- Front-end Avaya Voice Portal with Contact Center - Web Service Open Interfaces

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

There are two main mechanisms for transferring calls and call data between Contact Center and Avaya Voice Portal:

- 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 allows custom data to be passed with the call. To enable Contact Center Landing Pads you must configure Contact Center Web Service Open Interfaces. To enable Web Service Open Interfaces, you must procure Open Queue, OI Open Queue, and OI Universal Networking licenses.
- SIP header information. SIP includes a number of message headers in each SIP message. These headers contain information that enables the receiver to understand the message better and handle the message properly. In a contact center solution, SIP headers may be used to transfer small amounts of call-related information between SIP-enabled applications. Avaya Aura® Contact Center supports SIP header User-to-User Information (UUI) and Avaya custom P-Intrinsic SIP private header information. SIP header information does not use Web Service Open Interfaces.

In an Avaya Communication Server 1000 AML-based solution, Avaya Aura® Contact Center supports Landing Pads for integration with Avaya Voice Portal 5.x. SIP header is not supported in AML-based solutions.

In an Avaya Communication Server 1000 SIP-based solution, Avaya Aura® Contact Center supports Landing Pads and SIP header information for integration with Avaya Voice Portal 5.x.

In an Avaya Aura® Unified Communications platform SIP-based solution, Avaya Aura® Contact Center supports Landing Pads and SIP header information for integration with Avaya Voice Portal 5.x.

In SIP-enabled Contact Centers, front-end and back-end operations are not mutually exclusive; both are supported in a single call depending on your requirements.

The following table shows the call and data transfer mechanism supported by each platform type:

Transfer method	CS 1000 AML-based Contact Center	CS 1000 SIP-based Contact Center	Avaya Aura SIP-based Contact Center
Landing Pads	Yes	Yes	Yes
SIP header UUI	No	Yes	Yes
SIP P-Intrinsic private header	No	Yes	Yes

The following table shows the additional licensing requirements for each Avaya Aura® Contact Center and Avaya Voice Portal integration type:

Solution type	CS 1000 AML-based Contact Center	CS 1000 SIP-based Contact Center	Avaya Aura SIP-based Contact Center
Landing Pads	Open Queue, OI Open Queue, and OI Universal Networking.	Open Queue, OI Open Queue, and OI Universal Networking.	Open Queue, OI Open Queue, and OI Universal Networking.
SIP header UUI	No additional licenses required.	No additional licenses required.	No additional licenses required.
SIP P-Intrinsic private header	No additional licenses required.	No additional licenses required.	No additional licenses required.

For more information about Avaya Voice Portal, see *Planning for Voice Portal* on the Avaya support Web site, www.avaya.com/support.

Avaya Voice Portal Dialog Designer

Dialog Designer is an Eclipse-based application development environment which supports the development of Voice XML and CCXML speech applications. Dialog Designer generates Avaya Voice 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 may be integrated with a more traditional Interactive Voice Response (IVR) system and Voice XML dialog systems may 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 (UUI) SIP header information and P-Intrinsic SIP header information. Contact Center uses the header information in each SIP call to generate call-related Contact Intrinsic information and Call Attached Data (CAD). This Contact Intrinsic data may contain information relevant to that call, the calling customer, and other information retrieved by self-service or third party applications. Contact Intrinsics are key-value pairs of relatively small amounts of data. Call Attached Data is a longer unstructured amount of data.

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, SIP headers may be used 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 agent may receive the Contact Intrinsic data in a screen pop, or they may 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 may 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 Media Server

Avaya Media Server is a software-based media processing platform. All media processing is performed in software on the host CPUs. The Avaya Media Server architecture is uniquely scalable for all core functions of the platform, including media processing, signaling, application execution, and content management. Avaya Media Server is IP enabled with a strong focus on Web services and industry standards. The platform is designed for generic multimedia processing and is based on open standards protocols. Avaya Media Server uses standard SIP for signaling and Real-time Transport Protocol (RTP) to transport audio and video, which enables it to work with a wide variety of clients and gateways, including Avaya Aura® Contact Center.

Avaya Aura® Contact Center uses the media processing capabilities of Avaya Media Server to support conferencing, announcements, and dialogs in SIP-enabled contact centers. Each Avaya Media Server in a contact center is configured in Contact Center Manager Administration as a Media Server and is assigned to handle conference, announcement, or/and dialogs media services.

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 Voice Portal and Contact Center Web Service Open Interfaces

This section describes a front-end Avaya Voice Portal self-service integration using Avaya Aura® Contact Center - Web Service Open Interfaces. Integrating Avaya Voice 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 Voice Portal self-service system and Avaya Aura® Contact Center — Web Service Open Interfaces 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 Voice Portal uses XML speech applications to integrate with Avaya Aura® Contact Center Web Service Open Interfaces. The Avaya Aura® Contact Center Web Service Open Interfaces are supported in AML-based and SIP-enabled contact centers.

Avaya Voice 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 Dialog Designer. Avaya Voice Portal automatically includes all Dialog 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 Voice Portal self-service integration with Avaya Aura® Contact Center and Communication Manager platform.

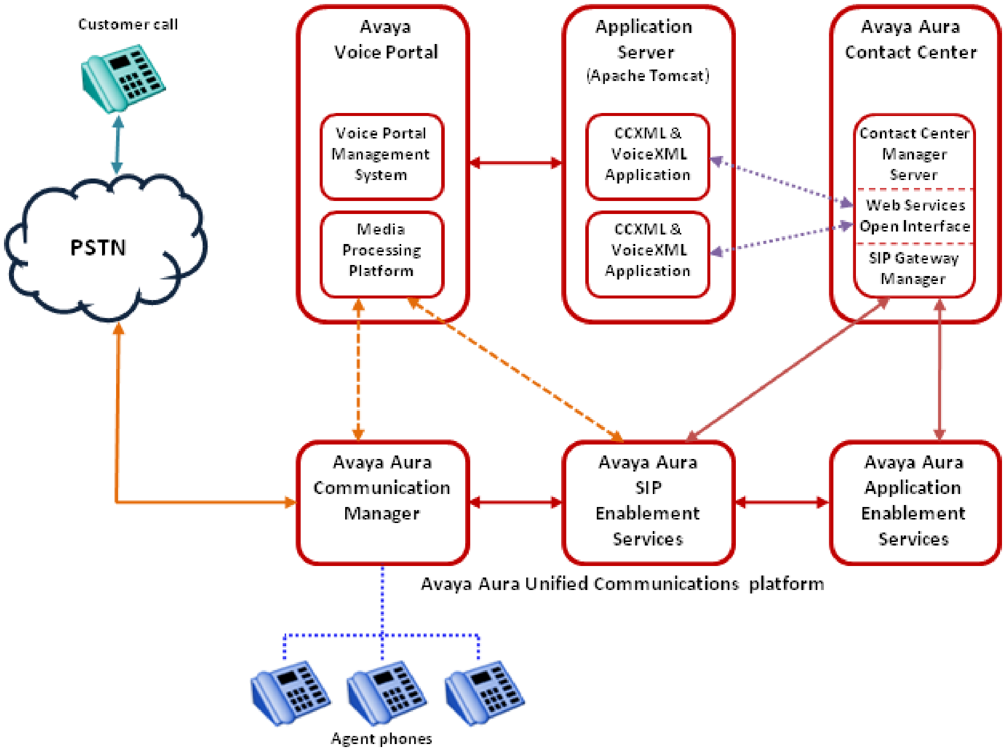

Figure 11: Example of front-end Avaya Voice Portal self-service

Call flow example

This call flow example shows how the Avaya Voice 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 Voice 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 VPMS server to match the number to a speech application on Avaya Voice Portal.
3. The System Manager 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 and specifies a destination Controlled Directory Number (CDN) or Agent, transfer type (Blind Transfer), contact ID number, and Contact Intrinsics.
10. Contact Center Manager Server returns the Landing Pad number.
11. The Voice 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. A Contact Center agent is offered the call. The agent can access customer details and Contact Intrinsics 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 Voice 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 Voice Portal and SIP-enabled Contact Center

A combined Avaya Voice 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 Voice 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 Voice 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 can 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, and makes the Contact Center is more efficient.

Avaya recommends that you create your XML speech applications with Dialog Designer. Avaya Voice Portal automatically includes all Dialog 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 Voice Portal self-service integration with Avaya Aura® Contact Center and Communication Manager.

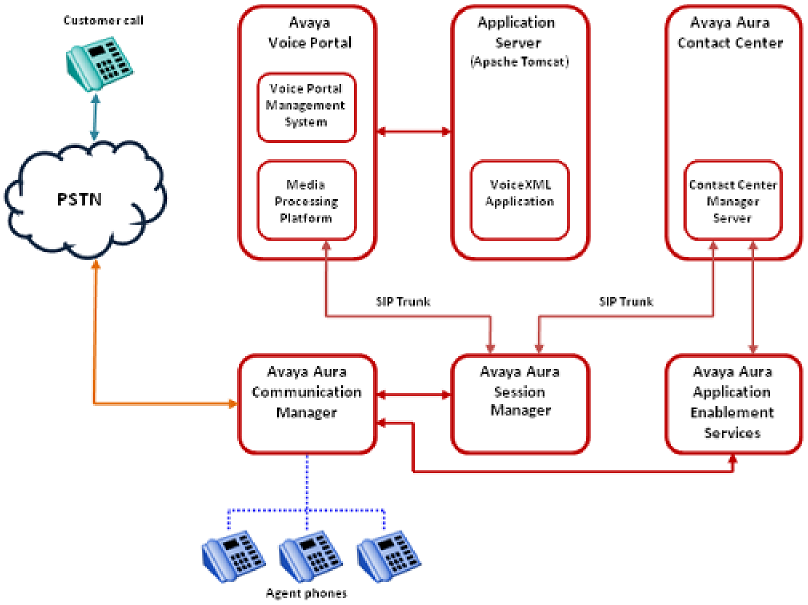
Customer call
PSTN
Avaya Voice Portal
Voice Portal Management System
Media Processing Platform
Application Server (Apache Tomcat)
VoiceXML Application
Avaya Aura Contact Center
Contact Center Manager Server
SIP Trunk
SIP Trunk
Avaya Aura Communication Manager
Avaya Aura Session Manager
Avaya Aura Application Enablement Services
Agent phones

Figure 12: Example of front-end Avaya Voice Portal and SIP-enabled Contact Center

Call flow example

This call flow example shows how the Avaya Voice 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 Voice 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 VPMS server to match the number to a speech application on Avaya Voice Portal.
3. The System Manager 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 Transfer), contact ID number, and UUI data generated Contact Intrinsics.
10. The Voice Portal Media Processing Platform (MPP) server completes the blind transfer of the Customer call to the destination CDN.
11. The Contact Center Manager Server SIP Gateway Manager (SGM) is now controlling the Customer call. The SGM routes the call to an appropriate agent skillset.
12. A Contact Center agent is offered the call. The agent can access Customer details and Contact Intrinsics before answering the call.
13. The Contact Center agent answers the Customer call.
14. The XML application terminates the call when it finishes execution or when the caller hangs up.

A combined Avaya Voice 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 Voice Portal uses Voice XML applications and SIP User-to-User Information (UUI) data to integrate with Avaya Aura® Contact Center. This gives enterprises complete flexibility and control of the integrated solution. The front-end Avaya Voice 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 Voice Portal system with an Avaya Aura® Contact Center.

Back-end Avaya Voice Portal and SIP-enabled Contact Center

Avaya Voice Portal (AVP) provides back-end Interactive Voice Response (IVR) services like text-to-speech, digit collection, music, and speech recognition. A combined Avaya Voice 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 AVP solution, Customer calls to the Avaya Aura® Contact Center are routed to AVP applications for automated processing. Avaya Voice 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 (AVP supports optional Automatic Speech Recognition servers). The AVP 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 appropriate Agent.

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

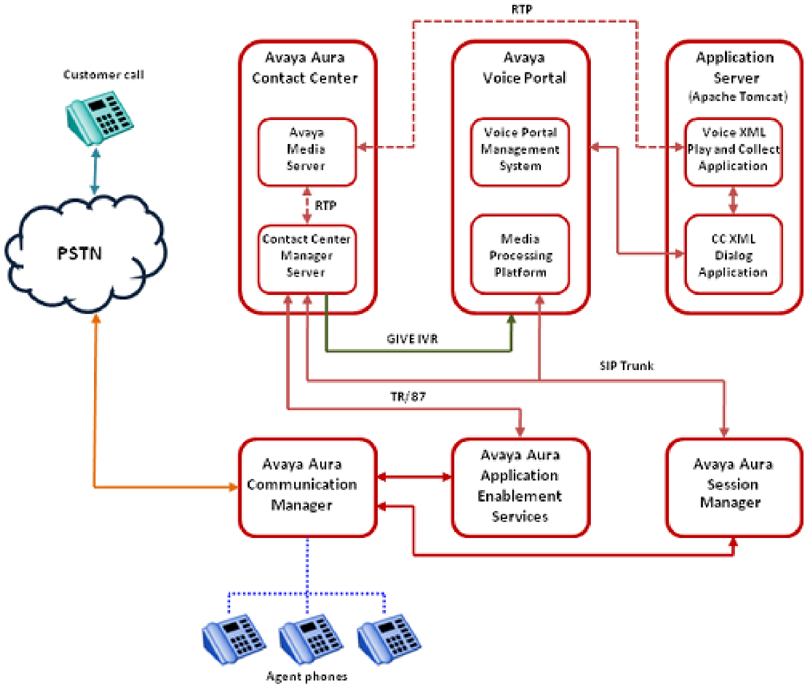
RTP
Customer call
Avaya Aura Contact Center
Avaya Voice Portal
Application Server (Apache Tomcat)
Avaya Media Server
Voice Portal Management System
Voice XML Play and Collect Application
RTP
PSTN
Contact Center Manager Server
Media Processing Platform
CC XML Dialog Application
GIVE IVR
SIP Trunk
TR/87
Avaya Aura Communication Manager
Avaya Aura Application Enablement Services
Avaya Aura Session Manager
Agent phones

Figure 13: Example of back-end Avaya Voice Portal with Interactive Voice Response

Call flow example

This call flow example shows how the Avaya Voice 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 or SIP Enablement Services to Avaya Aura® Contact Center (AACC).
2. Avaya Aura® Contact Center answers the call and executes the Master Script, and optional primary scripts. A primary script is an application executed or referenced by the Master Script. Contact Center Manager Server records Master script and Primary script actions in statistical records.
3. The AACC script issues a `GIVE IVR` for an external media server (XDIALOG), supplying the URI identifier of the Avaya Voice Portal.
4. AACC retains control of the call and sends a `SIP INVITE` message to Avaya Voice Portal. AACC specifies treatment parameters in the `SIP INVITE` message.
5. Avaya Voice Portal passes the call to a CCXML dialog application on the 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 AACC. SIP header-based shared User-to-User Information (UUI) data is also extracted and passed to the Voice XML application.
8. The Play and Collect Voice XML application streams Real-time Transport Protocol (RTP) streams into the associated Avaya 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 AACC script retrieves the IVR collected digits.

A combined Avaya Aura® Contact Center and Avaya Voice Portal solution gives Customers exceptional service and improved efficiency. Back-end Avaya Voice 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 Voice Portal. This gives enterprises complete flexibility and control of the solution integration. The Avaya Voice 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 Voice 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 18: 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.

The Avaya Aura® Experience Portal system consists of an Experience Portal Manager System (EPMS), 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
- Front-end Avaya Aura® Experience Portal with Contact Center - Web Service Open Interfaces

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

There are two main mechanisms for 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 may 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.

In an Avaya Communication Server 1000 AML-based solution, Avaya Aura® Contact Center supports Landing Pads for integration with Avaya Aura® Experience Portal. SIP header Information is not supported in AML-based solutions.

In an Avaya Communication Server 1000 SIP-based solution, Avaya Aura® Contact Center supports Landing Pads and SIP header Information for integration with Avaya Aura® Experience Portal.

In an Avaya Aura® Unified Communications platform based solution, Avaya Aura® Contact Center supports Landing Pads and SIP header information for integration with Avaya Aura® Experience Portal.

The following table shows the call transfer mechanism supported by each platform type:

Transfer method	CS 1000 AML-based Contact Center	CS 1000 SIP-based Contact Center	Avaya Aura SIP-based Contact Center
Landing Pads	Yes	Yes	Yes
UUI SIP header	No	Yes	Yes
P-Intrinsic SIP header	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-based Contact Center	Avaya Aura SIP-based Contact Center
Landing Pads	Open Queue, OI Open Queue, and OI Universal Networking.	Open Queue, OI Open Queue, and OI Universal Networking.	Open Queue, 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.

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-based Contact Center	Avaya Aura SIP-based Contact Center
Landing Pads	Maximum Call Attached Data is 4096 bytes. Maximum 5 ASCII key-value pairs of Contact Intrinsics. [1]	Maximum Call Attached Data is 4096 bytes. Maximum 5 ASCII key-value pairs of Contact Intrinsics. [1]	Maximum Call Attached Data is 4096 bytes. Maximum 5 ASCII key-value pairs of Contact Intrinsics. [1]
UUI SIP header using ASAI	N/A	96 bytes maximum.	96 bytes maximum.
P-Intrinsics SIP header	N/A	Depends on your solution. [2]	Depends on your solution. [2]

[1] Avaya Aura® Contact Center supports up to 5 ASCII key-value pairs of Contact Intrinsics. Avaya Aura® Contact Center supports a key name of up to 25 characters and a value size of up to 80 characters.

[2] The following limitations apply to P-Intrinsics SIP header information:

- The amount of P-Intrinsics information associated with a call depends on the other SIP headers in the call and on the call flow path. Typically, Avaya Aura® Contact Center supports up to 10 ASCII key-value pairs of P-Intrinsics. Avaya Aura® Contact Center supports a key name of up to 25 characters and a value size of up to 80 characters.
- 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.

For more information about Avaya Aura® Experience Portal, see *Planning for Avaya Aura® Experience Portal* on the Avaya support Web site, www.avaya.com/support.

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 may be integrated with a more traditional Interactive Voice Response (IVR) system and Voice XML dialog systems may 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 (UUI) SIP header information and P-Intrinsic SIP header information. Contact Center uses the header information in each SIP call to generate call-related Contact Intrinsic information and Call Attached Data (CAD). This Contact Intrinsic data may contain information relevant to that call, the calling customer, and other information retrieved by self-service or third party applications. Contact Intrinsics are key-value pairs of relatively small amounts of data. Call Attached Data is a longer unstructured amount of data.

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, SIP headers may be used 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 agent may receive the Contact Intrinsic data in a screen pop, or they may 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 may 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.

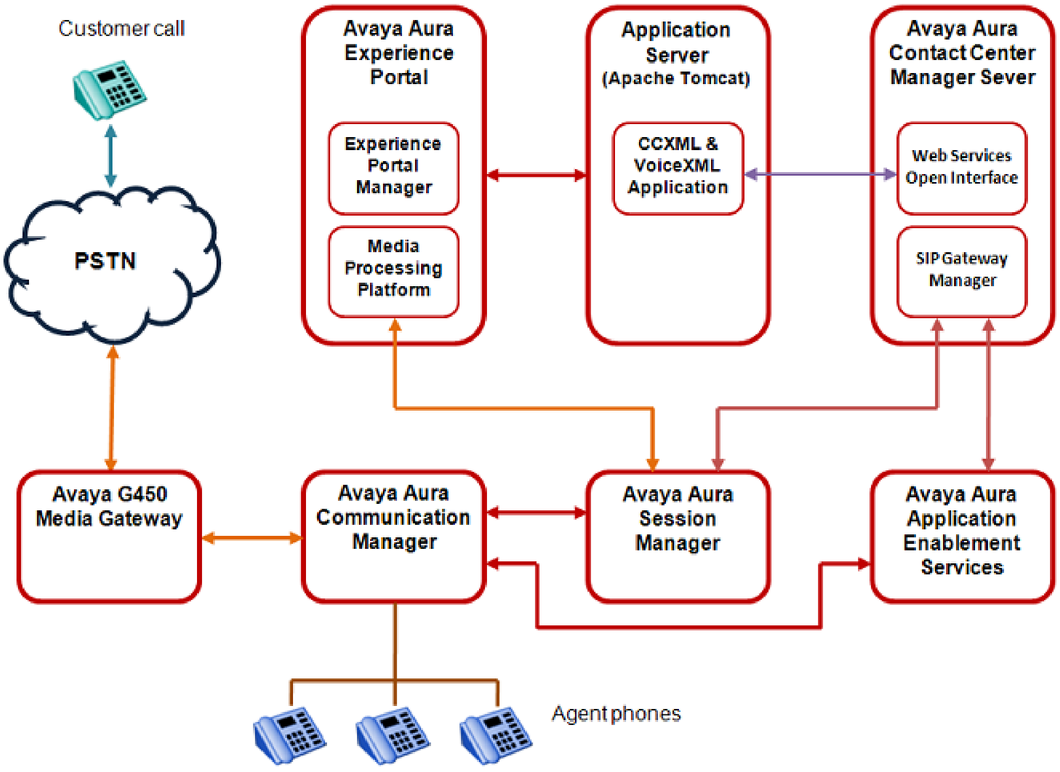
Customer call
PSTN
Avaya Aura Experience Portal
Experience Portal Manager
Media Processing Platform
Application Server (Apache Tomcat)
CCXML & VoiceXML Application
Avaya Aura Contact Center Manager Sever
Web Services Open Interface
SIP Gateway Manager
Avaya G450 Media Gateway
Avaya Aura Communication Manager
Avaya Aura Session Manager
Avaya Aura Application Enablement Services
Agent phones

Figure 14: Example of front-end Avaya Aura® Experience Portal using Contact Center Web Service Open Interfaces

Call flow example using CCMS Web service Open Interfaces

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

1. Incoming customer calls are routed to a Media Processing Platform (MPP) server in the Avaya Aura® Experience Portal system.
2. The MPP server checks the Dialed Number Identification Service (DNIS) for the incoming call and uses the configuration information downloaded from the Experience Portal Management System (EPMS) 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 and specifies a destination Controlled Directory Number (CDN) or Agent, transfer type (Blind Transfer), contact ID number, and Contact Intrinsics.
10. Contact Center Manager Server returns the Landing Pad number.
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. The agent can access customer details and Contact Intrinsics 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.

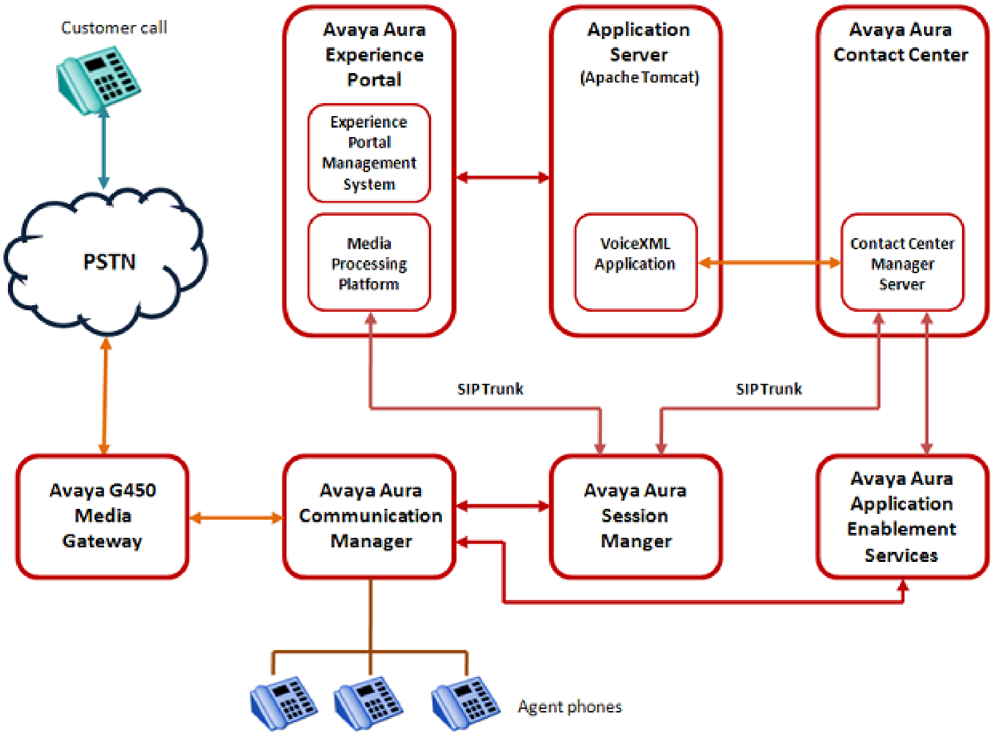
Customer call
PSTN
Avaya Aura Experience Portal
Experience Portal Management System
Media Processing Platform
Application Server (Apache Tomcat)
VoiceXML Application
Avaya Aura Contact Center
Contact Center Manager Server
SIP Trunk
SIP Trunk
Avaya G450 Media Gateway
Avaya Aura Communication Manager
Avaya Aura Session Manger
Avaya Aura Application Enablement Services
Agent phones

Figure 15: Example of front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

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

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

1. Incoming customer calls are routed to a Media Processing Platform (MPP) server in the Avaya Aura® Experience Portal system.
2. The MPP server checks the Dialed Number Identification Service (DNIS) for the incoming call and uses the configuration information downloaded from the Experience Portal Management System (EPMS), 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 Transfer), contact ID number, and UUI data generated Contact Intrinsics.
10. The Experience Portal Media Processing Platform (MPP) server completes the blind transfer of the customer call to the destination CDN.
11. The Contact Center Manager Server SIP Gateway Manager (SGM) is now controlling the customer call. The SGM routes the call to an appropriate agent skillset.
12. A Contact Center agent is offered the call. The agent can access customer details and Contact Intrinsics before answering the call.
13. The Contact Center agent receives the (customer and call) context information in a screen pop and answers the customer call.
14. The XML application terminates the call when it finishes execution or when the caller 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 (UUI and P-Intrinsics) information to integrate with Avaya Aura® Contact Center. This gives enterprises complete flexibility and control of the integrated solution. The front-end Avaya Aura® Experience Portal self-service system and Avaya Aura® Contact Center solution is highly flexible and efficient. Avaya supplies sample Voice XML applications for the rapid integration of a front-end Avaya Aura® Experience Portal system with an Avaya Aura® Contact Center.

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

Avaya 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.

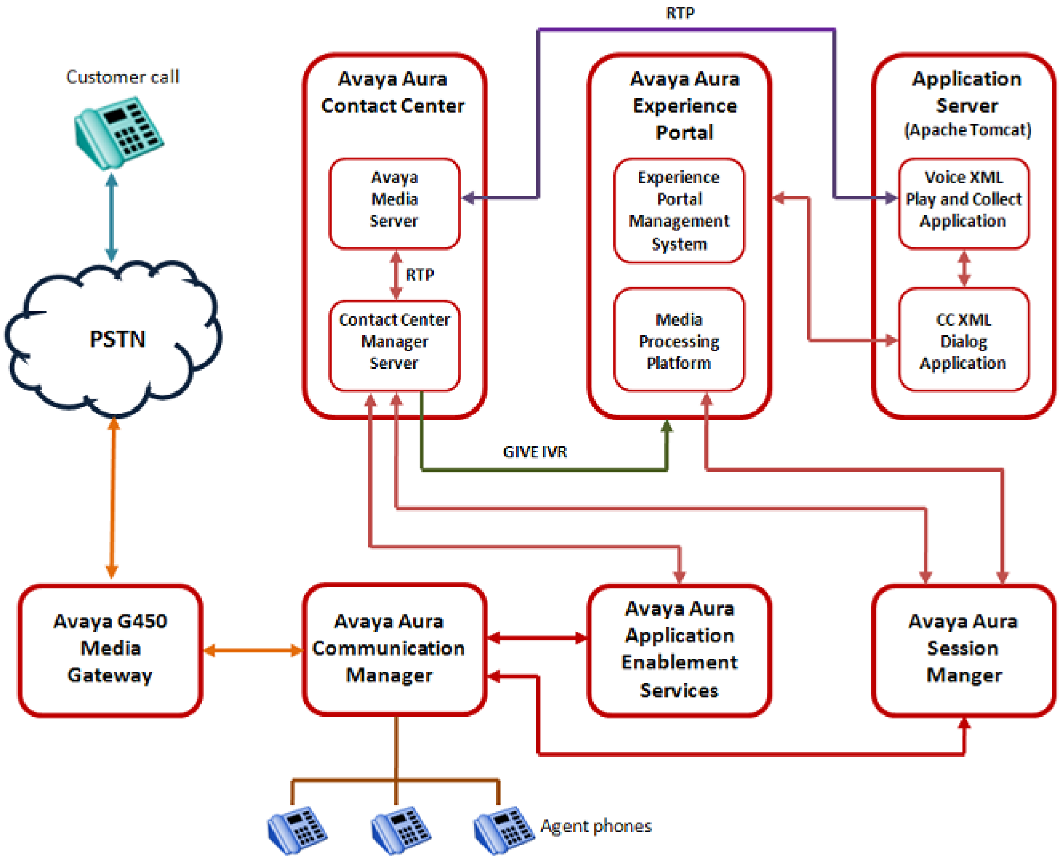
RTP
Customer call
Avaya Aura Contact Center
Avaya Media Server
RTP
Contact Center Manager Server
Avaya Aura Experience Portal
Experience Portal Management System
Media Processing Platform
Application Server (Apache Tomcat)
Voice XML Play and Collect Application
CC XML Dialog Application
PSTN
GIVE IVR
Avaya G450 Media Gateway
Avaya Aura Communication Manager
Avaya Aura Application Enablement Services
Avaya Aura Session Manger
Agent phones

Figure 16: Example of back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

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

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

1. Incoming customer calls to the Communication Manager are routed by the Session Manager to Avaya Aura® Contact Center.
2. Avaya Aura® Contact Center answers the call and executes a flow application, script, and/or optional primary scripts. A primary script is an application executed or referenced by the Master Script. Contact Center Manager Server records Master script and Primary script actions in statistical records.
3. The Avaya Aura® Contact Center script issues a `GIVE IVR` for an external media server (XDIALOG), supplying the URI identifier of the Avaya Aura® Experience Portal.
4. Avaya Aura® Contact Center retains control of the call and sends a `SIP INVITE` message to Avaya Aura® Experience Portal. Avaya Aura® Contact Center specifies treatment parameters in the `SIP INVITE` message.
5. Avaya Aura® Experience Portal passes the call to a CCXML dialog application on the Apache Tomcat application server.
6. The CCXML dialog application accepts and retrieves IVR parameters from the `SIP INVITE` message.
7. The CCXML dialog application invokes the Play and Collect Voice XML application (PlayAndCollect) with the parameters retrieved from Avaya Aura® Contact Center. If available, SIP header UUI data is also extracted and passed to the Voice XML application.
8. The Play and Collect Voice XML application streams Real-time Transport Protocol (RTP) streams into the associated Avaya 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.

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: Migration and patching fundamentals

This chapter describes the supported migration paths to Avaya Aura® Contact Center Release 6.2. Contact Center Release 6.2 server applications are supported only on the Windows Server 2008 Release 2 operating system. Older releases of Avaya NES Contact Center do not support this operating system so you cannot upgrade your existing installation to Avaya Aura® Contact Center Release 6.2. You can migrate all your old configuration and statistical data from a previous release of Contact Center to the new Contact Center Release 6.2 server so no data is lost in the move.

The High Availability feature lends itself to the provision of 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 hot standby applications do not process contacts and can therefore be stopped and patched without shutting down the Contact Center.

Upgrades versus migrations

For an upgrade, you reuse an existing server with a previous version of Contact Center for Contact Center Release 6.2 and import customer data. Upgrades to Contact Center Release 6.2 are not supported.

For a migration, you install a new server with a fresh version of Contact Center Release 6.2 and import the data from a previous Contact Center version.

The following steps describe the migration process.

1. Backup the old version of Contact Center database to a network location.
2. Install Avaya Aura® Contact Center Release 6.2 on a new server.

   During the installation, you are asked to define the location of the backed up data, and the data is migrated during installation.
3. Configure Avaya Aura® Contact Center Release 6.2.

Supported migrations

You can migrate the information from previous versions of Avaya Contact Center to the Contact Center application suite by using software migration procedures. Migration procedures move all historical, statistical, and configuration information from a previous release of Avaya NES Contact Center to the new release of Contact Center.

The following Contact Center Manager Server (CCMS) migrations are supported:

- Avaya NES Contact Center CCMS Release 6.0 to Avaya Aura® Contact Center CCMS Release 6.2
- Avaya NES Contact Center CCMS Release 7.0 to Avaya Aura® Contact Center CCMS Release 6.2
- Avaya Aura® Contact Center CCMS Release 6.2 to Avaya Aura® Contact Center CCMS Release 6.2 on a new server

The following Communication Control Toolkit (CCT) migrations are supported:

- Avaya NES Contact Center CCT Release 6.0 to Avaya Aura® Contact Center CCT Release 6.2
- Avaya NES Contact Center CCT Release 7.0 to Avaya Aura® Contact Center CCT Release 6.2
- Avaya Aura® Contact Center CCT Release 6.2 to Avaya Aura® Contact Center CCT Release 6.2 on a new server

The following Contact Center Manager Administration (CCMA) migrations are supported:

- Avaya NES Contact Center CCMA Release 6.0 to Avaya Aura® Contact Center CCMA Release 6.2
- Avaya NES Contact Center CCMA Release 7.0 to Avaya Aura® Contact Center CCMA Release 6.2
- Avaya Aura® Contact Center CCMA Release 6.2 to Avaya Aura® Contact Center CCMA Release 6.2 on a new server

The following Contact Center Multimedia (CCMM) migrations are supported:

- Avaya NES Contact Center CCMM Release 6.0 to Avaya Aura® Contact Center CCMM Release 6.2
- Avaya NES Contact Center CCMM Release 7.0 to Avaya Aura® Contact Center CCMM Release 6.2
- Avaya Aura® Contact Center CCMM Release 6.2 to Avaya Aura® Contact Center CCMM Release 6.2 on a new server

The following Network Control Center (NCC) migrations are supported:

- Avaya NES Contact Center NCC Release 6.0 to Avaya Aura® Contact Center NCC Release 6.2
- Avaya NES Contact Center NCC Release 7.0 to Avaya Aura® Contact Center NCC Release 6.2
- Avaya Aura® Contact Center NCC Release 6.2 to Avaya Aura® Contact Center NCC Release 6.2 on a new server

The following Contact Center applications have no databases and thus do not require database migration:

- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)

Migrations can occur only on the same switch types.

Backup locations

A backup location is a physical network location to store backup or migration data. Before a migration, you must create a backup location to store the data.

Use the Database Maintenance Utility to create a backup location. (Press `F1` to obtain online help) A backup location consists of the following elements:

- Drive letter
    - currently unassigned in Windows (You cannot use existing, already mapped Windows drive letters)
    - a letter from N to U
    - created during use (for example, to store backup data or migration data)
    - removed after use
    - used only with the Database Maintenance Utility
- UNC path
    - use a valid Uniform Naming Convention (UNC) path (for example, `\\cc_server\cc_share\cc_backup`)
- User name
    - Windows account that connects to the location specified by the UNC Path
    - must include computer name in the Account name (for example, `cc_server\Administrator`)
- Password
    - used for the Windows Account that connects to the location specified by the UNC Path

For information about how to create a backup location, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

When a server application performs a backup, it creates a folder in the backup location. To restore this backup on a different server (for example, to migrate to a new server), you must create a new backup location as part of the restore. Be careful to exclude the folder created by the server application backup from the UNC Path, as shown in the following examples:

- When you perform a backup on an old server, create a backup location with a UNC path of `\\NETSERVER01\DIRECTORY01\BACKUP01`.
- The backup creates a backup folder in this path, `\\NETSERVER01\DIRECTORY01\BACKUP01\CCMSR6.0`.
- To restore this backup on a new server, the UNC path you enter to create the new backup location is `\\NETSERVER01\DIRECTORY01\BACKUP01`.
- The restore on the new server uses the data from `\\NETSERVER01\DIRECTORY01\BACKUP01\CCMSR6.0`.

Co-resident migrations

Migrate co-resident applications at the same time.

The following co-resident configuration migrations are supported:

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

You can use the Contact Center DVD Controller to select multiple applications and install them at the same time.

Multinode migrations

Multinode migration refers to migrating a system on which multiple Contact Center applications are installed on servers and possibly located in various geographic locations.

The following table shows the compatibility of Contact Center Release 6.2 with previous releases.

	Avaya Aura® CCMS Release 6.2	Avaya Aura® CCMA Release 6.2	Avaya Aura® CCT Release 6.2	Avaya Aura® CCMM Release 6.2	Avaya Aura® License Manager Release 6.2	Avaya Aura® NCC Release 6.2	Avaya Aura® Server Utility Release 6.2
CCMS 7.0	Yes	Yes	No	No	Yes	Yes	Yes
CCMA 7.0	No	N/A	N/A	No	Yes	N/A	N/A
CCT 7.0	Yes	N/A	Yes	No	Yes	N/A	N/A
CCMM 7.0	No	Yes	No	N/A	Yes	N/A	N/A
CCMS 6.0	Yes	Yes	No	No	Yes	Yes	Yes
CCMA 6.0	No	N/A	N/A	No	Yes	No	N/A
CCT 6.0	Yes	N/A	Yes	No	Yes	N/A	N/A
CCMM 6.0	No	Yes	No	N/A	Yes	N/A	N/A
LM 6.0	No	No	No	No	N/A	No	N/A
NCC 6.0	No	Yes	N/A	N/A	Yes	N/A	Yes
SU 6.0	Yes	N/A	N/A	N/A	N/A	N/A	N/A

In a multinode system on which each application is installed on a single server, migrate your servers in the following order:

1. Contact Center Manager Administration
2. Contact Center License Manager
3. Network Control Center
4. Contact Center Manager Server
5. Communication Control Toolkit
6. Contact Center Manager Server Utility
7. Contact Center Multimedia

If your system configuration includes a Contact Center Manager Server Release 7.0 warm standby server, you can keep your Contact Center Manager Server active while you upgrade the standby server to Contact Center Release 6.2. After the upgrade, you can migrate the data collected on the Contact Center Manager Server Release 7.0 server to the Contact Center Release 6.2 server.

In this example, perform the migration in the following order:

1. Upgrade Contact Center Manager Administration.
2. Upgrade the Network Control Center.
3. Stop the replicating service on the Contact Center Manager Server Release 7.0 standby server.
4. Upgrade the Contact Center Manager Server Standby server to Contact Center Manager Server in Avaya Aura® Contact Center Release 6.2.
5. Upgrade Contact Center License Manager.
6. Upgrade Communication Control Toolkit.
7. Upgrade Contact Center Multimedia.

Multinode migration with co-resident servers

In a multinode environment with Contact Center Manager Server, Contact Center Manager Administration, License Manager, and Server Utility installed co-resident, upgrade your servers in the following order:

1. Network Control Center
2. Co-resident Contact Center Manager Server, Contact Center Manager Administration, License Manager, and Server Utility server
3. Communication Control Toolkit
4. Contact Center Multimedia

Backup and restore of database files

Avaya recommends that all contact centers regularly backup database files to a secure location such as a tape drive or network drive. Backing up your database is also required before you migrate or upgrade a release of your Contact Center software.

The Database Maintenance utility (see Database Maintenance on page 109) is installed on the Communication Control Toolkit, Contact Center Manager Server, and Contact Center Multimedia servers to perform the required database backups and restorations using a common tool. Procedures for using the Database Maintenance utility are in *Avaya Aura® Contact Center Server Administration* (NN44400-610) or *Avaya Aura® Contact Center Routine Maintenance* (NN44400-514).

For Contact Center Manager Administration, you can use the Avaya Backup and Restore utility (see Operations performed with Contact Center Manager Administration on page 156 to back up a selected series of Contact Center Manager Administration files (including Historical Reporting files, AD-LDS files, and database files). You can also use the utility to schedule single or multiple backup tasks daily, weekly, or monthly. However, you cannot use this utility to back up operating system files or data files that are not related to Contact Center Manager Administration.

In addition to backing up Contact Center Manager Administration files, you must record your Real-Time Reporting configuration settings and your Emergency Help configuration settings whenever these settings change. During the restore, you must manually reconfigure these settings.

Contact Center Manager Server data files

Contact Center Manager Server data includes the following:

- agents, supervisors, skillsets, and all related assignments (accessed through Contact Center Management)
- CDNs, DNISs, and all other data items (accessed through the Configuration component)

Because all of your user or agent assignments, CDNs, and DNISs are stored on the Contact Center Manager Server, if your stand-alone Contact Center Manager Administration server fails, calls continue to be routed according to your defined scripts and your Contact Center can still receive calls.

Contact Center Manager Administration data files

Contact Center Manager Administration data includes the following:

- schedule information for historical reports
- partitions, access classes, report groups, and the Contact Center Manager Administration users
- real-time display configuration data and real-time display filters
- private historical reports
- Contact Center Management scheduled assignment information

To ensure the proper functionality of Contact Center Manager Administration, you must synchronize your Contact Center Manager Administration data and your Contact Center Manager Server data. Therefore, each time you back up the Contact Center Manager Server database, you must back up the Contact Center Manager Administration server at the same time. Likewise, you must restore the Contact Center Manager Administration server and the Contact Center Manager Server database at the same time.

However, because the Contact Center Manager Server data files do not change as often as Contact Center Manager Administration data files, you can back up your Contact Center Manager Administration server without backing up Contact Center Manager Server at the same time.

Using AD-LDS (ADAM) for Contact Center Manager Administration

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

- user information and details
- access classes
- partitions
- private and graphical real-time reports
- real-time report filters

The data files that are stored outside of AD-LDS are:

- 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 reports and report definitions
- Audit Trail events

Communication Control Toolkit data files

Communication Control Toolkit data includes the following:

- users, user groups
- terminals, terminal groups
- address, address groups
- workstations
- mappings between the resources

Contact Center Multimedia data files

Contact Center Multimedia data includes the following:

- customer and contact information for all multimedia contacts
- outbound campaigns and outbound campaign settings
- e-mail contacts and e-mail contact settings
- Web communications contacts and the corresponding contact settings
- instant message contacts and the corresponding contact settings
- Agent Desktop configurations
- external server settings

Timing for backups and restorations

Avaya recommends that you back up your Contact Center data at least once a day (or more frequently, based on your Contact Center requirements) to avoid loss of data if the server fails. You can back up your data one time, or you can schedule regular backups.

Avaya recommends that you schedule backups during periods of low activity.

Performing one-time or immediate backups

Avaya recommends that you back up your files immediately after you install your Contact Center software.

When you perform an immediate backup, you can view the Progress Information field to monitor the progress of the backup in either the Avaya Backup and Restore utility (for Contact Center Manager Administration) or the Database Maintenance utility (for Contact Center Manager Server, Communication Control Toolkit, and Contact Center Multimedia).

Performing scheduled backups

Schedule a regular backup of the Contact Center Manager Server Release 6.2 database to save the data. You must regularly back up the database to ensure you always have current information in case you need to restore the data.

Regularly scheduled backups overwrite the same file each time they occur. To keep more than one backup file, you must configure a separate network drive.

You can back up one or more databases at one time. The backup folder contains separate backup files for each database or folder you select. If you have two scheduled backups occurring at the same time, the backup with the larger time frame occurs first. For example, if you have a weekly backup and a monthly backup scheduled at the same time, the monthly backup runs first.

If your Contact Center runs with a standby server, ensure that you back up the primary server, not the standby server, to back up the most current data.

Hot patching

The 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 hot standby applications do not process contacts and can therefore be stopped and patched without shutting down the Contact Center.

Hot Patching servers

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.

1. Stop shadowing on the standby server (server B).
2. Stop all Contact Center services.
3. Install and apply the patch to the standby server (server B).
4. Start shadowing on the standby server.

   Ensure that you synchronize the data between the servers.
5. Manually switch the current standby server to the active server. Server A is now the standby server and Server B is the active server.
6. Stop shadowing on Server A.
7. Install and apply the patch to Server A.
8. Start shadowing on Server A.
9. Manually switch the current standby server to the active server. Server B is now the standby server and Server A is the active server.

Index