Avaya Aura™ Contact Center

Planning and Engineering

NN44400-210

Document status: Standard
Document issue: 02.07
Document date: 02 March 2011
Product release: Release 6.0/6.1
Job function: Planning and Engineering
Type: Technical Publication
Language type: English

Notices
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
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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(s) 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 this product. 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://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said 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, AND 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 the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) 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. 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(s) 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(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

New in this release

The following sections detail what is new in *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).

Navigation

- Features (page 11)

Features

See the following sections for information about feature changes:

- Operating system support (page 11)
- Co-resident installation options (page 12)
- Licensing options (page 12)
- Disk space requirements (page 12)
- Contact Center Installer (page 12)
- Traces (page 13)
- Server virtualization (page 13)
- Secure Access Link (page 13)

Operating system support

All Avaya Aura™ Contact Center server applications are supported on the following operating systems:

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

Contact Center client applications are supported on the following operating systems:

- Windows Vista Business SP1 (32-bit)
- Windows Vista Enterprise SP1 (32-bit)
- Windows XP Professional Service Pack 2 or later
- Windows 7

Attention: Contact Center does not support Internet Protocol version 6 (IPv6).

Co-resident installation options

Contact Center supports installing Contact Center Multimedia co-resident with Contact Center Manager Server. Contact Center Manager Administration and Communication Control Toolkit must also be installed before installing Contact Center Multimedia co-resident Contact Center Manager Server.

Contact Center also supports installing the Media Application Server (MAS) platform co-resident with Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit and Contact Center Multimedia.

The MAS platform is supported only in SIP-enabled contact centers.

These co-resident options reduce the number of servers required. The more Contact Center components installed co-resident with the Contact Center Manager Server the fewer active agents Contact Center Manager Server can handle.

Licensing options

Contact Center supports Essential, Nodal Enterprise, Corporate Enterprise, Nodal NCC, and Corporate NCC licensing modes.

- Essential licensing supports a single-server voice-only contact center with fewer than 100 agents.
- Nodal Enterprise licensing supports a single contact center installation.
- Corporate Enterprise licensing supports a network of contact center installations.
- Nodal NCC licensing supports a single License Manager in a network of contact center installations using networked skill-based routing.
- Corporate NCC licensing supports a secondary License manager and a network of contact center installations using networked skill-based routing.

You can maintain a secondary License Manager, which takes over the licensing if the primary License Manager fails. For more information about licensing, see Licensing considerations (page 59).

Disk space requirements

Significant changes in disk space requirements are required for Contact Center. For more information about disk partitioning requirements, see Disk partitioning requirements (page 88).

Contact Center Installer

The Contact Center Installer manages all Contact Center installations. The Contact Center Installer supports integration installation and data sharing for selected Contact Center applications. The Contact Center Installer automatically

installs most third-party software required by Contact Center and manages the installation order. For co-resident installations, you can select multiple applications and install them at the same time.

The Contact Center Installation DVD requires a dual-layer DVD drive; ensure that your system is equipped with a dual-layer DVD drive. You need not have a dual-layer DVD drive to download and install Service Packs.

Traces

In this release of Contact Center, tracing is turned on by default. The default location for log files is in the same directory and drive and trace files follow a common format.

Server virtualization

This release supports improved server virtualization. Virtualization enables you to share the resources of a single computer across multiple environments. You can host multiple operating systems and multiple applications locally and in remote locations, removing the constraints of physical and geographical limitations. For more information, see Server virtualization support (page 209).

Secure Access Link

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. For more information about Avaya Secure Access Link, see www.avaya.com/support.

Introduction

This document describes how to determine the engineering requirements of the Avaya Aura™ Contact Center Release 6.0/6.1 products, including the following components:

- Contact Center Manager Server (Single and Network Control Center)
- SIP-enabled Contact Center Manager Server
- Contact Center Manager Administration
- Contact Center Multimedia
- Communication Control Toolkit
- Contact Center License Manager
- Contact Center Manager Server Utility
- Co-resident configurations
- Service Creation Environment
- Security Framework

Navigation

- Contact Center overview (page 17)
- General information (page 39)
- Co-resident deployment strategies (page 33)
- Planning tools and utilities (page 37)
- Additional server requirements (page 51)
- Licensing considerations (page 59)
- Contact Center Manager Server configuration requirements (page 75)
- Contact Center Manager Administration configuration requirements (page 85)
- Contact Center Multimedia configuration requirements (page 95)
- Communication Control Toolkit configuration requirements (page 113)
- Security Framework configuration requirements (page 129)
- Co-resident configuration requirements (page 133)
- SIP Contact Center configuration requirements (page 149)
- Avaya Communication Server 1000 configuration requirements (page 161)
- Avaya Communication Server 1000 voice processing system configuration requirements (page 165)

Contact Center overview

This section provides an overview of Avaya Aura™ Contact Center. This guide focuses primarily on Contact Center Manager Server and Contact Center Manager Administration, but, where appropriate, it provides references to other documentation.

Navigation

- Contact Center components (page 17)
- SIP Contact Center components (page 22)
- Contact Center Multimedia components (page 27)

Contact Center components

The Contact Center application suite consists of the following components:

- Contact Center Manager Server (CCMS)—The core contact center component, which provides intelligent call routing. You can use Contact Center Manager Server to identify each agent's unique abilities, or skillsets. All incoming calls are routed to the agent with the appropriate skillset. Rules for treating and routing calls can be simple or complex.
- Contact Center Manager Administration (CCMA)—A component that provides browser-based access to the contact center for administrators and supervisors.
- Contact Center License Manager—A component that provides centralized licensing and control of all Contact Center Suite components and features across the Contact Center suite.
- Contact Center Manager Server Utility—A component used to monitor and maintain Contact Center Manager Server activity. The Contact Center Manager Server Utility provides functionality and performs tasks that are not available through the Contact Center Manager Administration application.
- Network Control Center (NCC) server (optional)—The server in a Contact Center Manager network that manages the Network Skill-Based Routing (NSBR) configuration and communication between servers. This component is required when multiple servers in Contact Center Manager Server sites are networked and operate as a single distributed contact center. It runs the Network Control Center software application, which is a feature of the Contact Center Manager Server software.
- Contact Center Multimedia (CCMM) (optional)—A client/server contact center application that expands contact center e-mail capabilities to view, respond to, and track requests over the Internet. Unlike a conventional e-mail system, which directs e-mail contacts to a single e-mail account, Contact Center Manager Server directs contacts to a skillset, or a group of qualified agents. The contact is handled by the first available agent in the

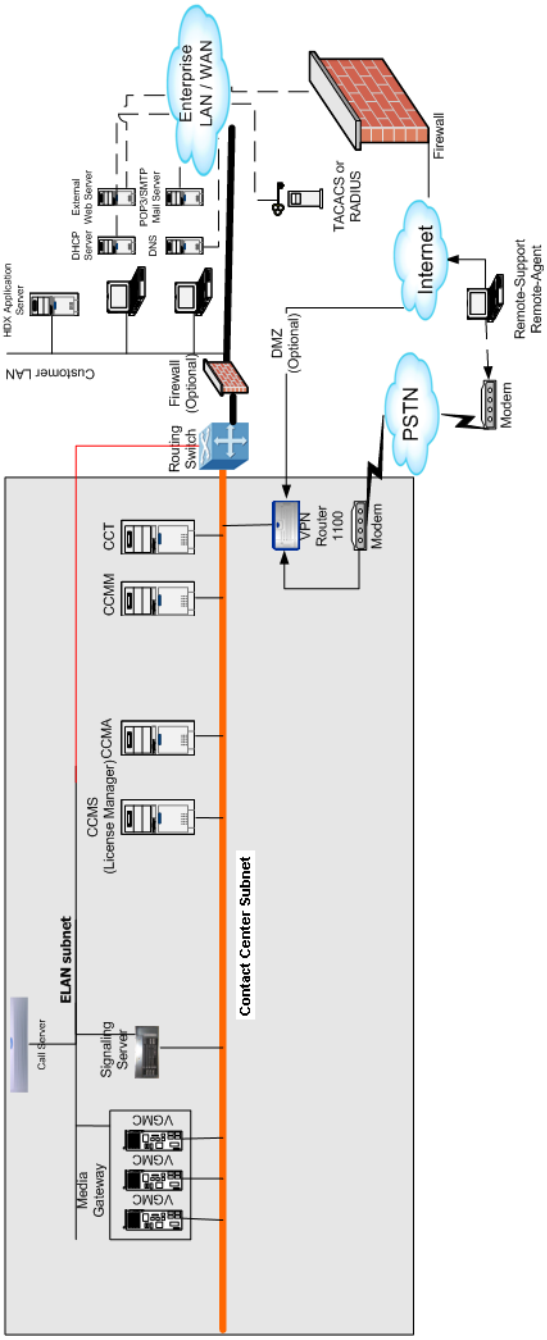
skillset. If more than one agent is available, the contact is routed to the agent with the highest priority for the skillset.
Contact routing ensures a contact center can measure and control the volume of traffic from the Internet. Supervisors and administrators can view real-time displays of contact center activities, as well as run historical reports.
The client component presents the agent with a browser-based graphical user interface. Agents can use it to respond to customers' requests over the telephone, by e-mail, or over the Internet.

- Communication Control Toolkit (CCT) (optional)—A client/server application that helps you implement Computer Telephony Integration for installed and browser-based client integrations. This application delivers a single cross-portfolio multiple-channel API that facilitates the integration of contact center, knowledge worker, and self-service solutions with your client applications.
- Host Data Exchange (HDX) application server (optional)—A host computer running a third-party provider application that receives data (such as a credit card number) from Contact Center Manager Server and returns data (such as an account balance) to Contact Center Manager Server. Contact Center Manager Server supports up to 10 HDX applications. Contact Center Manager Server installer includes a provider application. Contact Center Manager Server Utility includes a provider application as part of the installation.
- Service Creation Environment (SCE)—A graphical workflow application that you can use to program Contact Center applications. SCE provides a graphical editor to create TFE flows.
- Security Framework—Provides an identity management security framework that enables integration with the directory services infrastructure (for example Active Directory) for authentication and authorization of application users. The identify framework helps to reduce administrative costs and eliminates the redundant user information associated with per-application solutions. Single Sign-On (SSO) is a core feature of the framework which minimizes the necessity for end users to provide credentials after they log on. SSO with the desktop is supported, minimizing the need to authenticate after logging on to the desktop.

Hybrid solutions can be deployed for IP telephony configurations.

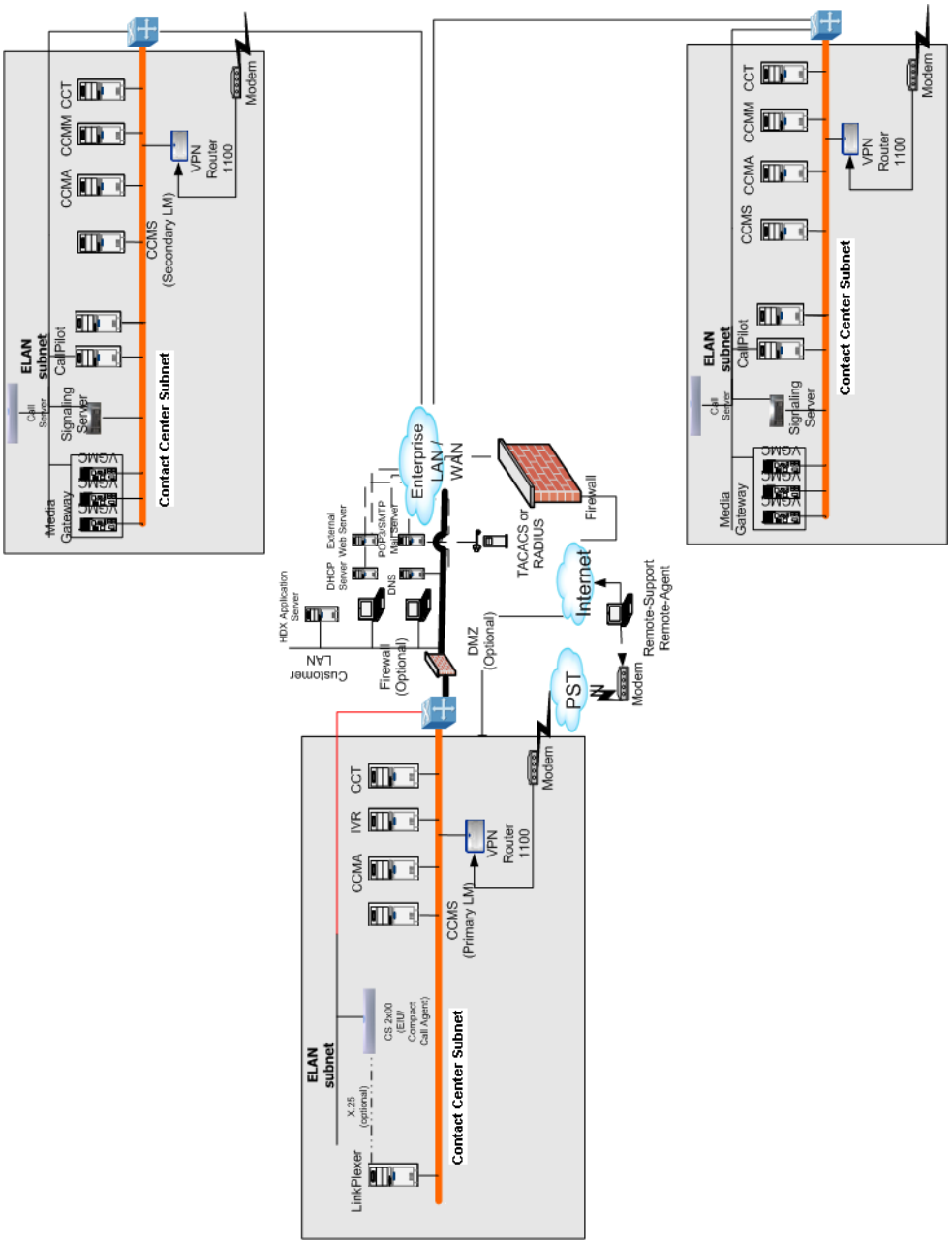
The following figure shows a contact center that is based on an Avaya Communication Server 1000 telephone switch in a nodal environment.

Avaya Communication Server 1000 nodal environment



The following figure shows a contact center that is based on an Avaya Communication Server 1000 telephone switch in a multinode environment.

Avaya Communication Server 1000 multinode environment



Contact Center Manager Server can co-reside with either Contact Center Manager Administration or both Contact Center Manager Administration and Communication Control Toolkit. Contact Center Manager Server can also co-reside with Contact Center Manager Administration, Communication Control

Toolkit, Contact Center Multimedia, and Media Application Server in limited circumstances. For more information about supported co-residency options, see Co-resident configuration requirements (page 133).

Contact Center client components

The Contact Center client components consist of the following components:

- Contact Center Manager Client—Client PCs used to administer the server and to monitor contact center performance using a browser-based interface. The number of these computers is usually proportional to the number of agents in the contact center.
- Avaya Aura™ Agent Desktop—Agent Desktop is a single-interface client application used by contact center agents to interact with customers. Agent Desktop agents can respond to customer contacts through a variety of media, including phone, outbound contacts, e-mail, Web communication, Fax messages, voice mail messages, scanned documents, SMS text messages, and instant messaging.

Telephony components

The telephony component consists of the following elements:

- IP phone—A telephone specifically for use in a Voice over IP (VoIP) system by converting standard telephone audio into a digital format that can be transmitted over the Internet, and by converting incoming digital phone signals from the Internet to standard telephone audio.
- Telephone—A device that converts acoustical energy (sound) into electrical energy for transmission to a distant point.
- Telephone switch—An electronic device that opens or closes circuits, changes operating parameters, or selects paths either on a space- or time-division basis. The switch directs the flow of electrical or optical signals from one side to the other. Switches with more than two ports, such as a LAN switch, can route traffic.

You can deploy Hybrid solutions for IP telephony configurations.

Voice services components

Voice services consist of the following components:

- Avaya CallPilot™—A voice mail system that can be used to provide front-end IVR or voice services to Contact Center Manager. If Avaya CallPilot is used for voice services—either Give IVR or ACCESS (Open/Close Voice Session, Give Controlled Broadcast, or Collect Digits)—the voice ports on this voice services platforms must be dedicated. (Contact Center Manager Server has direct access to them).
  - — Avaya CallPilot is an optional component and can only be used with Avaya Communication Server 1000 switches.

— On an Avaya Communication Server 1000E switch, this feature requires additional media card ports in the MG 1000E hosting the Avaya CallPilot server. For more information, see *Avaya Aura™ Contact Center Configuration – Avaya CS1000 Integration* (NN44400-512).

- Interactive Voice Response (IVR)—An application used by telephone calls to interact with a host computer using prerecorded messages and prompts. You can use IVR or third-party IVR systems to provide front-end IVR to calls before they are handed to Contact Center Manager Server.

SIP Contact Center components

The components in a SIP-enabled Contact Center are as follows:

- Contact Center Manager Server—SIP-enabled Contact Center Manager Server (CCMS) provides the existing range of features such as workflow scripting, agent and skillset management, agent selection, real time and historical reporting in a pure SIP environment.
- Communication Control Toolkit—Provides the application integration interface and Development Toolkit to support integration, control, and optionally the creation of the Agent Desktop user interface. Mandatory in SIP-enabled Contact Center to support application specifics such as Agent Login/Logout, Ready/Not Ready, and Activity Code Entry.
  The Communication Control Toolkit (CCT) APIs can integrate these Contact Center agent functions to third-party CRM or customer-defined agent user interface solutions.
- Contact Center License Manager (LM)—Use a License Manager for the centralized licensing and control of all Contact Center Suite components and features across the Contact Center suite.
- Media Application Server (MAS) is a software based media processing platform. All media processing is performed in software on the host CPUs. The MAS architecture is uniquely scalable for all core functions of the platform, including media processing, signaling, application execution, and content management.

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

  Conference–This service is used to create a MAS conference and anchor customer calls, announcements, and agent calls to the MAS conference.

  Announcement–This service is used to play treatment (ringback, announcements) into the MAS conference.

  Dialog–This service is used to play and collect DTMF digits entered in the

MAS conference.

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

Media Application Server (MAS)—The Media Server is the termination and origination point for RTP streams between the customer, media treatments, and eventually the agent.

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

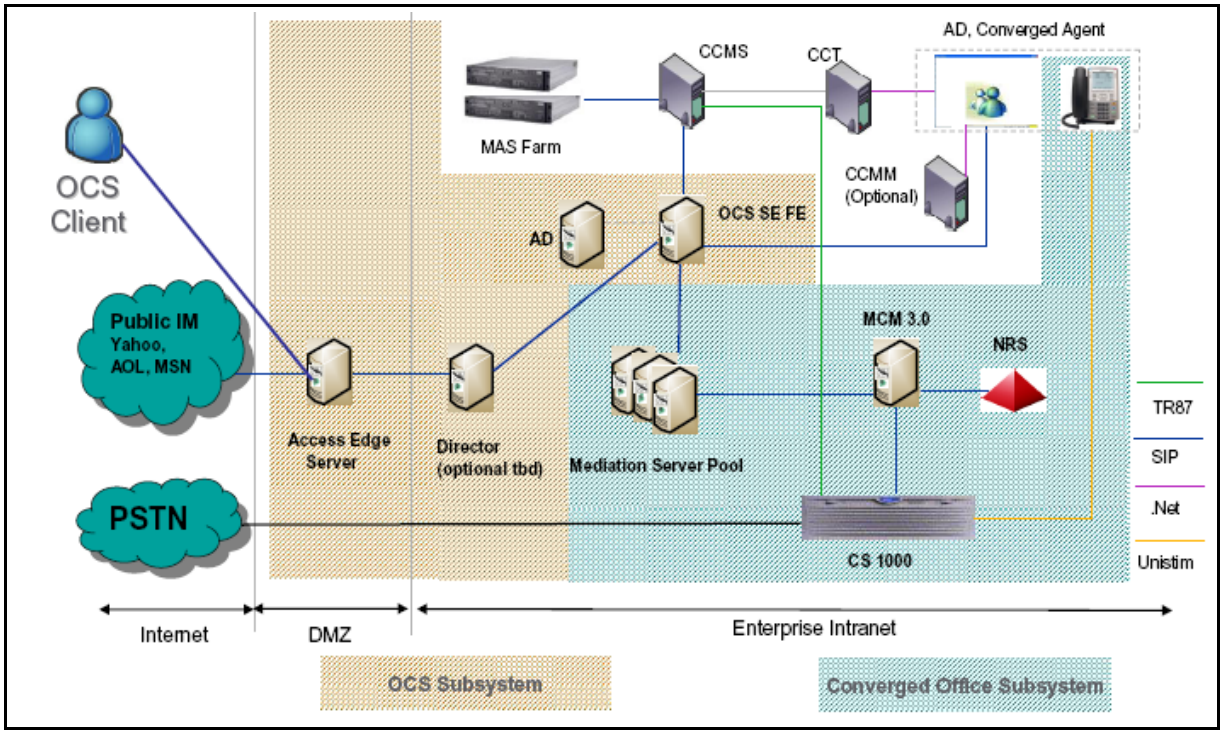
- Avaya Communication Server 1000 consists of the Call Server and Signaling Server
  - Avaya Communication Server 1000 Call Server—Avaya Communication Server 1000 is the call server that supports the agent desktop phones, which provide the voice support aspects of Converged Desktop. The desktop set is not an ACD set.
  - Avaya Communication Server 1000 Signaling Server. Engineer the Avaya Communication Server 1000 system so it can support SIP, in particular DSP hardware resources to support TDM/IP transcoding. Incoming PSTN calls require one DSP for each call. Agents with TDM phones each require another DSP. For more information, see Avaya *Communication Server 1000M Large System Planning and Engineering* (NN43021-220) and *Communication Server 1000E Planning and Engineering* (NN43041-220).
  - Avaya Communication Server 1000 Network Routing Service
- Microsoft Office Communications Server (OCS) 2007—OCS provides features such as enterprise-wide presence, security-enhanced enterprise instant messaging, host on-premise audio, and VoIP capabilities. The use of OCS as the SIP server in the SIP-enabled Contact Center solution opens new functionality and channels into the contact center with its support for federation with a wide range of public instant message clients such as Yahoo, AOL, and MSN.
- Agent Desktop solution
  - Agent Desktop—CCT-compliant Agent Desktop. A configurable smart client solution, SIP Contact Center agents can perform contact center-specific functions (such as Agent Login/Logout, Ready/Not Ready, and Activity Code Entry).

— Supported IP phone.

- Converged Office (optional)—The Converged Office feature for Avaya Communication Server 1000 provides a convergence of Avaya Communication Server 1000 capabilities with the real time multimedia communication and Remote Call Control (RCC) provided by OCS and Office Communicator (OC) applications. Converged Office integrates the Avaya Communication Server 1000 with the Microsoft OCS 2007 Enterprise Voice solution for a powerful converged office solution set that improves worker productivity. This efficiency is driven by telepresence and multimodal (business set VoIP, IM, and e-mail) communications bundle, with applications such as click-to-call and access mobility so workers can stay connected when not at their desks.

The following figure shows the SIP Contact Center solution and subsystems, including the optional Converged Office components such as the MCM and the Mediation Servers (administration-related components, such as Contact Center License Manager and Contact Center Manager Administration are omitted for clarity purposes). For more information about SIP-based Contact Centers, see SIP Contact Center configuration requirements (page 149).

SIP-based Contact Center



Differences between SIP architecture and standard Contact Center architecture

Differences between SIP architecture and standard Contact Center architecture include the following:

- In SIP architecture, the Contact Center interfaces with a SIP switch using an open standard SIP protocol, rather than a proprietary protocol such as AML for the Avaya Communication Server 1000.
- In SIP architecture, agent phones are not connected directly to the external switch as they are in Communication Server 1000, resulting in the different CTI requirements for configuring Converged Desktop for agents.
- SIP-enabled Contact Center directly controls a farm of new Avaya Media Application Servers (MAS) to provide media services, whereas Avaya Communication Server 1000 switches provide these services independently.
- SIP architecture does not use Avaya CallPilot.
- SIP architecture does not include support for IP call recording.

SIP-only interface

The SIP Contact Center solution uses a SIP-only interface between Contact Center Manager Server and the SIP Call Server. The SIP infrastructure is unaware of the nature of the Contact Center application it interoperates with; therefore, no ACD functionality is required.

A SIP-only interface Contact Center contains the following elements:

- Customer interface points—Telephone customers, multimedia-enabled internal help desks, 3G Video enabled wireless handsets, and SIP-supporting multimedia applications.
- SIP signaling (Internet to Intranet interface points) or SIP to Gateway Protocol converters (including SIP to PSTN Trunking, 3G Gateways, and SIP to H.323 Gateways)
- SIP Communication Control Toolkit—For a completely integrated desktop solution, the core SIP infrastructure must support the SIP CTI (ECMA) Converged Desktop signaling standard over SIP.
- SIP server—The Contact Center application is SIP-enabled.
- Avaya Media Application Server (MAS) farm
  - Servers are generally configured as an array of static IP addresses on the Contact Center. As such, the farm is hidden from the SIP infrastructure.
  - Specific services are offered, including Conversation Space, RAN, music, and integrated IVR.

— The Media Servers terminate SIP signaling from the Contact Center. They originate and terminate RTP signaling (for example, for voice) to the customer and the agent.

— Media Services can be invoked on non statically configured Media Servers where the SIP session is offered to the SIP proxy to locate and deliver the SIP session to the appropriate MAS.

- Communication Control Toolkit—Supports the requirements for Agent Desktop.
- Agent media termination device—For the Avaya Communication Server 1000/ OCS integration this is the Converged Office solution that supports Media Termination for voice, instant messaging, and presence.
- Avaya Aura™ Agent Desktop—Provides the Contact Center application functions such as Contact Center logon and logoff, Ready/Not Ready, Supervisor Observe, and screen pop functions.

Call server configuration support

Due to the requirement to support SIP CTI level desktop phone control, the chosen Agent Desktop solution is Avaya Communication Server 1000/Office Communications Server Converged Desktop. This requires an infrastructure that includes the following components:

- Avaya Communication Server 1000 Release 5.0, 5.5, 6.0 or 7.0 Call Server
- Avaya Communication Server 1000 Release 5.0, 5.5, 6.0 or 7.0 Signaling Server

The Avaya Communication Server 1000/OCS combination acts as a SIP protocol gateway transferring or redirecting calls to the SIP Contact Center.

Data network architecture considerations

With this architecture, no physical separation of subnets exists because Contact Center Manager Server acts as a SIP endpoint. Use a single-NIC card with mandatory selection of a single server subnet when you install Contact Center Manager Server for SIP connectivity.

SIP Contact Center usage of a contact center subnet

The SIP Contact Center solution uses the contact center subnet to enable the following components:

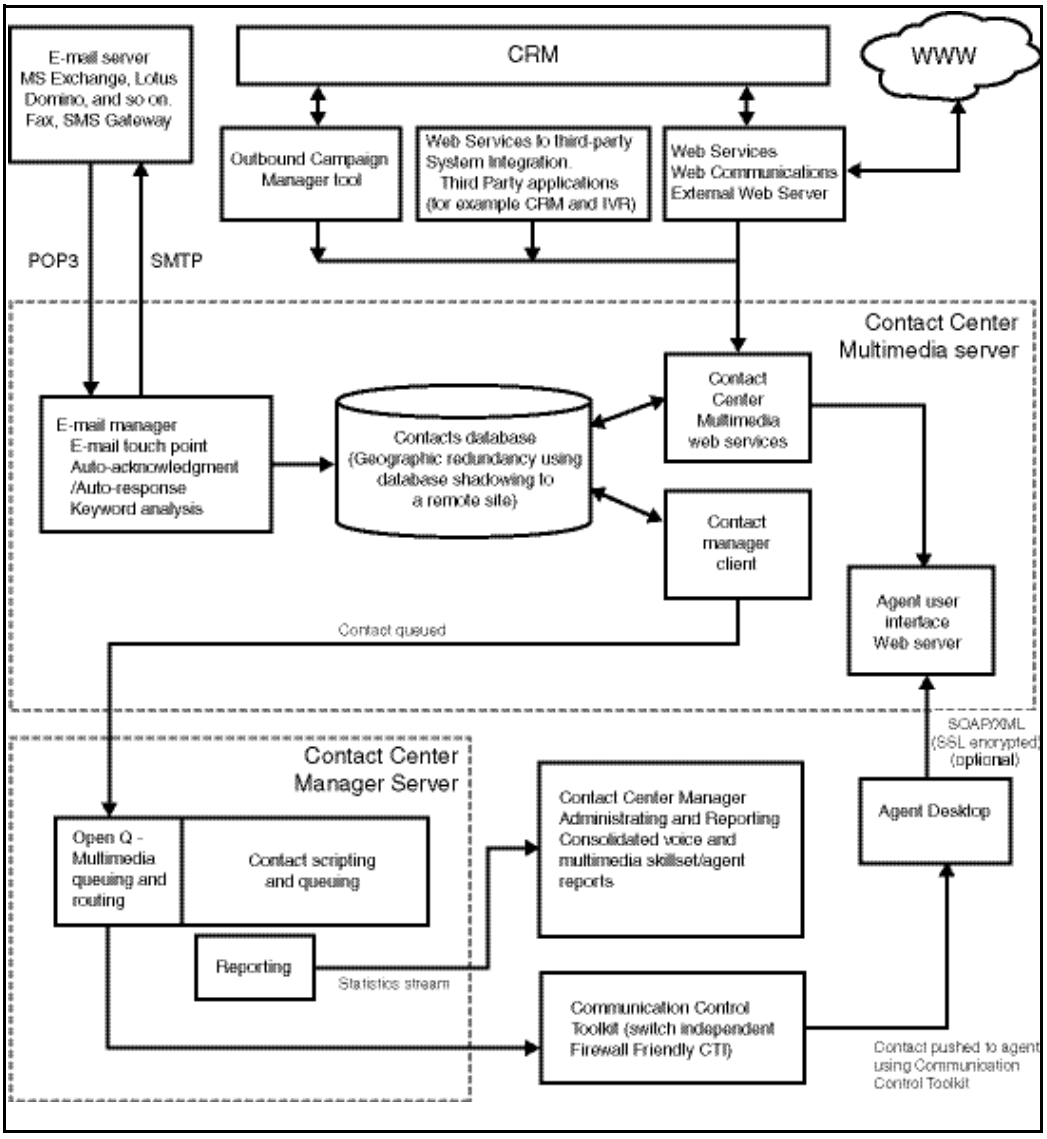
- SIP Signaling Communications between SIP Contact Center and OCS.
- SIP Signaling Communications between SIP Contact Center and Avaya Communication Server 1000 Signaling Server.
- SIP Signaling Communications between SIP Contact Center and one or more Media Application Server (MAS) running SIP Contact Center application services.

- RTP streams to and from the Media Application Server and Customer Gateway (Avaya Communication Server 1000, 3G Gateway, PRI Gateway, and so on). Therefore, standard VoIP engineering is required for voice streaming.
- Other miscellaneous communications (such as Contact Center Manager Server to Communication Control Toolkit or Contact Center Manager Server to Agent Desktop).

Contact Center Multimedia components

Contact Center Multimedia is part of the Contact Center Manager suite of applications. Contact Center Multimedia provides outbound, e-mail, and Web communication features for the contact center. The following figure provides an overview of Contact Center Multimedia with Contact Center Manager Server.

CCMM components



Contact Center Multimedia consists of the following components:

- Contact Center Multimedia database—This component is installed on the Contact Center Multimedia server and is an InterSystems Caché database that stores all contact center activity. All incoming e-mail, Web requests, and associated responses are stored in a structured format within the database. Information about Outbound campaigns are also stored in this database.
- E-mail Manager—This component is installed on the Contact Center Multimedia server. The E-mail Manager connects to the e-mail server at regular intervals. During each connection, all configured mailboxes are accessed. E-mail from the customer is read from the e-mail server,

processed, and stored in the database. Outgoing e-mail, generated from the e-mail responses stored in the database, is sent to the e-mail server.

- Outbound Campaign Management Tool—This component is installed on the Contact Center Multimedia server and is accessed using the Contact Center Manager Administration application. The Outbound Campaign Management Tool is used to create, modify, and monitor outbound campaigns. An outbound campaign is a series of outbound calls for one specific purpose, for example, a customer survey, or a sales promotion. Use the Outbound Campaign Management Tool for the following activities:
  - define campaign parameters
  - import and review call data
  - create agent call scripts
  - monitor campaign results
  - export campaign data

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

- Web communications—The Web communications component includes a set of Web Services on the Contact Center Multimedia server for communication between the agent and the customer. A set of sample Web pages are installed on the Contact Center Web site showing how Web Services are used to implement Web pages to provide Web Chat (click to chat) and Scheduled Callback (click to talk) features.
- Agent Desktop interface—This component is installed on the Contact Center Multimedia server. Agents use Internet Explorer to connect to the Contact Center Multimedia server to retrieve the Agent Desktop interface. The Communication Control Toolkit pushes e-mail, Web requests, outbound contacts and voice calls to the Agent Desktop interface. The Agent Desktop interface uses Web services to retrieve e-mail, Web requests, outbound campaign information, and customer details and history from the Contact Center Multimedia database. Web services are also used to send e-mail replies and save outbound call details in the Contact Center Multimedia database.
  E-mail contacts are presented to agents through the Agent Desktop interface, where agents can;
  - verify customer information
  - access historical e-mail to and from the customer
  - create responses to customer inquiries
  - provide a closed reason (if configured)

When an outbound campaign is running, contacts are presented to agents through the Agent Desktop interface, where the agents can;

- — preview contact information
- — review call scripts (if configured)
- — save scripts
- — select a disposition code

- Contact Center Multimedia Administrator—This component is installed on the Contact Center Multimedia server. The Contact Center Manager Administration provides administrative and management capabilities.

Processing multimedia contacts

Contact Center Multimedia receives multimedia contacts through two external interface points: the e-mail server and the External Web server.

E-mail server contacts

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

The IMH logs on to the mailboxes on the e-mail server as listed in the E-mail Manager. It parses e-mail in the mailboxes and stores them in the Contact Center Multimedia database. Any attachments associated with an e-mail are stored in the Inbound attachment folder, as specified in the Contact Center Manager Administration. After an e-mail is successfully stored in the Contact Center Multimedia database, it is deleted from the e-mail server.

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

External Web server transactions

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

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

A set of sample pages is distributed with Contact Center Multimedia to provide Java Server Pages (JSP) script examples of how a Web server can access the Web services. You must create your own Web pages, with their own look, feel, and business logic.

Integration with Contact Center Manager Server

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

Contact Center Manager Server supports Open Queue.

Co-resident deployment strategies

This section provides information about co-resident support for Avaya Aura™ Contact Center applications, migration procedures, and functionality.

Navigation

Supported co-resident applications

You can install Contact Center Manager Server either alone on a server or on a server with other Contact Center applications. When the Contact Center Manager Server is installed alone, 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 you can install on the same server with the Contact Center Manager Server software.

Contact Center co-resident configurations

	CCMS	CCMA	CCT	CCMM	License Manager	Server Utility	AAAD	SCE	MAS
CCMS	N/A	Yes	Yes (see Note 3)	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 (see Note 2)	Yes	Yes
CCT	Yes (see Note 3)	Yes (see Note 1)	N/A	Yes (see Note 4)	Yes (see Note 1)	Yes	Yes (see Note 2)	Yes	Yes
CCMM	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	N/A	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)
License Manager	Yes	Yes (see Note 1)	Yes (see Note 1)	Yes (see Note 4)	N/A	Yes	Yes (see Note 2)	Yes (see Note 1)	Yes
Server Utility	Yes	Yes	Yes	Yes (see Note 4)	Yes	N/A	No	Yes	Yes
Security Framework	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
AAAD	Yes (see Note 2)	Yes (see Note 2)	Yes	Yes	Yes (see Note 2)	Yes (see Note 2)	N/A	Yes (see Note 2)	Yes
SCE	Yes	Yes	Yes (see Note 1)	No	Yes (see Note 1)	Yes	No	N/A	Yes
MAS	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	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 on the same server 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. CCMM and CCMS co-residency is supported to a 200-agent limit. The agent limit is 100 with an Essential license.

Note 5: CCMS, CCMA, CCT, and CCMM must be installed on the same server for MAS to co-reside with CCMS. MAS is supported only in SIP enabled contact centers. If the 200-agent limit is reached for a SIP-enabled single server installation with MAS and CCMM, MAS and CCMM must be removed from the server at the same time.

Note 6: In SIP-enabled contact centers, for CCMM to co-reside with CCMS, MAS must also be installed co-resident.

- 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 be used only to administer the co-resident Contact Center Manager Server and not to 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 administer only 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. For more information, see Co-residency and your network (page 139).

For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).

Co-resident upgrade procedures

The Contact Center migration procedure requires that you migrate all co-resident Avaya NES Contact Center Release 7.0 applications at the same time.

Security Framework deployments

If you plan to use a single security domain for 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 to host the primary security server based on the deployed applications:

- Avaya Communication Server 1000 Release 6.0.

  If the Avaya Communication Server 1000 Release 6.0 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.

- Media Application Server (MAS) or NMC.

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 MAS, you must configure Avaya Communication Server 1000 Release 6.0 to host the primary security server, or security domain in your network.

If you do not want to configure your application 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.

Security Framework is not supported co-resident with Media Application Server (MAS).

Application start order

Due to the multiple server configuration of most contact centers, it is important to note the start order of the servers. Contact Center Manager Server is the main server. It must be running first, before the Contact Center Manager Administration, Contact Center Multimedia, and Communication Control Toolkit server can communicate with it.

Contact Center Manager Administration administers the Contact Center Manager Server and the Contact Center Multimedia, so it is the last server that is required to be running.

No dependency exists between the Contact Center Multimedia server and the Communication Control Toolkit server in terms of startup sequence.

Communication Control Toolkit cannot work until Contact Center Manager Server is working. If Communication Control Toolkit starts first, it repeatedly attempts to connect to Contact Center Manager Server. After Contact Center Manager Server starts and is working, Communication Control Toolkit connects to it and starts working.

Planning tools and utilities

You can purchase your choice of server hardware as long as it complies with the Platform Vendor Independence (PVI) specification for Avaya Aura™ Contact Center software. You have the flexibility to purchase a hardware specification that conforms with your corporate standard. Contact Center is a suite of software applications. Contact Center has two utilities to help you choose and check your hardware for compliance with the Contact Center Platform Vendor Independence (PVI) specification.

Navigation

- Capacity Assessment Tool (page 37)
- Platform Vendor Independence checking utility (page 38)

Capacity Assessment Tool

You must ensure that the platform on which you plan to install Contact Center satisfies the capacity requirements of your contact center. To assist you, Avaya provides the Capacity Assessment Tool (CapTool).

The Capacity Assessment Tool (CapTool) is a stand-alone Microsoft Excel spreadsheet application that you use to determine the processor capacity requirements of the following components:

- Contact Center Manager Server
- Network Control Center
- Contact Center Manager Administration
- Contact Center Multimedia
- Communication Control Toolkit
- Contact Center License Manager
- Co-resident server

CapTool helps you to plan for a new Contact Center Manager system, or to determine how proposed changes affect an existing system. CapTool can also estimate the following requirements:

- the number of voice ports required for a specified call complexity and call load
- the data network bandwidth requirement on the contact center subnet, as generated by each contact center server, due to real-time data, reporting, and other data-intensive activities
- (in a networked-contact center server environment) the bandwidth requirements due to network data traffic for the WAN connecting the local

Contact Center Manager Server and all remote Contact Center Manager Servers

CapTool uses mathematical models to estimate the performance and capacity of the required components. The requirements are based on your specifications for your contact center parameters; for example, your agent count, your expected call rate and call complexity.

The quality of the results obtained from the tool is directly proportional to the quality of the input received from the user. To use CapTool effectively, you must ensure that the input is as accurate as possible. You can download the CapTool utility from the support Web site (www.avaya.com/support).

The most recent version of the Capacity Assessment Tool User's Guide is included in the Capacity Assessment Tool download.

Platform Vendor Independence checking utility

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

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

Use the Platform Vendor Independence utility in conjunction with the guidelines stated in this document.

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

General information

This section provides information about product compatibility with Avaya Aura™ Contact Center and differences between supported telephony switches.

Navigation

- Product compatibility (page 39)
- Supported switch releases and system types (page 44)
- Contact Center content by switch platform (page 47)
- Supported upgrade and migration paths (page 48)

Product compatibility

This section describes product compatibility with Contact Center.

Avaya Communication Server 1000

Contact Center Manager Server provides switch connectivity to the Avaya Communication Server 1000 switching platform.

For more information about the Avaya Communication Server 1000 switching platform, see Avaya Communication Server 1000 configuration requirements (page 161).

Avaya Aura™ Unified Communications platform

Contact Center Manager Server provides switch connectivity to the Avaya Aura™ Unified Communications platform.

Voice services: Avaya Voice Portal, Avaya CallPilot and Avaya MPS

The following table lists Avaya Voice Portal, Avaya CallPilot™ and Avaya MPS products and versions that are compatible with Contact Center.

Contact Center voice services product compatibility

Product name	Supported releases
Avaya IVR-CTI Integration server (MPS)	3.5
Avaya Agent Greeting	3.0X and later (for AML only)
Avaya Voice Portal	5.1 and later
Avaya CallPilot	5.0 and later
Avaya MPS 500	3.5
Avaya MPS 1000	3.5

Contact Center voice services product compatibility

Product name	Supported releases
MAS	6.4
Remote Agent Observe	(Avaya Communication Server 1000 AML only)

Avaya CallPilot and Avaya MPS are not supported in a SIP-enabled Contact Center. For the SIP-enabled Contact Center the Media Application Server (MAS) component provides media services.

Other product release compatibility

The following table lists other products supported with Contact Center Manager Server and Avaya Communication Server 1000.

Product compatibility with Contact Center

Product name	Supported releases
Optivity Telephony Manager (OTM)	2.0 or later
IRA (formally MIRAN)	2.0, 3.0
Internet Telephony Gateway Trunk (ITG-T)	2.2, 3.0
Internet Telephony Gateway Line (ITG-L)	2.2, 3.0
Avaya i2002 Digital Deskphones (as Agent)	All releases
Avaya i2004 Digital Deskphones (as Agent or Supervisor)	All releases
Avaya i2050 Digital Deskphones (as Agent or Supervisor)	All releases
Avaya 3904 Digital Deskphones (as Supervisor)	All releases
Avaya 3905 Digital Deskphones (as Agent or Supervisor)	All releases
Remote Office 9150	1.3.4
Remote Office 9110, 9110, IP adapter	1.3.4

For phones, Internet Telephony Gateway, Optivity Telephony Manager, Remote Office, and MIRAN users, the switch release determines which product version is relevant.

Supported telephone switches

Contact Center Manager Server supports the following switch types:

- Avaya Communication Server 1000
- Avaya Communication Server 1000 and *or* with Microsoft Office Communications Server (SIP)
- Avaya Aura™ Unified Communications platform

The term telephone switch is used in this document as a generic term to refer to any of the previously specified telephony platforms that interoperate with Contact Center Manager.

The following table outlines the differences between features supported by the Avaya Communication Server 1000 and SIP switch.

Telephone switch comparison

Feature	Avaya Communication Server 1000	Avaya Communication Server 1000 + Office Communications Server (SIP)
Agent features		
Number of active agents	5000 for each Contact Center Manager	1500 per Contact Center Manager
Agent logon location	The agent can log on at any ACD phone.	Any Communication Control Toolkit-compliant desktop application (for example Agent Desktop). The agent's media termination device must be SIP-addressable. The media termination device does not need ACD capabilities.
Length of Agent ID	4 to 16 digits	4 to 16 digits
Validation of agent login	Contact Center Manager validates agent login.	Contact Center Manager validates agent logon
Agent non-ACD DN	Personal DN follows agent (FWD)	DN (or SIP address) is specific to the user
Call presentation features	Contact Center Manager phone Union Break Time, Call Forcing, Alternate Call Answer, Host Delay Time for each agent	Contact Center Manager phones Union Break Time, Call Forcing, Alternate Call Answer, Host Delay Time for each agent
Walkaway trigger	Headset removal	Agent Not Ready
Phone features		
Conference	6-way Conference	Consult only
Transfer and conference	Separate transfer, conference, simple	Consult only conference and transfer

(1 of 4)

Telephone switch comparison

Feature	Avaya Communication Server 1000	Avaya Communication Server 1000 + Office Communications Server (SIP)
Entry/reporting of activity (Line of Business) code	Supported	Supported by CCT application (Agent Desktop)
Blind transfer to CDN	Not applicable	Not applicable
Blind transfer to busy/ invalid number	Supported (with CCT)	Not applicable
Agent transfer/ conference from InCalls to second agent InCalls key	Not applicable	Supported
Entry of activity (LOB) and emergency key while in conference	Not applicable	Emergency key not supported
Completion of transfer while far end is ringing (including blind transfers)	If the far end address is out-of-provider (not monitored by CCT), the remote connection state transitions immediately from the Alerting state to Established.	The remote connection state remains in the Alerting state until the far end actually answers the call.
Telephone switch resource features		
Telephone switch interface	AML connection	SIP only
Number of digits for CDN	7	7 (to maintain compatibility with Communication Server 1000 Converged Desktop)
Number of characters for CDN URI	Not applicable	Up to 30
Number of digits for DNIS	7	7 (to maintain compatibility with Avaya Communication Server 1000 Converged Desktop)
Number of characters for DNIS URI	Not applicable	Up to 30
Number of digits for agent ID	5	5

(2 of 4)

Telephone switch comparison

Feature	Avaya Communication Server 1000	Avaya Communication Server 1000 + Office Communications Server (SIP)
Number of digits for activity (Line of Business) code	3 to 32	3 to 32
Trunk and route statistics and displays	Supported	Not applicable
Synchronization of deleted resources	Reported by telephone switch	
Monitoring of link status	Telephone switch brings down link after 20 non response calls	Through SIP registration refresh events
Handling of resources upon link failure	Retained	Re-registered upon link recovery
Recovery after link failure	Issues call release messages	Automatic upon SIP registration refresh events
Order of call presentation	Telephone switch alternates Contact Center Manager CDN and NACD ACD calls	Direct to Contact Center through SIP proxy
Treatments		
IVR	Supports integrated IVR with Avaya CallPilot	Supports integrated IVR with Media Application Server
Caller-entered data for external IVR	Not supported	Not supported
Give IVR script command	Supported	Supported and enhanced for Voice XML
IVR statistics, displays	Supported	Limited support
RAN	Supported	Supported by MAS for voice and video
Controlled option for treatments	Supported. Return to CDN without answer supervision	
Automatic ringback	Supported	Supported
Automatic treatment resumption	Supported	Not supported - can be provided by Contact Center Manager script

(3 of 4)

Telephone switch comparison

Feature	Avaya Communication Server 1000	Avaya Communication Server 1000 + Office Communications Server (SIP)
Networking features		
Ability to network multiple Contact Center Manager Servers	Supported	Not supported
Networking statistics and displays	Supported	Not supported
Other features		
Call information	Directly supports call information (for example, CLID, DNIS, trunk, NPA)	Supports some call information (DNIS) as well as SIP call information (for example, SIP to address, SIP from address)
Hardware dongle	Not required	Not required
Call ID reuse	Depends on telephone switch configuration	Every 40 000 calls
Language support	Multilanguage support	
Reporting of internal and external DN calls	Reported separately	Reported as a combined total
Trigger for pegging of outgoing DN call	Call connection	When dialing complete
ACD and NACD calls	Reported separately	Not applicable
Taking skillsets out of service manually	Not applicable	Not applicable
Emergency	Not applicable	Not supported
(4 of 4)		

Supported switch releases and system types

Contact Center Manager continues to provide switch connectivity to the Avaya Communication Server 1000 telephone switching platforms.

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

AML-compatible switch	Supported versions
Avaya Communication Server 1000E	5.0, 5.5, 6.0, 7.0
Avaya Communication Server 1000E SA Co-res	5.0, 5.5, 6.0, 7.0
Avaya Communication Server 1000E SA	5.0, 5.5, 6.0, 7.0
Avaya Communication Server 1000E HA	5.0, 5.5, 6.0, 7.0
Avaya Communication Server 1000M Single Group	5.0, 5.5, 6.0, 7.0
Avaya Communication Server 1000M Multi Group	5.0, 5.5, 6.0, 7.0
Avaya Communication Server PBX 11C - Chassis	5.0, 5.5, 6.0, 7.0
Avaya Communication Server PBX 11C - Cabinet	5.0, 5.5, 6.0, 7.0
Avaya Communication Server PBX 61C	5.0, 5.5, 6.0, 7.0
Avaya Communication Server PBX 51C	5.0, 5.5, 6.0, 7.0
Avaya Communication Server PBX 81C	5.0, 5.5, 6.0, 7.0

Contact Center provides support for the Avaya Communication Server 1000 software releases and switching platforms for a converged OCS Communication Server with SIP as shown in the following table.

SIP-compatible switch	Supported versions
Avaya Communication Server 1000E	5.0, 5.5, 6.0, 7.0
Avaya Communication Server 1000E SA Co-res	5.0, 5.5, 6.0, 7.0
Avaya Communication Server 1000E SA	5.0, 5.5, 6.0, 7.0
Avaya Communication Server 1000E HA	5.0, 5.5, 6.0, 7.0
Avaya Communication Server 1000M Single Group	5.0, 5.5, 6.0, 7.0
Avaya Communication Server 1000M Multi Group	5.0, 5.5, 6.0, 7.0

Engineer the Avaya Communication Server 1000 PABX so it can support Contact Center, in particular engineer PABX resources to support the required agent numbers and call volume. For more information, see *Communication Server 1000M Large System Planning and Engineering* (NN43021-220) and *Communication Server 1000E Planning and Engineering* (NN43041-220).

The Avaya Aura™ Contact Center High Availability feature is supported on Avaya Communication Server 1000 Release 6.0 or later. If using an Avaya Communication Server 1000 Release 6.0 PABX, patch MPLR30010 must be applied to the PABX to support Avaya Aura™ Contact Center High Availability functionality.

Contact Center provides support for the Avaya Aura™ Unified Communications platform as shown in the following table.

SIP-compatible switch	Supported versions
Avaya Aura™ Unified Communications platform	5.2.1 or later.

For more information about the Avaya Aura™ Unified Communications platform, see *Avaya Aura™ Contact Center Configuration – Avaya Aura™ Unified Communications Platform Integration* (NN44400-521).

All other switches are not supported.

Supported phones

This section describes the phones supported with Contact Center Manager Server.

Avaya Aura™ Unified Communications platform

Avaya Aura™ Contact Center supports the following Avaya Aura™ Unified Communications platform phones:

- Avaya 4600 Series IP Deskphone
- Avaya 9600 Series IP Deskphone
- Avaya one-X Communicator 5.2 or later

Contact Center phones

Phones that are designed specifically for contact centers are recommended for use with Contact Center Manager Server.

- Avaya 3905 Digital Deskphone –Contact Center Telephone

Avaya Communication Server 1000 ACD phones

Contact Center Manager Server also supports all phones that can be configured for use with Avaya Communication Server 1000. These include:

- Avaya 39xx Digital Deskphone
  - Avaya 3904 Digital Deskphone
  - Avaya 3905 Digital Deskphone
- IP phones and Softphones
  - Avaya 1120E IP Deskphone
  - Avaya 1140E IP Deskphone
  - Avaya 1150E IP Deskphone
  - Avaya 1200 Series IP Deskphone
  - Avaya 2002 IP Deskphone
  - Avaya 2004 IP Deskphone

— Avaya 2050 IP Softphone

The following conditions apply:

- Support of specific types of phones can change with each software release of the call server (Avaya Communication Server 1000). Consult the Avaya Communication Server 1000 documents for an up-to-date list of supported phone types for the software release in use.

Contact Center content by switch platform

The following table lists the available Content Center portfolio features depending on the choice of switch platform, either Avaya Communication Server 1000 or Office Communications Server (SIP).

Content by switch platform

Content	Avaya Communication Server 1000	Avaya Communication Server 1000 + OCS (SIP)
UNSBR—Universal networking	Yes	No
Standby server enhancements	Yes	Yes
Geographic redundancy	Yes	No
Corporate License Manager	Yes	Yes
Communication Control Toolkit	Yes	Yes
Agent Desktop	Yes	Yes
Contact Center Multimedia	Yes	Yes
Contact Center Outbound	Yes	Yes
Network-wide agent administration	Yes	Yes
ICM support	No	No
Single network interface card (NIC)	Yes	Yes
Server Utility	Yes	Yes
Report Creation Wizard	Yes	Yes
Five-digit agent ID	Yes	Yes

Supported upgrade and migration paths

A software upgrade occurs on the same hardware and operating system platform. It requires placing Contact Center operation out of service during the upgrade. The software upgrade procedure ensures that the statistical and configuration data is retained and converted for the Contact Center (Avaya Aura™ CC) applications. A software upgrade occurs on the same hardware platform.

Windows Server 2008 Release 2 is the only Operating System platform supported for Contact Center; therefore, software upgrades using the operating system from previous contact center releases are not supported.

A migration procedure migrates the statistical and configuration data from one server to another. You can migrate your existing Contact Center customer data to Contact Center on a new Windows Server 2008 Release 2 64-bit server. You can migrate all your old configuration and statistical data to the new Contact Center server so no data is lost in the move.

The following table shows the supported migration paths from Avaya NES Contact Center Release 6.0 and 7.0 releases to this release of Avaya Aura™ Contact Center.

Contact Center migration paths

	CCMS	CCMA	CCT	CCMM	License Manager	Server Utility	Security Framework	Service Creation Environment	Media Application Server
CCMS 7.0	Yes	—	—	—	—	—	—	—	—
CCMA 7.0	—	Yes	—	—	—	—	—	—	—
CCT 7.0	—	—	Yes	—	—	—	—	—	—
CCMM 7.0	—	—	—	Yes	—	—	—	—	—
LM 7.0	—	—	—	—	Yes	—	—	—	—
SP 7.0	—	—	—	—	—	N/A*	—	—	—
SF 7.0	—	—	—	—	—	—	N/A*	—	—
SCE	—	—	—	—	—	—	—	N/A*	—
CCMS 6.0	Yes	—	—	—	—	—	—	—	—
CCMA 6.0	—	Yes	—	—	—	—	—	—	—
CCT 6.0	—	—	Yes	—	—	—	—	—	—
CCMM 6.0	—	—	—	Yes	—	—	—	—	—
LM 6.0	—	—	—	—	Yes	—	—	—	—
SP 6.0	—	—	—	—	—	N/A*	—	—	—

Contact Center migration paths

	CCMS	CCMA	CCT	CCMM	License Manager	Server Utility	Security Framework	Service Creation Environment	Media Application Server
SF 6.0	—	—	—	—	—	—	N/A*	—	—
SCE	—	—	—	—	—	—	—	N/A*	—

* Server Utility, Security Framework, and Service Creation Environment do not use a database. Migration is basically a new installation on the new server.

At a high level, an Avaya NES Contact Center Release 7.0 migration proceeds as follows:

1 Backup the database on the Avaya NES Contact Center Release 7.0 server.

2 On the new Contact Center server, map a drive to the location of the backed up data.

3 On the new Contact Center server, start the Product Installation on the Contact Center DVD.

4 During the installation interview phase you provide the locations of the backed up data. This applies to CCMS, CCT, and CCMM components.

5 During the installation, the backed up data is migrated to the new Contact Center server.

6 Restart the system.

For more information about upgrades, see *Avaya Aura™ Contact Center Upgrade and Patches* (NN44400-410).

Additional server requirements

Before you start to install of the Avaya Aura™ Contact Center components, determine which configuration your contact center requires and your server hardware requirements.

Navigation

Overview

All requirements in this section of the document apply to the full list of Contact Center applications:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Network Control Center (NCC)
- Contact Center Manager Administration (CCMA)
- Contact Center Multimedia (CCMM)
- Contact Center Outbound
- Communication Control Toolkit (CCT)
- Service Creation Environment (SCE)
- Security Framework
- Contact Center co-resident configurations
- Contact Center Media Application Server (CCMAS)

The term Contact Center applications is used to refer collectively to all the applications in the previous list.

You can install Contact Center applications on servers that

- meet the minimum hardware specifications in this document
- meet the operating system and third-party software guidelines in this document
- meet any other guidelines in this document

Server naming requirements

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

- Use only characters a to z, A to Z, and 1 to 9 can be used in a host name.
- Do not use the underscore character (_) and period character (.).
- Do not use spaces in the host name.
- Host names must be 6 to 15 characters in length.
- Host names must not start with a number.

Fully qualified domain names must not exceed 255 characters.

Each Contact Center server must be able to resolve the host name or computer name of all other Contact Center servers within the configuration. If you have a Domain Name Service (DNS) server, make sure an entry exists for each Contact Center server. If you do not have a DNS server, you must manually update the HOSTS file on each server with the host name or computer name of all other Contact Center servers to ensure that all clients can interpret the server names.

Third-party software requirements

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

Application class software generally requires a certain amount of system resources and must not be installed on a server running Contact Center applications. The installation of third-party applications can cause Contact Center applications to operate outside of the known engineering limits and can create potential unknown system problems (for example, CPU contentions, increased network traffic loading, disk access degradations).

Certain third-party utility class software applications, such as hardware diagnostics or backup tools, generally require less system resources during the normal operation of Contact Center applications and are permitted. Exceptions are utilities such as screen savers, which can cause system problems and degrade performance.

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

Generic guidelines for utility-class software applications

The following are generic guidelines for utility-class software:

- During run-time, the utility must not degrade the contact center application beyond an average percentage of CPU use (see each specific application section in this document for the recommended maximum CPU usage level) Furthermore, the utility must not lower the minimum amount of free hard disk space required by contact center application and the Windows Operating system.
- The utility must not cause improper software shutdowns or out-of-sequence shutdowns.
- The utility must not administer the contact center application.
- If the utility has a database, it must not affect the contact center application database.
- Disk compression utilities must not be used.
- Memory tweaking utilities (for example, WinRAM Turbo, Memory Zipper) used to reclaim memory that is unused by Microsoft must not be used.
- The installation or uninstallation of the third-party software must not impact or conflict with the contact center application (for example, it must not cause DLL conflicts). If such conflicts are discovered, a server rebuild may be necessary.
- The implementation personnel must perform tests to ensure these conditions and recommendations are met before you place the Contact Center application into production. Support personnel may ask for the results of the testing during fault diagnosis. As part of fault diagnosis, the distributor or end user may be asked to remove third-party software.
- HyperTerminal must not be installed on the Communication Control Toolkit Server as it interferes with the operation of the Communication Control Toolkit Telephony Server.

Additional guidelines for the use of anti-virus software

Your security policies may require the installation of antivirus software on the application server.

The Contact Center supported anti-virus products are:

- Symantec AntiVirus 10.2
- eTrust antivirus software 8.0
- TrendMicro 7.3
- McAfee 7.0

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

- Infected file quarantine policy on the server and client: antivirus software can be configured to clean up the detected virus automatically and files must be quarantined if infected files cannot be cleaned. Contact Avaya to verify whether the quarantine file is part of our product files or dependent system file. If a virus is detected, remove the server from the network immediately during virus eradication to prevent further virus propagation.
- Do not connect a contact center application platform directly to the Internet to download virus definitions or updated files. Furthermore, Avaya recommends that you do not use a contact center application client PC to connect to the Internet. Instead, download virus definitions and updated files to another location on the customer network and manually load them from this interim location onto the contact center application platform.
- Perform the previous steps to download Contact Center application service packs (SP). This method limits access to the Internet, and thus reduces the risk of downloading infected files.
- Scan all SP files, DVD-ROMs, and floppy disks before you upload or install to the server. This practice minimizes any exposure to infected files from outside sources.
- Capacity considerations: running virus scan software can place an additional load on a contact center application platform. The implementation personnel must run the performance monitor tool on the server to gauge CPU usage. If the antivirus software scan causes the platform average CPU usage to exceed the recommended percentage for longer than 20 minutes, the antivirus software must not be loaded onto the contact center application platform.
- Product Support do not provide support on the configuration of antivirus software, but offer guidance where possible. Direct questions or problems on antivirus software to the appropriate vendor.
- If performance or functionality issues are raised to Avaya support personnel as part of the fault diagnosis, you may be asked to remove third-party utility software or antivirus software.

Operating system updates

Operating system updates includes service updates and service packs.

Service updates

Given the number of operating system security service updates and the complexity inherent in any network, Avaya recommends that you create a systematic and accountable process for identifying and applying service updates. To help create such a process, you can follow a series of best practices guidelines, as documented in the National Institute of Standards and Technology (NIST) Special Bulletin 800-40, Procedures for Handling Security Patches.

This bulletin suggests that if an organization has no central group to coordinate the storage, evaluation, and chronicling of security service updates into a library, then system administrators or the contact center administrator must fulfill this role. In addition to these guidelines, whenever possible, Avaya recommends that you follow Microsoft recommendations regarding newly discovered vulnerabilities and that you promptly install Microsoft security service updates.

Whenever possible, Avaya incorporates the most recent operating system security recommendations and service updates in an integrated solutions testing strategy during each test cycle. However, due to the urgent nature of security service updates when vulnerabilities are discovered, Avaya recommends that customers follow Microsoft guidelines as they are issued, including any Microsoft installation procedures and security service update rollback processes that may 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 update, you must remove the service update and revert to the previous version of the application (from the backup you made before applying the service update). For added security, always determine whether Avaya verified the Microsoft service update for compatibility with Contact Center Manager.

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

Service packs

Avaya has a policy to implement co-residency testing of all new operating service packs for compatibility with the suite of Contact Center applications as soon as they are available. In practice, because a service pack can contain a significant amount of new content, Avaya requires that you wait until compatibility testing is complete before you apply the service pack. Note that operating system service packs are typically tested with the most recent Contact Center application SP and, therefore, an upgrade to a new service pack necessitates an upgrade to the most recent Avaya SP.

Before you upload a new service pack, you must perform a full system backup (for system rollback as in the updating scenario).

Attention: Service pack compatibility for all Contact Center applications is documented in the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* on the Web site at www.avaya.com/support.

Java Runtime Environment updates

Contact Center only supports specific versions of Java Runtime Environment (JRE). The Contact Center Installer installs a supported JRE version, and Contact Center service packs install required JRE updates. You must disable JRE automatic updates in the Control Panel on all contact center servers.

Attention: Updating to an unsupported version of JRE can cause the contact center to stop working and can require the reinstallation of the contact center server.

.

Hardware requirements

The following sections describe the additional hardware requirements for all servers.

Redundant Array of Independent Disks

Servers with a Redundant Array of Independent Disks (RAID) (type 1) controller are strongly recommended. The (RAID) technology provides disk data redundancy and error detection and correction. Avaya strongly recommends RAID-1 for maximum flexibility in providing technical support.

Uninterruptible Power Supply

The use of an Uninterruptible Power Supply (UPS) with a server is permitted. A UPS provides the following benefits:

- Reduction in data loss—A UPS shuts down the server gracefully if an interruption in AC power occurs. A graceful shutdown prevents data corruption and reduces the risk of data loss.
- Reduction in power dips and spikes—The UPS regulates AC power supplied to the server.

Data backups running at the time of shutdown are unusable.

UPS requirements

The UPS must meet the following requirements:

- Provides at least 10 minutes of power to stop all services and shut down the server.
- Fits physically within the workplace.
- Affects environment minimally.
- Applies power to the server when line voltage reaches a stable state.
- Recharges before powering up the server if the server is down for a long time.

- Is compatible with the operating system running on the server.
- Meets all local regulatory requirements. For the European market, the UPS must generate a pure sine wave AC waveform.
- Has hot-swappable batteries. Replacement or capacity upgrades of the batteries must not interrupt service.
- Does not affect the Contact Center application software. UPS software must not replace software or drivers installed on the server with different versions. Install only the basic software functions necessary for UPS operation. Do not install advanced features as they can affect the Contact Center application software.
- If you install Smart UPS software on the server, it must conform to the guidelines in this document for third-party utilities. The UPS solution provider must perform the documentation, testing, and support of server shutdown and startup with UPS software.

Licensing considerations

The Contact Center License Manager provides central control and administration of application licensing for all of the elements of Avaya Aura™ Contact Center.

You can choose Essential licensing for a single-server, single-site, voice-only contact center with up to 100 agents.

You can choose Nodal Enterprise licensing mode for a single contact center installation or Corporate Enterprise licensing mode for a network of Contact Center installations. You can also maintain a secondary License Manager, which takes over licensing if the primary License Manager fails. Avaya Aura™ Contact Center supports upgrading from an entry-level voice-only Essential license to a full-featured multimedia Enterprise license.

You use Nodal NCC or Corporate NCC licensing when you install a Network Control Center.

This section describes the Essential, Nodal Enterprise, and Corporate Enterprise licensing modes, how to interpret your license file, where to install and configure the Contact Center License Manager for your contact center, and the licensing grace period.

Navigation

- Enterprise licensing (page 59)
- Essential licensing (page 62)
- Comparing Enterprise and Essential licensing (page 64)
- About the license file (page 65)
- Licensing grace period (page 72)
- License manager statistics (page 72)
- Media Application Server licensing (page 73)

Enterprise licensing

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 would be least affected by the real-time operation of the Contact Center License Manager.

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

- If you install Contact Center components in a networked environment with a NCC server, and you use Corporate Licensing, Avaya recommends that you 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 Contact Center 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 Contact Center License Manager on the same server.
- If you install Communication Control Toolkit in a Knowledge Worker environment, you can install the License Manager on the Communication Control Toolkit server.

The following table shows where to install Contact Center License Manager.

Contact Center License Manager server installation location

	Essential Nodal	Enterprise Nodal Standard	Enterprise Nodal Networked	Enterprise Corporate Standard	Enterprise Corporate Networked	CCT Knowledge Worker
Where to install Contact Center License Manager	CCMS Server	CCMS Server	CCMS Server	CCMS Server	NCC Server Or CCMS Server	CCT Server

Nodal Enterprise licensing

The options in the license file apply to a single installation of Contact Center Manager Server (CCMS), Contact Center Manager Administration (CCMA), Contact Center Multimedia (CCMM), and Communication Control Toolkit (CCT). When you choose Nodal Enterprise licensing, all licensing options for the applications in the Contact Center node are in a single license file managed by the License Manager.

Corporate Enterprise licensing

You can use Corporate Enterprise licensing to distribute licenses to multiple servers so they can share licenses from a single pool.

For example, assume you have two sites: Galway and Auckland. Both sites share 100 Voice Agents. The Contact Center License Manager is installed co-resident with the Galway Contact Center Manager Server. When the day

starts, all of the voice agents in Galway request licenses from the license server. One hundred licenses are issued in Galway. As Galway closes, the Auckland day starts. As the Galway agents log off, the licenses are made available for the agents in Auckland.

In this example, you require only 100 Voice Agent licenses to share across the two sites.

Each license that the Contact Center License Manager grants to the Contact Center Manager Server, Contact Center Manager Administration, Contact Center Multimedia, or Communication Control Toolkit is refreshed by the respective application. This ensures that licenses always return to the Contact Center License Manager pool if the applications fail. The refresh mechanism requires an available network connection to the Contact Center License Manager.

Managing two License Manager servers

In a Corporate Licensing environment, you can configure two Contact Center License Manager servers: a primary Contact Center License Manager and a secondary Contact Center License Manager. Only one Contact Center License Manager can be active at one time. The primary Contact Center License Manager actively maintains the licenses. The secondary Contact Center License Manager runs as a standby Contact Center License Manager to provide redundancy in a corporate environment. You can configure the secondary Contact Center License Manager as the Standby Contact Center License Manager for the Contact Center License Manager components so that it is not actively used for licenses unless the active Contact Center License Manager fails.

Configure your preferred active Contact Center License Manager as the primary license manager.

For Corporate License environments that have a Network Control Center, Avaya recommends that you install the primary License Manager software on the Network Control Center.

Install the secondary License Manager on any Contact Center Manager Server that does not contain the primary License Manager, including the NCC. You cannot install the primary and secondary License Manager software on the same server.

The following conditions apply:

- You cannot configure a Standby License Manager in a Nodal licensing environment.
- Do not use the Standby License Manager for load balancing issues.

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.

TDM-based contact centers

In a TDM-based contact center Essential licensing supports a single co-resident server with the following applications:

- Contact Center Manager Server
- Contact Center Manager Administration
- Communication Control Toolkit
- Contact Center License Manager
- Contact Center Manager Server Utility
- Service Creation Environment

When using Essential licensing engineer the server to accommodate all these Avaya Aura™ Contact Center applications co-resident on the single-server.

SIP-enabled contact centers

In a SIP-enabled contact center Essential licensing supports a single co-resident server with the following applications:

- Contact Center Manager Server
- Contact Center Manager Administration
- Communication Control Toolkit
- Contact Center License Manager
- Contact Center Multimedia
- Media Application Server
- Contact Center Manager Server Utility
- Service Creation Environment

When using Essential licensing in a SIP-enabled contact center, Contact Center Multimedia and Media Application Server must be installed co-resident with Contact Center Manager Server on the single-server. The server must be engineered to accommodate all these Avaya Aura™ Contact Center applications installed co-resident on the single-server.

Essential licensing features and interfaces

Essential licensing supports entry-level, voice-only, single-site, single-server contact centers. Essential licensing supports the following features:

- Up to 100 voice-only agents
- Single server deployment
- Single site deployment
- Skills based routing - voice only
- Integrated reporting
- Universal Queue
- Voice-only contacts
- Graphical call flows
- Integrated Music, RAN
- Default Play prompts/Collect Digits (only in a SIP-enabled contact center)
- Optional Dialog (basic IVR) ports (only in a SIP-enabled contact center)
- CCMA and CCT basic Web Services

Essential licensing does not support the following features:

- Multimedia contacts
- Networking
- Predictive Outbound
- High Availability Standby Server (Campus and Geographic)
- Report Creation wizard (RCW)
- Text based scripts
- SOA Web Services
- Agent Web Statistics

Essential licensing does not support the following interfaces:

- Host Data Exchange (HDX)
- Database Integration Wizard (DIW)
- MLS HER (Host Enhanced Routing)
- SOA Web Services (Open Queue and Open Networking)

Essential licensing does not support the following historical reports:

- Networking
- Predictive Outbound

- Call by call
- Contact Summary Reporting (CSR)
- Access & Partition Management
- Configuration - Agent skillset assignment
- Configuration - Agent Supervisor assignment

Comparing Enterprise and Essential licensing

Essential licensing supports entry-level, voice-only, single-site, single-server contact centers. Essential licensing supports a subset of the Enterprise licensed features and interfaces.

The following table compares Essential and Enterprise licensed features.

Comparison of Essential and Enterprise licensed features

Features and Interfaces	Essential	Enterprise
Voice contacts	Yes	Yes
Multimedia contacts	No	Yes
Maximum Voice Agents	<101	CS 1000 TDM: <5000 CS 1000 SIP: <1500 Avaya Aura SES SIP: <1000 Avaya Aura MBT SIP: <300
Maximum Multimedia Agents	Not supported	3000
Multi-site contact center	No	Yes
Multi-server contact center	No	Yes
High Availability Standby Server	No	Yes
Networking	No	Yes
Network Control Center	No	Yes
Predictive Outbound	No	Yes
Report Creation wizard (RCW)	No	Yes
SOA Web Services	No	Yes
Agent Web Statistics	No	Yes
Host Data Exchange (HDX)	No	Yes
Database Integration Wizard (DIW)	No	Yes
MLS HER (Host Enhanced Routing)	No	Yes
SOA Web Services (Open Queue and Open Networking)	No	Yes

Comparison of Essential and Enterprise licensed features

Features and Interfaces	Essential	Enterprise
Graphical call flows	Yes	Yes
Text-based scripts	No	Yes
Integrated reporting	Yes	Yes
Skills based routing	Voice-only	Yes
Universal Queue	Yes	Yes
Integrated Music, RAN	Yes	Yes
Default Play prompts/Collect Digits	Yes	Yes
Optional Dialog (basic IVR) ports	Yes	Yes
Unified Reporting	No	Yes
Historical reports - Call by call	No	Yes
Historical reports - Contact Summary Reporting (CSR)	No	Yes
Historical reports - Access & Partition Management	No	Yes

Avaya Aura™ Contact Center supports upgrading from an entry-level voice-only Essential license to a full-featured multimedia Enterprise license.

About the license file

The Contact Center License Manager offers flexible licensing options and supports licensing of features at the node (Nodal License) or network (Corporate License) level.

The license file provides a single point of administration for licensing and includes multiple keycodes for Contact Center Manager Server, Contact Center Manager Administration, Contact Center Multimedia, and Communication Control Toolkit. This single file reduces the number of separate keycodes that you must maintain. If you require additional features or if your requirements change, you can upload a new license file, containing the new licensing information, to the server and replace the existing licensing file.

The following table shows when the license file is generated from the Contact Center License Manager server MAC address and when it is generated from the Avaya Communication Server 1000 Serial ID. The Avaya Communication Server 1000 Serial ID is also known as the Site ID.

License file generation method

	Essential Nodal AML	Essential Nodal SIP	Enterprise Nodal AML	Enterprise Nodal SIP	Enterprise Corporate
CS 1000 Serial ID or LM server MAC address	Serial ID	MAC	Serial ID	MAC	MAC

You can find the license file in the D:\Avaya\Contact Center\License Manager\ bin folder on the server.

Attention: A corporate license file can only be generated from the server subnet Network Interface Card (NIC) MAC address. The nodal license file can be generated from either the server subnet NIC MAC address or the Avaya Communication Server 1000 serial ID.

Corporate Enterprise license file

A license key in the product name identifies the Corporate Enterprise license.

In Corporate Enterprise licensing mode you can use a secondary License Manager for redundancy. Both the primary and secondary License Managers can use the same license file.

Nodal Enterprise license file

Licensing indicates that the licenses are distributed only to that node. You cannot share nodal licenses. A license key in the product name identifies the Nodal Enterprise license.

Interpreting the license file

Contact Center licensing includes agent, and feature licensing.

Agent licenses

Agent licenses determine the number of agents that can log on to Contact Center. Agent licenses are available for both Nodal and Corporate Licensing.

Licensing is available for the following types of agents:

- voice agent
- outbound agent
- e-mail agent (covering FAX messages, SMS text messages, voice mail messages, and scanned document messages)
- Web communications agent
- Instant messaging agent

Feature licenses

The following feature licenses are available:

- Open Queue
- Universal Networking
- Progressive and Preview Outbound
- Predictive Outbound
- Report Creation Wizard (supported with SIP)
- Standby Server (High Availability) Campus and Geographic
- Call Recording enablement
- Open Interfaces Open Queue
- Open Interfaces Universal Networking
- Agent Web Statistics
- Multiplicity (Included by default with multimedia agents)

Supported License Manager servers

This section describes some of the licensed features in Contact Center. You cannot use Avaya NES License Manager Release 7.0 with Avaya Aura™ Contact Center.

Supported License Manager options

The following table shows the supported Contact Center License Manager servers.

Contact Center License Manager servers

Compatible with	NES CC 6.0 Licence	NES CC 7.0 Licence	AACC Licence
NES CC 6.0	Yes	Yes	Yes
NES CC 7.0	No	Yes	Yes
AACC 6.X	No	No	Yes

Licensed features

This section describes some of the licensed features in Contact Center. You must use License Manager for Contact Center applications. You cannot use Avaya NES License Manager Release 7.0 with Avaya Aura™ Contact Center.

Open Queue

With Open Queue, you can queue voice and multimedia contacts in Contact Center and then route the contacts to agents by using the Avaya Aura™ Agent Desktop. Configure Open Queue by using the Contact Center Manager Server Configuration utility. Open Queue is included by default with multimedia agents. Open Queue is available as an optional extra with the SOA Development Kit.

Universal Networking

Universal Networking is the networking between Avaya Communication Server 1000 systems and Avaya NES Communication Server 2x00 systems.

Universal Networking refers to the following features:

- Network Skill-based Routing between all switch types supported by Contact Center
- attached data transport during agent-initiated transfers or conferences when under the control of the Communication Control Toolkit

Configure the Universal Networking feature by using the Contact Center Manager Server Configuration utility.

Progressive and Preview Outbound

Only licensed users can access the Outbound Campaign Manager Tool using Contact Center Manager Administration.

The Outbound Campaign Manager Tool is compatible only with Contact Center Multimedia/Outbound.

For more information about the Outbound feature, see *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).

Predictive Outbound

Licensed users can use the Multimedia server and Predictive Outbound solutions software to create predictive outbound campaigns where calls are made and agents are assigned to the outgoing calls.

Report Creation Wizard

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

Report Creation Wizard is a user-based license. License Manager controls the maximum concurrent Report Creation Wizard users.

Contact Center Manager Administration includes a one-user license for the Report Creation Wizard feature. You can order additional licenses in groups of 5 up to a maximum of 25 licenses (that is, 5, 10, 15, 20, or 25 licenses).

For more information about Report Creation Wizard, see the *Avaya Aura™ Contact Center Performance Management* (NN44400-710).

Standby Server (High Availability)

The High Availability feature allows the replication of primary Contact Center servers to provide a warm backup database if the primary server is down.

Contact Center Manager Administration resiliency is performed through Active Directory Lightweight Directory Services (AD-LDS). For information about configuring resiliency on Contact Center servers, see *Avaya Aura™ Contact Center Commissioning* (NN44400-312).

Call Recording enablement

Avaya Aura™ Contact Center supports SIP-enabled call recording. Avaya Aura™ Contact Center requires a single Call Recording Super User license per Contact Center node.

License identifiers

License identifiers connect a license file to a particular server or to a particular installation, as shown in the following example of a CCT license identifier:

5Q+GUqilIwmanh1srOz89DIxMLDQzYENrmeP4Xn38LZn9paGys5aeewwClCc CiHoqLC4vL6+ # LM_CCTN 8.0 00:1d:09:71:8d:d0 Identifier (1) 60 secs

The following table lists all license identifiers within the license file and the descriptions.

Identifier	Description
cshdxls	IVR HDX Interface Devices
csrsmls	IVR RSM Interface Devices
cstapils	IVR Data Devices
LM_CCT	CCT
LM_CCT_ST	CCT Replication\Standby Server
LM_CONTACTREC	Open Interface Contact Recording
LM_ENTERPRISEC	Enterprise Corporate
LM_ENTERPRISEN	Enterprise Nodal
LM_ESSENTIAL	Essential
LM_HETERO	Nodal Open Networking license
LM_HET_ADM	NCC Open Networking license
LM_IM_PRESENCE	IM Presence (with OCS server)
LM_KW_VOD	Knowledge Worker
LM_LOC_EMA	Non-Network e-mail Agent
LM_LOC_IMA	Non-Network IM Agent
LM_LOC_OBA	Non-Network Outbound Agent
LM_LOC_OQA	Non-Network Open Queue Agent

Identifier	Description
LM_LOC_PRA	Non-Network Predictive Agent
LM_LOC_VOA	Non-Network Voice Agent
LM_LOC_WCA	Non-Network Web Communications Agent
LM_LP	Linkplexer
LM_MLSM_DN_REG	Multiple DN Registration
LM_MLSM_ROD_REG	Record On Demand
LM_MMP	CCMM Primary License
LM_MMS	CCMM Standby License
LM_MULP	Multiplicity
LM_NETWORKING	Networking License
LM_NET_EMA	Network e-mail Agent
LM_NET_IMA	Network IM Agent
LM_NET_OBA	Network Outbound Agent
LM_NET_OQA	Network Open Queue Agent
LM_NET_PRA	Network Predictive Agent
LM_NET_VOA	Network Voice Agent
LM_NET_WCA	Network Web Communications Agent
LM_OB	Outbound
LM_OI	Open Interface
LM_OIOpenN	Open Interface Open Networking
LM_OIOpenQ	Open Interface Open Queue
LM_OQ	Open Queue interface
LM_RCW_USER	RCW Users
LM_STANDBY	CCMS Replication\Standby Server
LM_VOD	Voice Devices
LM_WBSTAT	Web Statistics
tls	IVR Devices
__sip-annc	SIP Announcements
__sip-conf	SIP Conference
__sip-dialog	SIP Dialog

Avaya Communication Server 1000 server

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

You can also 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 Server cannot start.

Attention: A corporate license file can only be generated from the contact center subnet NIC MAC address. The nodal license file can be generated from either the server subnet NIC MAC address or the Avaya Communication Server 1000 serial ID.

Communication Control Toolkit 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.

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

The MAC address can be any MAC address of the NICs; however, Avaya recommends that you 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 Manager cannot start.

SIP server

The only identifier allowed for SIP installations is the MAC address of the Contact Center Manager Server running License Manager.

The MAC address can be any NIC MAC address; however, Avaya recommends that you 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 Manager 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 NIC MAC address; however, Avaya recommends that you 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 Manager cannot start.

Licensing grace period

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 during the grace period.

The grace period is 30 days. If a communication problem occurs between the Contact Center Manager Server and the Contact Center License Manager, 30 days are available for the Contact Center Manager Server to continue normal operation. After the communication problem is resolved, the grace period adds back 20 minutes every 20 minutes until the grace period is back up to 30 days. For example, if the communication problem is resolved in two days, the grace period counts backs up to 30 days after two days of successful connection to the Contact Center License Manager.

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

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

Emergency license files

If you cannot fix the connection between the Contact Center License Manager and Contact Center Manager Server within the 30-day grace period, contact your Avaya customer service representative to determine if you need to activate an emergency license file on your system.

The emergency license file expires after 30 days and is used only to ensure temporary operation of the Contact Center Manager Server.

You must install the emergency license file through the Contact Center License Manager configuration tool. If you use corporate licensing, you may need to change the Contact Center Manager Server configuration if the Contact Center License Manager is installed on a different server than it was previously.

License manager statistics

Contact Center License Manager produces historical reporting data to support the analysis and management of concurrent license usage in the network. Historical data is available in 15-minute intervals daily, weekly, or monthly. License utilization is reported on a client basis, with the IP address of the client used to denote individual clients.

The Contact Center License Manager reports the following statistics:

- Timestamp—The time the data is written to the database.
- IP Address—The IP address of the Contact Center Manager Server, Contact Center Manager Administration, Contact Center Multimedia, and Communication Control Toolkit.
- License identifier—The name of the license.
- Maximum allocation during interval—The maximum number of licenses allocated to the server during the 15-minute interval.

If an interval has 10 licenses issued for a feature, then 10 is written to the database table. If another 5 licenses are issued in the next interval, then 15 is written to the database table. However, at the end of the interval, if only 14 licenses were issued, but 15 were issued at some stage during the interval, then a value of 15 is written to the database.

The data is written to the database on the server on which you installed the License Manager for each 15-minute interval. These statistics are consolidated daily, weekly, and monthly.

The License Manager reports any errors by writing error data to the database. The data is stored on a site-by-site basis where the site identifier is the IP address of the server.

A report template is available to generate reports using this statistical information. The data is available from the following database views:

- iLicenseStat—interval statistics
- dLicenseStat—daily statistics
- wLicenseStat—weekly statistics
- mLicenseStat—monthly statistics

Real-time statistics

You can use the Real Time Usage tab in the Contact Center License Manager utility to view a snapshot of the licenses issued by the License Manager.

Media Application Server licensing

The MAS license resides on the server on which you plan to install MAS and is specific to the SIP Contact Center application that resides on the server. Install this license using the Element Manager.

MAS requires licenses for the CCSM conference, announcement, and dialog features. When installed co-resident with Contact Center Manager Server, MAS uses the Contact Center License Manager and the license server on MAS is

disabled. When not co-resident with Contact Center Manager Server, MAS uses the MAS License Server and the Contact Center Services for MAS (CCSM) licenses must be applied using the MAS Element Manager.

You can configure the following licenses for MAS:

- Advanced SIP Contact Center Service (for each port)—Voice Conversation space, observe, barge-in; Announcements, Tones, and Give RAN/MOH.
- Premium SIP Contact Center Service (for each port)—Voice Conversation space, observe, barge-in; Announcements service - Tones, Give RAN/MOH; Dialog service/Give IVR - advanced treatments including play prompts, collect digits, Web page push, canned applications like EWT/PIQ, send IM, and VXML invocation.
- SIP Video Contact Center Service (On/off)—Enables video agents and video streaming treatments.
- SIP Contact Center Services DVD—Media for installing services on the MAS.

Contact Center Manager Server configuration requirements

This section provides the configuration requirements for Contact Center Manager Server.

Prerequisites

- Engineer the Avaya Communication Server 1000 PABX so it can support Contact Center, in particular engineer PABX resources to support the required agent numbers and call volume. For more information, see Avaya *Communication Server 1000M Large System Planning and Engineering* (NN43021-220) and Avaya *Communication Server 1000E Planning and Engineering* (NN43041-220).

Navigation

- Hardware requirements (page 75)
- Operating system requirements (page 77)
- Disk partitioning requirements (page 79)
- Third-party software requirements (page 80)
- Contact Center Manager Server port requirements (page 82)

Hardware requirements

The following specifications provide guidelines regarding platform types and the level of functionality supported. These specifications are for stand-alone configurations only. For information about co-resident configurations, see Co-resident configuration requirements (page 133).

Use the Contact Center Capacity Assessment Tool (CapTool) to determine the platform size required for a contact center configuration.

Attention: The hardware specifications in this section are for general guidance only. Carefully analyze your contact center capacity requirements using the Capacity Assessment Tool before you decide the specifications for your PVI server.
You can download the CapTool software utility from the support Web site (www.avaya.com/support).

The following table lists the hardware requirements for Contact Center Manager Server (stand-alone configuration only).

The recommended minimum values support a typical configuration (Multimedia, Outbound, Universal Networking) with the following functionality enabled:

- Size: < 600 agents, < 12 000 CPH
- License Manager
- Open Queue
- Universal Networking

Contact Center Manager Server hardware requirements

Hardware item	Recommended minimum	Additional information
CPU	Quad-core Xeon 2.8 GHz or equivalent. Use the Contact Center CapTool to determine the appropriate CPU required.	Quad-CPU systems are supported with or without Hyperthreading enabled. AMD processors of the same or higher specification are also supported. Non supported processors include: Intel Celeron and Intel Itanium (IA 64).
Maximum number of physical CPUs	4	
RAM	8 GB	
Hard disk space	235 GB of logical disk space (470 GB of physical disk space with RAID-1)	RAID-1 is recommended for all disks on the shared SCSI bus to eliminate disk drives as a potential single source for hardware failures.
Hard disk partitioning See Disk partitioning requirements (page 79).		
Hard disk type	SCSI, SATA, or SAS	IDE drives not supported. At this time, a Storage Area Network (SAN) configuration is not supported.
Hard disk speed	7200 RPM	
DVD ROM	One dual-layer DVD ROM drive	Minimum speed is 4X.
Serial port	One serial port (for modem access) or USB port (if using USB modem)	Additional serial ports are required to use a serial UPS. You must use COM2 for the Access Link.

(1 of 2)

Contact Center Manager Server hardware requirements

Hardware item	Recommended minimum	Additional information
Network interface	One network interface card (Network Control Center only requires one network interface card)	ELAN subnet must be 10/100 Mb/s Ethernet. The server subnet facing network interface card can be 100 Mb/s Ethernet and higher. Only Ethernet supported.
Note : All hardware devices must be on the Microsoft Hardware Compatibility List for Windows Server 2008. For a complete list of compatible hardware devices, see the Microsoft Web site (www.microsoft.com).		
(2 of 2)		

CPU use

For optimal performance, average CPU use must not exceed 70 percent over a 15 minute interval.

RAID controller

For RAID requirements, see Redundant Array of Independent Disks (page 56).

Additional requirements for Contact Center Manager Server

You can implement RAID-5 with Contact Center Manager Server; however, Avaya strongly recommends RAID-1 because it provides maintenance personnel with extra flexibility in providing technical support. Other RAID levels are not supported. The RAID Vendor must address any RAID-specific issues.

Uninterruptible Power Supply

For Uninterruptible Power Supply (UPS) requirements, see Uninterruptible Power Supply (page 56).

Operating system requirements

The following table provides the operating system compatibility for Contact Center Manager Server.

Contact Center Manager Server operating system requirements

Operating system	International versions supported	Minimum service pack required
Windows Server 2008 Release 2, Standard Edition and Enterprise Edition, 64-bit See Note 1.	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	
Note 1: Only the 64-bit version is supported.		

Operating system installation and configuration

Contact Center Manager Server runs on the Windows components installed by default in Windows Server 2008 with the following exceptions:

Attention: These exceptions apply to a stand-alone server only.

- The Simple Network Management Protocol (SNMP) service must be installed on your server. Installation enables you to use an SNMP management system for remote monitoring. This service is not installed by default, so you must select it when you install or configure the operating system.
- When Contact Center Manager Server is used in an Avaya Communication Server 1000 environment, you must disable all time synchronization features of the operating system to avoid potential call processing outages.

Do not install additional services on your server that are not installed by default or described in this document.

See the Avaya Contact Center Security Guide, available on the Web site (www.avaya.com/support), for detailed guidelines about operating system configuration.

Microsoft security hotfixes

You must operate your server with the most current Microsoft patches.

- Review the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* (available from Technical Support Web site) for the list of applicable Microsoft security hotfixes to apply.

- Back up the entire server, and then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Disk partitioning requirements

The following table provides detailed information about partitioning a server hard disk drive to meet the requirements of Contact Center Manager Server.

Attention: This table provides requirements for a stand-alone Contact Center Manager Server only. For information about disk partitioning requirements for a co-resident server, see Co-resident configuration requirements (page 133).

If the space in your dynamic database drive is full, you can expand the database drive.

To avoid database expansions, Avaya recommends that you have at least 500GB on your disk. For more information about expanding the dynamic disk, see *Avaya Aura™ Contact Center Installation* (NN44400-311).

Contact Center Manager Server disk partitioning requirements

Drive letter	Recommended size	Notes
C	60 GB	NTFS partition on disk 0. This drive must be partitioned as the Primary partition. The Windows 2008 operating system is installed here
D (application partition)	25 GB	Additional NTFS partition on disk 0 or an NTFS partition on a different disk. This drive must be partitioned as a logical drive within an extended partition because this partition is not used for startup. Contact Center Manager Server is installed here.
E	N/A	DVD drive
Database partition (usually F)	120 GB	This drive is used to store the database.
Trace logs partition	30 GB	—
Total disk size	235 GB	—

- Partitioned sizes on all database drives must be in increments of 1 GB (equivalent to 1024 MB).

- You must partition the Drive C as a primary partition. All other drives can be partitioned as logical drives.
- One partition is dedicated to the database. .
- You can locate the C drive, D drive, and database partitions on the same hard disk, if required, as long a sufficient disk space is available. However, you may want to keep the database and the Contact Center Manager Server application on different hard disks as you can upgrade each component separately.
- Avaya does not guarantee the support for future Windows 2008 Server Service Packs, which may require more disk space.

See *Avaya Aura™ Contact Center Installation* (NN44400-311) for additional information regarding disk partitioning.

Note the following for precise size definitions:

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

Third-party software requirements

This section describes the third-party software requirements for Contact Center Manager Server.

Third-party backup software

Two types of backups are available on Contact Center Manager Server:

- Full (offline) backup
- Database (online) backup

Use third-party backup software only for full (offline) backups. To create a full backup, you must use a third-party backup utility such as Microsoft backup utility. See the third-party documentation for information about the full backup procedure, and *Avaya Aura™ Contact Center Server Administration* (NN44400-610) for information about procedures that you must perform before a full backup. If you use a third-party backup utility, it must comply with the general third-party software guidelines specified in Third-party software requirements (page 52).

You must shut down all Contact Center Manager Server services before you perform a full backup. Even though some third-party backup utilities can provide an online backup of all files, Contact Center Manager Server does not support an online backup from these third-party backup utilities.

Avaya recommends that you back up your database daily.

Antivirus software

Several maintenance tasks are automatically activated on Contact Center Manager Server at 12:00 midnight. Therefore, you must schedule virus scans at a time other than midnight.

For Contact Center Manager Server, Avaya recommends that you exclude the following files and folders from scans (both real-time and scheduled):

- F:\Avaya\Contact Center\Database\
- <additional database drive>:\Avaya\Database\
- TSM_OAM log folder location
- D:\Avaya\Contact Center\Manager Server\iccm\bin\data
- D:\Avaya\Contact Center\Manager server\iccm\data
- D:\Avaya\Contact Center\Manager Server\iccm\sdm\log
- OAMContainer*.log located at D:\Avaya\Contact Center\CMF
- D:\Avaya\Contact Center\Manager Server\bin\tools2.exe—File access errors occur in the Scan Activity log if you do not exclude this file from scanning.
- D:\Avaya\Contact Center\Manager Server\iccm\logs (SIP logs)
- D:\Avaya\Contact Center\Manager Server\iccm\sgm\config\ (SIP log configuration files)
- D:\Avaya\Core\CMF\(current version of CMF)

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in <Install_Directory>:\Avaya\Cache\CacheSys. Databases and journal files are installed in <Install_Directory>:\Avaya\Contact Center\Databases.

Simple Network Management Protocol (SNMP) alerting on virus confirmation

Avaya recommends that you do not activate this feature.

Remote support access tool

Avaya requires you to configure a remote support access tool on the server to provide remote support. You can use LogMeIn Rescue from LogMeIn (www.logmein.com). LogMeIn Rescue supports remote systems over the Web without installing software.

You can use the Remote Desktop Connection feature in Windows as an alternative for remote support access tool instead of LogMeIn Rescue. Remote Desktop Connection is supported in console or admin mode only. Refer to the Microsoft Web site for details about how to verify that you are connected to the console/admin session (session 0).

Contact Center Manager Server port requirements

Contact Center Manager Server uses ports for communication between its own components. Most ports do not have implications for external network components like firewalls; however some ports may be used externally and therefore can affect an external firewall. In particular, port 10000 is a hard-coded port used to enable interoperability between Contact Center applications and external third-party applications (applications developed using the Real-Time Data (RTD) API).

No third-party application installed on Contact Center Manager Server can use the ports listed in the following table as it can cause the Contact Center Manager Server application to malfunction.

The following table shows the ports that Contact Center Manager Server uses.

Contact Center Manager Server port usage

Contact Center Manager Server port number	Functionality
1550	HDX CAPI
1972	Caché database, and Caché shadowing
4422	HDX NameService
12668–12670	TraceControl
10000	Hardcoded Toolkit Name Service
10001–10082	Networking
For example:	
10038	NCP_CHANNEL—This channel is used to communicate between the NCP of one node to the NCP of another node. The NCP on one node sends sanity messages to the other node through this port.
10039	ASM_CHANNEL—Different modules like NCP and TFE send messages to ASM through this channel.
10040	NCP_ASM_CHANNEL—ASM uses this channel to send messages to NCP.

(1 of 2)

Contact Center Manager Server port usage

Contact Center Manager Server port number	Functionality
10060	ASM_Service—The ASM service runs on this port. The Service Control Manager can send messages such as START, STOP, and RESTART to the ASM service through this port.
10062	NCP_Service—The NCP service runs on this port. The Service Control Manager can send messages such as START, STOP, and RESTART to NCP on this port.
3998	License Manager destination port—This is the first of 10 consecutive ports required for license management.
3999–4007	License Manager client source port
3389	Remote Desktop Connection for support.
5060	SIP Proxy
9080–9083	Web Services Open Interfaces
9086	CC Web Statistics

(2 of 2)

Contact Center Manager Administration configuration requirements

This section provides the configuration requirements for the Contact Center Manager Administration server and Contact Center Manager Administration clients.

Navigation

Server hardware requirements

This section describes hardware requirements for the Contact Center Manager Administration server.

The following table lists the hardware requirements for a stand-alone Contact Center Manager Administration server.

Attention: The hardware specifications in this section are for general guidance only.
Carefully analyze your contact center capacity requirements using the Capacity Assessment Tool (CapTool) before you decide the specifications for your Platform Vendor Independence (PVI) server.
You can download the CapTool software utility from the support Web site (www.avaya.com/support).

These specifications are for stand-alone configurations only. For co-resident configurations, see Co-resident configuration requirements (page 133).

Security Framework can co-reside with Contact Center Manager Administration under the recommended specification.

Contact Center Manager Administration hardware requirements

Hardware item	Recommended minimum	Additional information
CPU	Quad-core Xeon 2.8 GHz or equivalent. Use the Contact Center CapTool to determine the appropriate CPU required.	Quad-CPU systems are supported with or without Hyperthreading enabled. AMD processors of the same or higher specification are also supported. Unsupported processors include Intel Celeron, and Intel Itanium (IA 64) processors.
Maximum number of physical CPUs	4	
RAM	8 GB	
Hard disk space	60 GB of logical disk space (120 GB of physical disk space with RAID-1)	Disk space is required for historical reports saved to disk.
Hard disk partitioning	No specific partitioning requirements	
Hard disk type	SCSI, SATA, or SAS	At this time, a Storage Area Network (SAN) configuration is not supported.
Hard disk speed	> 7200 RPM	
DVD ROM	One dual layer DVD ROM drive	
Network interface	One network interface card	
Note: All hardware devices must be on the Microsoft Hardware Compatibility List for Windows Server 2008. For a complete list of compatible hardware devices, see the Microsoft Web site (www.microsoft.com).		

CPU use

For optimal performance, average CPU use on both the Contact Center Manager Administration server and the client must not exceed 70 percent over a 15 minute interval.

RAID controller

For RAID requirements, see Redundant Array of Independent Disks (page 56).

Uninterruptible Power Supply

For Uninterruptible Power Supply (UPS) requirements, see Uninterruptible Power Supply (page 56).

Server operating system requirements

This section describes the operating system requirements for the Contact Center Manager Administration server.

The Contact Center Manager Administration application server supports Windows Server 2008 Release 2 Standard and Enterprise Edition 64 bit with Internet Information Services (IIS). The Windows Server 2008 must be running Active Directory Lightweight Directory Service (AD LDS). The CCMA application server with AD LDS is not supported as a domain controller. Running both Active Directory and Active Directory Lightweight Directory Service on the application server is not supported.

The following table lists the operating system requirements for Contact Center Manager Administration server.

Contact Center Manager Administration operating system requirements

Operating system	International versions supported	Minimum service pack
Windows Server 2008 Release 2, Standard Edition and Enterprise 64-bit See Note 1	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	
Note 1: Only the 64-bit version is supported.		

Application server operating system installation and configuration

Contact Center Manager Administration runs on the Windows components installed by default in Windows Server 2008, with the following exceptions:

- Microsoft Windows Server 2008 with Internet Information Services (IIS).
- Simple Network Management Protocol (SNMP).
- Active Directory Lightweight Directory Service (AD-LDS).
- CCMA does not flag event log alarms as SNMP traps. However, you can configure the server to send SNMP traps at an operating system level. The SNMP service is not installed by default, so if it is required, select it when you install or configure the operating system.

Recommended for diagnostics

Avaya recommends the following programs for diagnostics:

- Microsoft Internet Explorer 7.0 or later

Microsoft security hotfixes

You must operate your server with the most current Microsoft patches.

- Review the Avaya Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List (available from Technical Support Web site) for the list of applicable Microsoft security hotfixes to apply.
- Backup the entire server, then shut down all Contact Center services before you apply Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Disk partitioning requirements

No specific guidelines or restrictions exist regarding the number or size of the disk partitions for Contact Center Manager Administration server. Each Contact Center must decide upon its own capacity requirements depending on how the software components are installed.

For example, you can have separate disk partitions for the operating system, the application software, and the shared folders required for exporting historical reports, or you can install and configure everything on the same disk partition.

Avaya recommends that you install the operating system and Contact Center Manager Administration on an NT File System (NTFS) partition because File Allocation Table (FAT) partitions do not support security.

Client hardware requirements

The following table lists the hardware requirements for Contact Center Manager Administration client.

This specification applies to the Supervisor Client PC but can also apply to computers that run Agent Desktop Displays.

Contact Center Manager Administration client hardware requirements

Hardware item	Recommended minimum	Additional information
CPU	Intel-based CPU - Pentium IV 1.8GHz	Dual- and quad-CPU systems are supported with or without Hyperthreading enabled. AMD processors of the same or higher specification are also supported. Unsupported processors include Intel Celeron, and Intel Itanium (IA64) processors.
RAM	1 GB	
Hard disk space	60 GB	60 GB is recommended only to store large reports.
Hard disk partitioning	No specific partitioning requirements	—
Hard disk type	IDE/SCSI Bus for hard drives	—
Hard disk speed	> 7200 RPM	—
DVD ROM	One dual-layer DVD ROM drive	—
Network interface	One network interface card	—
Video card	One video card and monitor	1024*768 pixels minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—
Serial ports	One serial port (if connection of the CS 1000 Data Extraction Tool to the Communication Server 1000 switch must use a serial port)	—

Client operating system requirements

The following table lists the operating system requirements for Contact Center Manager Administration client PCs.

Contact Center Manager Administration client operating system requirements

Operating system	International versions supported (See Note)	Minimum service pack
Windows XP Professional	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	Service Pack 2 or later
Windows Vista Business 32-bit Windows Vista Enterprise 32-bit	English	SP1 or later
Windows 7 (32-bit and 64-bit)	English	
Windows Server 2008 Release 2 Standard Edition and Enterprise Editions 64-bit	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	
Note: The client operating system must be of the same language family as the Contact Center Manager Administration server.		

Client operating system installation and configuration

The following components are required on the Contact Center Manager Administration client PC:

- Microsoft Internet Explorer 7.0 or later
- Microsoft Excel 2000 Service Release 1a or later (for configuration tool only)

Third-party software requirements

This section describes the third-party software requirements for the Contact Center Manager Administration (CCMA) server.

Antivirus software

For antivirus software requirements, see Additional guidelines for the use of anti-virus software (page 53).

Remote support access tool

You must configure a remote support access tool on the server to provide Contact Center Manager Administration remote support. You can use LogMeIn Rescue from LogMeIn (www.logmein.com). LogMeIn Rescue supports remote systems over the Web without installing software.

You can use the Remote Desktop Connection feature in Windows as an alternative for remote support access tool instead of LogMeIn Rescue. Remote Desktop Connection is supported in console or admin mode only. Refer to the Microsoft Web site for details about how to verify that you are connected to the console/admin session (session 0).

Sybase Open Client v 12.5

Avaya requires that you install Sybase Open Client v 12.5 before you install the Contact Center Manager Administration server software, if the CCMA server is managing an Avaya NES CCMS Release 6.0 server. Sybase Open Client is required for the Historical Reporting and Contact Center Manager components and is included on the Contact Center DVD.

Contact Center Manager Administration port requirements

The following table shows the ports that Contact Center Manager Administration uses.

Contact Center Manager Administration port usage

Contact Center Manager Administration port number	Functionality
TCP 80	For Internet Explorer communication
TCP 443	For secure HTTP communication (only applicable if SSL is enabled for secure Internet Information Services (IIS) communication).
	(1 of 3)

Contact Center Manager Administration port usage

Contact Center Manager Administration port number	Functionality
TCP Ports 389 and 636	For Active Directory Lightweight Directory Services (AD-LDS) functionality. Port 389 is for LDAP, and port 636 is for SSL. When you install CCMA on a server that runs Window Server 2008, these ports usually appear by default in the Port Configuration for AD-LDS installation window. If the values 50 000 and 50 001 appear instead, port numbers 389 and 636 are already taken. In this case, you can either accept the new values, or choose other ports for security reasons. These ports are also used for AD-LDS replication in High Availability solutions
TCP Port 3389	For remote desktop connection.
TCP Port 25 (SMTP)	For the Historical Reporting component to send e-mail notifications when reports are printed and saved.
3899, 6366	For AD-LDS when CCMA is co-resident with the security framework or MAS. These ports are also used for AD-LDS replication in High Availability solutions.
TCP Port 8200	For the Emergency Help component on the client PC.
UDP ports 6020, 6030, 6040, 6050, 6060, 6070, 6080, 6090, 6100, 6110, 6120, 6130	For the CCMA server to receive IP multicasting data from CCMA Server (needed for Real-Time Reporting and Agent Desktop Display).
UDP ports 7 020, 7030, 7040, 7050, 7060, 7070, 7080, 7090, 7100, 7110, 7120, 7130	For the CCMA server to send IP multicasting data to client PCs (needed for Real-Time Reporting and Agent Desktop Display).
UDP ports 7025, 7035, 7045, 7055, 7065, 7075, 7085, 7095, 7105, 7115, 7125, 7135	For the CCMA server to send IP unicast data to client PCs. This is an optional method of sending the data required for Real-Time Reporting. If you do not use the multicast method, then you must configure the unicast option. You can also use a combination of the two methods.
	(2 of 3)

Contact Center Manager Administration port usage

Contact Center Manager Administration port number	Functionality
TCP Port 10000	Used by the Nameservice process on the CCMA server (nbnmsrvc.exe). It permits communication between the CCMA server and the server in Contact Center Manager Server. **Attention:** The default port for the third-party software. This conflicts with the default port used by the CCMA Toolkit NameService. To avoid issues with CCMA functionality when using Veritas Backup Exec, you must change the default port of Veritas Backup Exec to another port number that is not being used by the network.
Default UDP port 3998	License Manager destination port
Default UDP ports 3999 - 4007	License Manager destination source port
	(3 of 3)

Contact Center Multimedia configuration requirements

This section describes the requirements for Contact Center Multimedia (CCMM). CCMM makes outbound, e-mail, and Web communications available in your contact center.

Navigation

Contact Center Multimedia overview

Contact Center Multimedia delivers Outbound, e-mail, and Web communication to the contact center.

Outbound campaigns are created through the Outbound Campaign Management Tool, which is accessed though Contact Center Manager Administration. An outbound campaign is loaded on the Contact Center Manager database where it routes contacts to skillsets for queueing to specific agents based on priority.

Contact Center Multimedia server provides an e-mail manager that monitors specific e-mail boxes. Contact Center Multimedia server provides Web services for integrating your Web site with the contact center. The Web services features text chat and scheduled callback (known as click-to-call).

Checklist

When you plan a contact center, the tasks you perform depend upon the components you plan to use.

For base systems and outbound, e-mail, and Web communications, see the *Avaya Aura™ Contact Center Installation Checklist* (NN44400-310).

Server hardware requirements

This section describes the hardware requirements for the Contact Center Multimedia server.

Contact Center Multimedia server is the server platform for Outbound, e-mail, and Web communications media types. This server is deployed in addition to the Contact Center Manager Server, Contact Center Manager Administration, and Communication Control Toolkit requirements.

Attention: The hardware specifications described in this section are for general guidance only.
Carefully analyze your contact center capacity requirements using the Capacity Assessment Tool (CapTool) before you decide the specifications for your PVI server.
You can download the CapTool software utility from the support Web site (www.avaya.com/support).

The following table lists the hardware requirements for the Contact Center Multimedia server.

Contact Center Multimedia hardware requirements

Hardware item	Recommended minimum	Additional information
CPU	Quad-core Xeon 2.8 GHz or equivalent. Use the Contact Center CapTool to determine the appropriate CPU required.	AMD processors of the same or higher specification are also supported. Unsupported processors include: Pentium IV, Intel Celeron, and Intel Itanium (IA 64) processors.
RAM	8 GB	
Hard disk space	440 GB of logical disk space (880 GB of physical disk space with RAID-1)	RAID-1 is recommended for all disks on the shared SCSI bus to eliminate disk drives as a potential single source for hardware failures. Partition drives according to the requirements in this document.

(1 of 2)

Contact Center Multimedia hardware requirements

Hardware item	Recommended minimum	Additional information
Hard disk drives	Two separate physical drives: one for the operating system, Contact Center Multimedia application, database software, and attachments, and the second physical drive for the database partition.	Separate physical disks provide reliable and easy recovery in case of disk failure. A RAID-1 implementation covers this requirement.
Hard disk partitioning		
Hard disk type	SCSI, SATA, or SAS	
Hard disk speed	> 7200 RPM	
DVD ROM	Dual layer DVD ROM drive	Recommended drive letter is E. Minimum speed is 4x.
Serial ports		Additional serial ports are required to use a serial UPS.
Network interface	One network interface card	The contact center subnet-facing network interface card must be 100 Mb/s Ethernet or higher. The Contact Center Multimedia server MUST be on the same server subnet as the Contact Center Manager Server.
Note: All hardware devices must be on the Microsoft Hardware Compatibility List for Windows Server 2008. For a complete list of compatible hardware devices, see the Microsoft Web site (www.microsoft.com).		
(2 of 2)		

CPU use

For optimal performance, average CPU use on the Contact Center Multimedia server must not exceed 50 percent over a 20 minute interval.

RAID controller

For RAID requirements, see Redundant Array of Independent Disks (page 56).

Uninterruptible Power Supply

For Uninterruptible Power Supply (UPS) requirements, see Uninterruptible Power Supply (page 56).

E-mail message memory requirements

The maximum attachment size formulas use the following variables and the approximate values, to calculate how much memory to reserve to process an e-mail message.

Variable	Description	Value
Encoding adjustment	The factor by which the attachment size increases when the attachment is encoded and attached to an e-mail message.	1.3 (this can vary slightly based on the encoding used)
Memory adjustment	The factor by which the encoded size increases when an e-mail message is loaded into the internal representation of the e-mail message in memory.	1.2 (this factor decreases slightly, the larger the e-mail is, but it remains as a fixed value)
Buffer memory	The memory, which is fairly static, required by the parts of the application not involved in processing inbound e-mail messages.	20 MB

When the following sections specify an attachment size, they mean the total size of all attachments of an e-mail message. Also, the size of the body of an e-mail lowers the supported attachment size by the size of the content of the message. In most cases, the content of an e-mail is negligible compared to large attachments.

JVM size – Buffer memory / Memory adjustment / Encoding adjustment = Maximum attachment size

JVM sizes (MB)	Maximum attachment sizes (MB)
128	69.2
256 (default)	151.3
512	315.4
1024	643.6

Minimum JVM size formula

Attachment size * Encoding adjustment * Memory adjustment + Buffer memory = Minimum JVM size

Attachment sizes (MB)	Minimum JVM sizes (MB)
10	35.6
20	51.2
30	66.8
40	82.4
50	98
60	113.6
70	129.2
80	144.8
90	160.4
100	176
500	800

Server operating system requirements

This section describes operating system requirements for the Contact Center Multimedia server.

Contact Center Multimedia software runs Microsoft Windows Server 2008 Release 2 64-bit Software Standard Edition or Enterprise Edition. Other versions of Windows Server 2008 are not supported.

You must install the Windows Server 2008 Language Pack to read some e-mail attachments.

The following table lists the operating system requirements for the Contact Center Multimedia server.

Contact Center Multimedia server operating system requirements

Operating system	International versions supported	Minimum service pack
Windows Server 2008 Release 2, Standard Edition and Enterprise Edition, 64-bit	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	

Microsoft security hotfixes

You must ensure that you operate your server with the most current Microsoft patches.

- Review the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* (available from Technical Support Web site) for the list of applicable Microsoft security hotfixes to apply.
- Back up the entire server, and then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Disk partitioning requirements

This section describes partitioning for the Contact Center Multimedia server hard disk drive.

The operating system resides on the C partition. If only one physical disk exists on the server you install, all other partitions (for example, D, F, and G) must be Logical drives within an extended partition. This requirement also applies where a RAID configuration presents one disk to the operating system. See the documentation provided with the operating system for details.

Primary and extended partitions

The following table lists the recommended Contact Center Multimedia server partitions.

Contact Center Multimedia disk partitioning requirements

Drive letter	Recommended size	Notes
Operating system partition (usually C)	60 GB	NTFS partition on disk 0. This must be partitioned as the Primary partition. Windows 2008 Server is installed here.
Application partition (usually D)	80 GB	An additional NTFS partition on disk 0 or an NTFS partition on a different disk. This partition stores the attachment folders. When the NTFS partition is created on disk 0, the disk must be partitioned as the first logical drive in an extended partition. The Contact Center Multimedia software (plus required third-party software such as Caché and Java Runtime Environment) is installed on this partition.
DVD ROM drive (usually E)	N/A	DVD ROM
Database partition (usually F)	300 GB	Database and attachments partition. Additional NTFS partition on disk 0 or an NTFS partition on a different disk. When the NTFS partition is created on disk 0, the disk must be partitioned as the second logical drive in an extended partition. The Contact Center Multimedia and Outbound database is installed here.
Total disk size	440 GB	—

Do not create the attachment folder on the C partition. When the attachment folder is full, the folder size affects the total operation of the entire system.

The minimum total system disk space for the database is 300 GB. This is critical for the database partition.

Calculating disk storage requirements

This section lists the database files used by Contact Center Multimedia and provides database capacity calculations.

Required database files

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

- CACHE.DAT in the Avaya\Contact Center\Databases\CCMM\MULTIMEDIA folder. This stores the two CACHE.DAT Contact Center Multimedia folders and files, one for code and one for data.

- Avaya\Contact Center\Databases\Journals folder is created during installation. This folder contains the Database Journal Files used for Geographic Redundancy.
- Avaya\Contact Center\Databases\ShadowJournals folder is created during installation. This folder is used if Geographic Redundancy is configured and this server is running as the Redundant server.

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

The CACHE.DAT file grows dynamically as the volume of data in the database grows. Initially it is just under 45 MB. One million contacts take approximately 20GB of space.

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

E-mail attachment storage

E-mail attachments are stored in the attachment folder. The disk space required to store attachments is calculated as

```
Disk space for e-mail attachments in MB
   = number of e-mail messages per day
   * percent with attachment
   * average attachment size in MB
   * number of days before purging
```

Example

Following is the disk storage calculation for a contact center that receives 9000 e-mail messages every day, where 30 percent of the e-mail messages have an attachment averaging 0.5 MB in size, and attachments are stored for 10 days before they are deleted.

```
Disk space for e-mail attachments in MB
   = 9 000 * 0.3 * 0.5 * 10
   = 13500 MB
```

Client hardware requirements

Agent Desktop and Outbound Campaign Management Tool are clients for the Agent Desktop server.

Agents use the Agent Desktop to handle contacts—inbound and outbound voice, e-mail, and Web communications interactions are handled through this client.

Supervisors or administrators access the Outbound Campaign Management Tool through the Contact Center Manager Administration Web browser to create outbound campaigns and load them into the Contact Center Multimedia server to run them.

Agent Desktop and Outbound Campaign Management Tool require TCP/IP network access back to the Contact Center Multimedia, Contact Center Manager Administration, and Communication Control Toolkit servers— Avaya recommends 100 Mb/s connectivity. For specific network traffic between Agent Desktop and Contact Center Multimedia server and Outbound Campaign Management Tool and Contact Center Multimedia server, see *Avaya Aura™ Contact Center Installation* (NN44400-311).

The following table lists the hardware requirements for Agent Desktop and Outbound Campaign Management Tool.

Contact Center Multimedia client hardware requirements

Hardware item	Recommended configuration	Additional information
CPU	Intel-based CPU - Pentium III 733 MHz	Pentium IV, Intel Xeon (32- and 64-bit), Dual core Xeon and Intel Xeon DP are supported. Dual- and quad-CPU systems are supported with or without Hyperthreading enabled. AMD processors of the same or higher specification are also supported. Unsupported processors include Intel Celeron, and Intel Itanium (IA 64) processors.
RAM	1 GB	2 GB minimum is required, if you run other memory intensive applications at the same time as Avaya Aura™ Agent Desktop (AAAD).
Hard disk space	> 4 GB	—
Hard disk partitioning	No specific partitioning requirements	—
Hard disk type	IDE/SCSI Bus for hard drives	—
Hard disk speed	> 7200 RPM	—
Floppy drive	Not required	If a floppy drive is installed, it must be A.
DVD ROM	Not required	

(1 of 2)

Contact Center Multimedia client hardware requirements

Hardware item	Recommended configuration	Additional information
Network interface	One network interface card	100 Mb/s Ethernet or higher is recommended.
Network bandwidth	Recommended bandwidth is at least 1581Kbits/s The delay or Round Trip Time (RTT) between the client and the CCT or CCMM server must be less than 50ms.	
Video card	Video card and monitor	1024 x 768 pixels minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—
Serial ports	Not required	—
(2 of 2)		

Client operating system requirements

The following table lists the operating system requirements for the Contact Center Multimedia client PCs.

Contact Center Multimedia client operating system requirements

Operating system	International versions supported (See Note 1)	Minimum service pack
Windows XP Professional	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	Service Pack 2 or later
Windows Vista Business	English	Service Pack 1 or later
Windows Vista Enterprise	English	Service Pack 1or later
(1 of 2)		

Contact Center Multimedia client operating system requirements

Operating system	International versions supported (See Note 1)	Minimum service pack
Windows 7 (32-bit and 64-bit)	English	—
Note: The client operating system must be of the same language family as the Contact Center Multimedia server.		
(2 of 2)		

Client Citrix support

Avaya Aura™ Agent Desktop (AAAD) is supported as a Citrix published application.

On the Contact Center Multimedia (CCMM) server the AAAD folder is typically located in:

D:\Avaya\Contact Center\Multimedia Server\Agent Desktop\client folder.

This folder contains the entire AAAD application so copying it onto any client computer and clicking CCAD.exe will run AAAD. Copy this Avaya Aura™ Agent Desktop folder on the CCMM server to the Citrix server. Then configure your Citrix server to publish AAAD as a published application, accessed from this AAAD folder on the Citrix server. On the Citrix server select the users (agents) allowed to execute the AAAD published application. For more information about Citrix application publishing, see your Citrix documentation.

Third-party software requirements

This section describes the third-party software requirements for the Contact Center Multimedia server and client PCs.

Third-party backup software

If you plan to back up your Contact Center Multimedia across the network, be aware that disk capacity affects the speed of the backup and restore. To reduce the speed of a database back up or restore, follow disk capacity requirements on the remote locations.

Remote computer requirements

The remote computer for your database backup can be a server or a workstation that meets the following requirements:

- The operating system must be Windows 2008 Release 2 64-bit (Standard or Enterprise Edition).
- The drive partition for the remote directory must be NTFS.

- The directory you use for the backup requires sufficient space to hold the backup files.
- The remote computer must be on the same network as the Contact Center Multimedia server.
- The network connection must be through the contact center subnet. Ensure that the contact center subnet has low traffic during the scheduled time for the database backup. If you run the backup when contact center subnet traffic is high, the database backup can take longer than planned.

Antivirus software

Contact Center Multimedia interacts with an external e-mail system and enables agents to send attachment files from their computers to the Contact Center Multimedia server. Both methods of retrieving data are potential sources of software infection.

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the e-mail server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Contact Center Multimedia server do not have a virus. Contact Center Multimedia does not block specific attachment file types. Third-party antivirus software must be installed on the Portal Server according to guidelines in this document for such utilities.
- Exclude the Contact Center Multimedia partition from being scanned.
- If firewalls on individual computers are enabled on the Agent Desktop computer, the Report Listener may be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.
- You must not enable the Microsoft Updater to Auto-Run. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

WARNING:

WARNING

Running a Virus Scan on the Contact Center Multimedia attachment folder, which contains thousands of files, can use significant CPU time on a server and can cause drastic slowdown in agent's response times. Avaya recommends that you run scans, if necessary, during off-peak hours.

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed under <Install_Directory>:\Avaya\Cache\CacheSys. Databases and journal files are installed under <Install_Directory>:\Avaya\Contact Center\Databases.

Remote support access tool

You must configure a remote support access tool on the server to provide remote support. You can use LogMeIn Rescue from LogMeIn (www.logmein.com). LogMeIn Rescue supports remote systems over the Web without installing software.

You can use the Remote Desktop Connection feature in Windows as an alternative for remote support access tool instead of LogMeIn Rescue. Remote Desktop Connection is supported in console or admin mode only. Refer to the Microsoft Web site for details about how to verify that you are connected to the console/admin session (session 0).

Client third-party software requirements

Agent Desktop and Outbound Campaign Management Tool use the .NET Framework v3.5. After you install .NET Framework and service updates, further client deployments are through Microsoft Internet Explorer URL or SMS deployment.

Both Contact Center Multimedia (CMM) server and the Agent Desktop toolbar require Internet Information Services (IIS). Install IIS before installing the CCMM server or the Agent Desktop toolbar.

Contact Center Multimedia ports

The following table lists the configurable Multimedia ports.

Contact Center Multimedia ports

Port	Host	Client	Network interface	Functionality
1972	Contact Center Multimedia	Contact Center Manager Administration Server	Contact Center Multimedia Cache database	Port opened on database for reporting. Caché database, and Caché shadowing in High Availability solutions.
110	E-mail server	E-mail Manager	E-mail server POP3	Receiving e-mail
995	E-mail server	E-mail Manager	POP3 over SSL (optional)	Receiving secure e-mail (optional)
25	E-mail server	E-mail Manager	SMTP	Sending e-mail

(1 of 2)

Contact Center Multimedia ports

Port	Host	Client	Network interface	Functionality
80	Contact Center Multimedia Server	Any Web services client (Agent Desktop, OCMT, and third-party Web services	SOAP protocol	Accessing http Web services
29373	Communication Control Toolkit Server	Agent Desktop	Communication Control Toolkit	Remote access from clients to Communication Control Toolkit server (for Agent Desktop application)
(2 of 2)				

Networking requirements

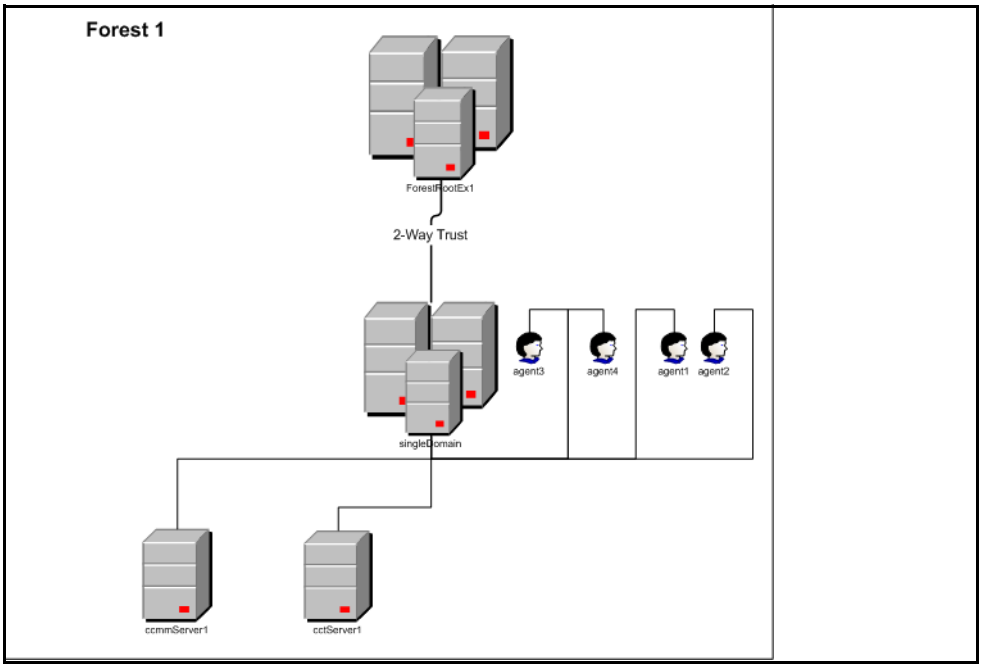
Before you install Contact Center Multimedia, your network administrator must configure your Microsoft Windows network.

Simplest configuration

In the simplest configuration, the network administrator adds your Contact Center Multimedia and Communication Control Toolkit servers to the domain forest of the Agent Desktop.

The following figure shows a single domain configuration.

Single domain example



Multiple domain configuration

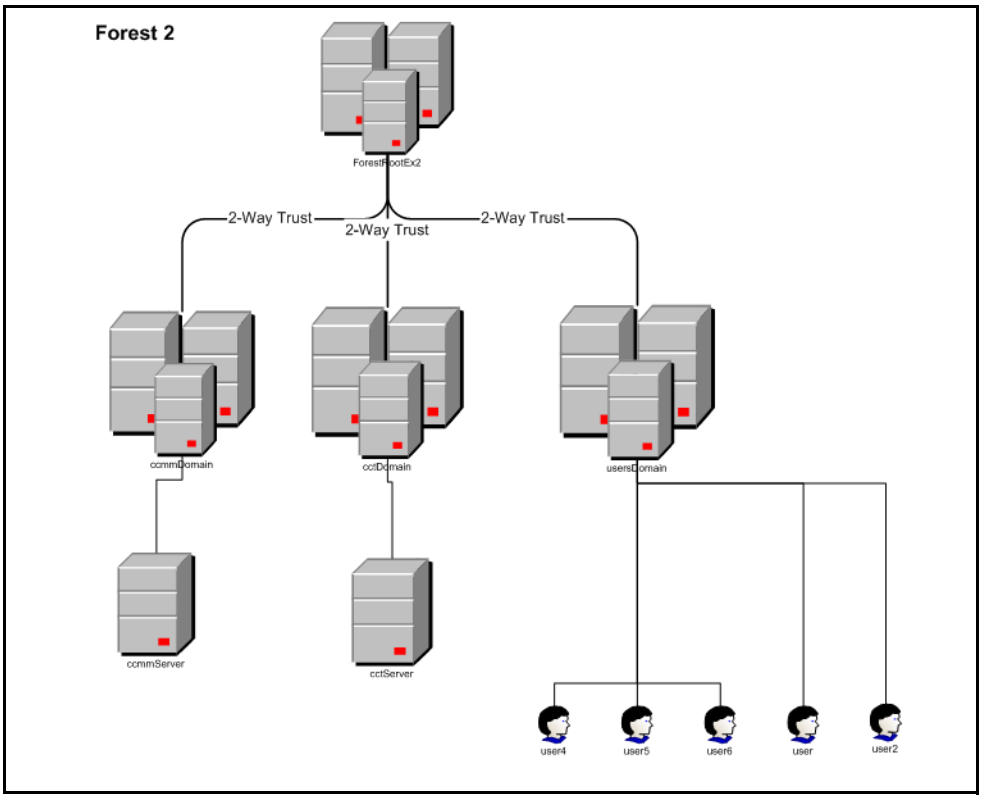
Optionally, the network administrator can place the Contact Center Multimedia server, the Communication Control Toolkit server, or both, into a domain different from the Agent Desktop. However, each of these domains need a two-way trust relationship with the others. If all domains are in the same forest, then a two-way trust is automatically set up between the domains.

For example, if you have three domains, one containing your Contact Center Multimedia server, one containing your Communication Control Toolkit server, and one containing your Agent Desktop, the following conditions must be true:

- The Contact Center Multimedia domain needs a two-way trust relationship with both the Communication Control Toolkit and Agent Desktop domains.
- The Communication Control Toolkit domain needs a two-way trust relationship with both the Contact Center Multimedia and Agent Desktop domains.
- The Agent Desktop domain needs a two-way trust relationship with both the Contact Center Multimedia and Communication Control Toolkit domains.

The following figure shows a multiple domain configuration.

Multiple domain example



Windows configuration checklist

When configuring the Microsoft Windows network, the network administrator must complete the tasks in the following checklist. For more information about completing these tasks, see *Avaya Aura™ Contact Center Commissioning* (NN44400-312).

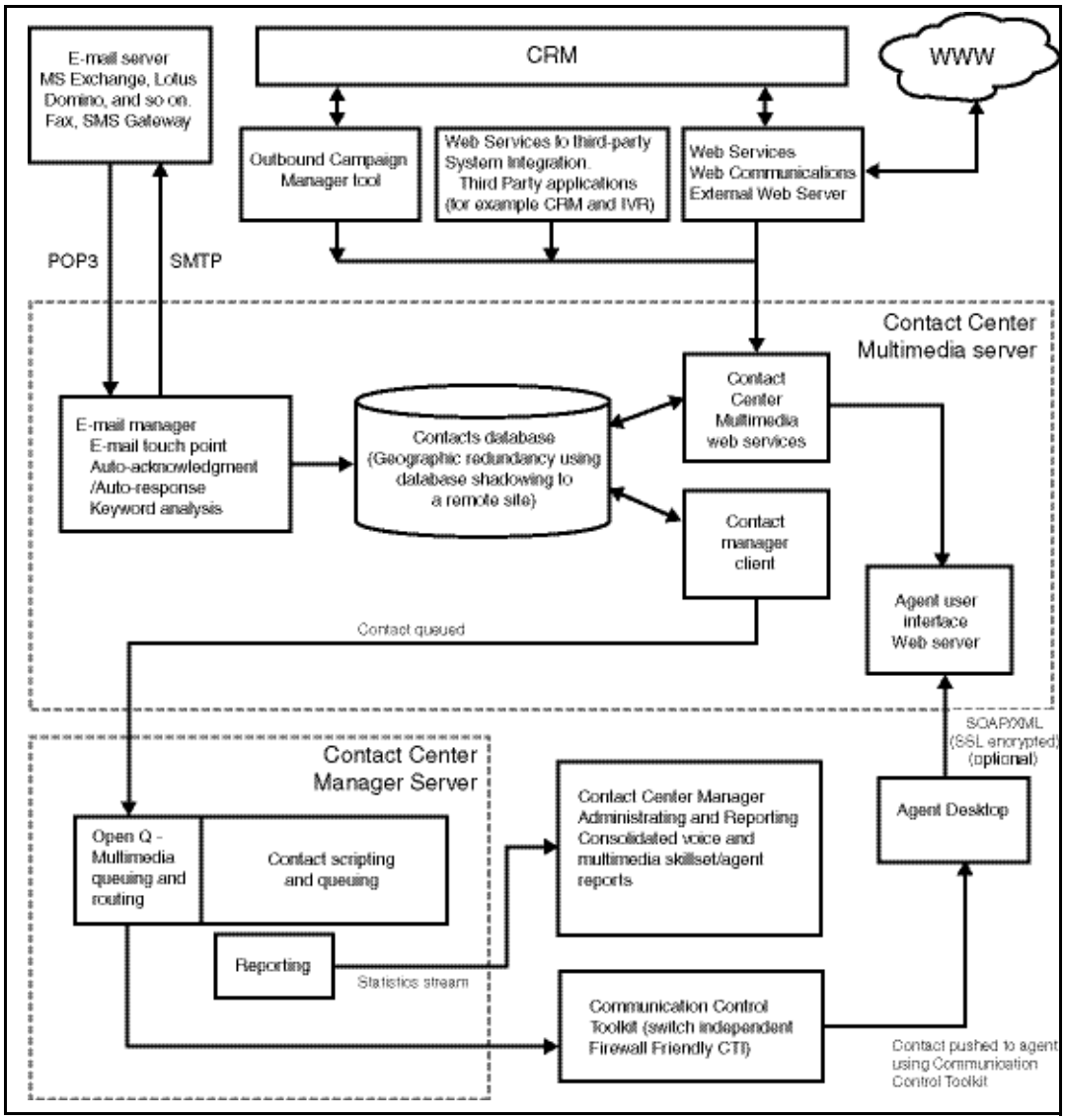
Configuration checklist

Configuration task	Completed? (Y/N)
Configure the Communication Control Toolkit desktop Configure Agent Roaming	

System network configuration

The following figure shows a sample Contact Center Multimedia network configuration.

Sample network configuration



Bandwidth requirements

Avaya recommends that the average contact center subnet usage not exceed 30 percent of the total bandwidth. This includes all the traffic (even customer traffic).

Integrating the external Web server

Before you install the Contact Center Multimedia components on the External Web server, you must consider the following:

- Web traffic estimates (including LAN traffic)
- Contact Center Multimedia provides a sample customer interface. You must have a Web designer modify and integrate your Web site to enable

transactions to enter Contact Center Multimedia. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).

- Contact Center Multimedia Web server integration with the Contact Center Multimedia server is through HTTP protocol, which is transported through Port 80. These are standard ports and need no special firewall configuration.

Communication Control Toolkit configuration requirements

This section describes the configuration requirements for the Communication Control Toolkit server.

Navigation

Communication Control Toolkit overview

With Communication Control Toolkit, three stand-alone configurations are possible:

- Contact Center/Self-service installation—Used when Communication Control Toolkit is deployed in a Contact Center environment.
- Knowledge Worker (Direct Connect) Installation—A non-Contact Center installation, used where Communication Control Toolkit connects directly to the switch and provides functionality to knowledge workers.
- Self-Service installation—Typically used in an environment where a non-Avaya switch is used, but integration with the Self-Service portfolio is still a requirement.

Communication Control Toolkit components

The Communication Control Toolkit simplifies integration. The transport components provide firewall friendliness, Network Address Translation (NAT), and Citrix support. The server components enable open telephone switch connectivity.

The Communication Control Toolkit consists of Avaya developed software and third-party components, as described in this section.

Attention: Q Signaling (QSIG) Path Replacement and Trunk Anti Tromboning is not supported in Communication Control Toolkit.

Client application

Client applications are third-party components and can include the following:

- software phones
- agent telephony toolbars with screen pop-ups
- intelligent call management applications

The Communication Control Toolkit API provides five levels of API that you can use to develop a range of client applications.

An easy-to-use graphical API delivers Windows Form Controls (Win Forms), that you can import into a project for rapid development of form-based toolbars. The Win Forms provide graphical API abstractions that enable rapid development of Communication Control Toolkit-enabled applications.

The Communication Control Toolkit API also provides abstraction layers to COM client interfaces.

Attention: TAPI legacy clients are not supported.

Communication Control Toolkit server

The component that manages client sessions consists of the following subcomponents:

- Contact Management Framework—An infrastructure component that manages the states of contacts, agents, terminals, and addresses.
- TAPI Connector—An application that converts Communication Control Toolkit requests to TAPI API calls, and TAPI events to Communication Control Toolkit events. The TAPI Connector resides between the TAPI Service Provider and the Contact Management Framework.
- TAPI Service Provider—A Microsoft TAPI client responsible for CTI operations of all lines controlled by the Communication Control Toolkit platform initialized by TAPI.
- Communication Control Toolkit API—An API that controls voice resources. The API is published as Microsoft .NET types and distributed as a Windows assembly, which is referenced by application developers.

Communication Control Toolkit supported functionality

The tables in this section indicate which functions are supported by Communication Control Toolkit.

Attention: If your phone supports Multiple Appearance Reduction Prime (MARP) of Multiple Appearance Directory Number (MADN) you must disable the configurations. These configurations are not supported in Communication Control Toolkit.

The following table list the basic Communication Control Toolkit call control functions.

Basic Communication Control Toolkit functions

Event	Supported in Communication Server 1000
Make Call	Yes
Hold Current Call	Yes
	The Swap Hold switch feature is not supported.
Unhold Call	Yes (Retrieve Call)
Drop Current Call (Release)	Yes
Blind Transfer Call	Yes
Initiate Supervised Transfer	Yes
Complete Transfer	Yes
Initiate Conference Call	Yes (up to six parties)
Complete Conference Call	Yes
Call Forward	Yes
Cancel Call Forward	Yes
Join Conference	No
Deflect Calls	No
Get Status	Yes
Get Call Capabilities	Yes
Get Data	Yes
Delete Data	Yes
Append Data	Yes
Add Data Observer	No
Remove Data Observer	No
Make Set Busy	Yes
	Make Set Busy is not supported in direct connect mode.
Reserved Function	No

(1 of 2)

Basic Communication Control Toolkit functions

Event	Supported in Communication Server 1000
Get/Set UUI	No (UUI attached as call data)
Send DTMF (for example, credit card number to IVR)	Yes DTMF is not supported in direct connect mode.
Mute/Unmute	No
Consult	Yes (but must designate as transfer or conference)
Park/Unpark	No
Message Waiting Indicator	No
HER (Host Enhanced Routing)	Yes
Answer	Yes
Auto Hold Allowed	Yes
(2 of 2)	

The fast transfer functionality does not support completing a fast transfer call to an external trunk number. This functionality is for predictive dialing environments in which the application sends a MakeCall request to an external customer number and, when the customer answers, the application sends the FastTransfer request to blind transfer the customer to a live agent.

The following table lists the Contact Center-specific functions.

Contact Center-specific functions

Event	Supported in Communication Server 1000
Agent Login	Yes
Agent Logout	Yes
Set Ready	Yes
Set Not Ready	Yes
ACD Set Activity Code	Yes
ACD Set Not Ready/Reason Codes	Yes
Work Ready Key support	No
Agent Whisper	No
Monitor (Observe)/Record Call	No
Set Call treatment	Yes
Barge In	No
(1 of 2)	

Contact Center-specific functions

Event	Supported in Communication Server 1000
Call Supervisor	Yes
Answer Emergency call	Yes
Redirect to another skillset	Yes
Return a call to the queue skillset that it came from	No
Redirect to another skillset	No
Return a call to the queue skillset that it came from	No
(2 of 2)	

The following table indicates which events are delivered by Communication Control Toolkit.

Communication Control Toolkit events

Event	Supported in Communication Server 1000
Ringing Event	Yes
Dialtone Event	No
Busy Event	No
Offering Event	Yes
Ringback Event	Yes
Inbound Connected Event	Yes
Outbound Connected Event	Partial
Connected Event	Yes
Disconnected Event	Yes
Held Event	Yes
Unheld Event	Yes
OnHold Pending Conference Event	Yes
Onhold Pending Transfer Event	Yes
Transferred Event	Yes
Conference Event	No
Initiated Transfer Event	Yes
Initiated Conference Event	Yes
(1 of 2)	

Communication Control Toolkit events

Event	Supported in Communication Server 1000
Session Disconnect Event (includes shutdown)	Yes
Device Forward Event	No
Status Change Event	Yes
Notice Message Waiting Event	No
Notice No Message Waiting Event	No
Agent Logged out Event	Yes
Agent Logged in Event	Yes
Agent Ready Event	Yes
Agent Not Ready Event	Yes
Agent Busy Event	Yes
Agent Work Ready Event	No
Reserved Event	No
Activity Code Entered	Yes
WalkAway Activated	No
WalkAway Return	No
Emergency Invoked	No
Call Supervisor Invoked	No
(2 of 2)	

Client Terminal Relationships

The Communication Control Toolkit server supports a maximum of 5000 client-to-terminal relationships.

- A client monitoring a voice device (see voice terminal control capacity specification below)
- A client monitoring a multimedia terminal (see CCMM terminal control capacity specification below)

If a client monitors voice and multimedia terminals, each pair of voice + multimedia terminals are counted once; for example,
1 voice terminal + 1 multimedia terminal = 1

2 voice terminals + 1 multimedia terminal = 2
2 voice terminals + 2 multimedia terminals = 2
2 voice terminals + 3 multimedia terminals = 3

The CCT server supports a maximum of 5000 CTI client-to-telephony- device relationships where the CTI client-to-telephony device relationship is defined as a CTI client (CCT client or TAPI client) that monitors and controls a telephony device. A telephony device refers to one of the following:

- A CCT Voice Terminal (TN)
- A CCT RoutePointAddress (CDN)
- CCMM terminal control capacity

CCT clients can monitor or control a multimedia terminal. A multimedia terminal is created dynamically when a Contact Center agent that is configured with one or more multimedia contact types logs on.

The following are some examples of capacity configurations.

- 5000 CCT clients, each monitoring and controlling a single Terminal (5000 CTI clients x 1 telephony device = 5000)
- 1 CCT client monitoring and controlling 5000 Terminals (1 CTI client x 5000 telephony devices = 5000)
- 100 CCT clients, each monitoring and controlling 10 Terminals (100 CTI clients x 10 telephony devices = 1000)

Voice and multimedia

- 2750 CCT clients, each monitoring and controlling a single voice terminal + 600 CCT Clients each controlling a single multimedia terminal
- 2750 CCT clients, each monitoring and controlling a single voice terminal + 600 CCT clients, each monitoring a single voice terminal and a single multimedia terminal

Server hardware requirements

This section describes hardware requirements for the Communication Control Toolkit server.

The following table lists the hardware requirements for Communication Control Toolkit server installed with Windows Server 2008 Release 2 Standard Edition and Enterprise Edition 64 bit. These specifications are for stand-alone configurations only. For co-resident configurations, see Co-resident configuration requirements (page 133).

Attention: The hardware specifications in this section are for general guidance only. Carefully analyze your contact center capacity requirements using the Capacity Assessment Tool (CapTool) before you decide the specifications for your PVI server.
You can download the CapTool software utility from the Partner Information Center Web site (www.avaya.com/support).

You can install the Agent Desktop Toolbar on the Communication Control Toolkit server.

You can install Contact Center License Manager co-resident on the Communication Control Toolkit server in a Knowledge Worker configuration.

Communication Control Toolkit server hardware requirements

Hardware item	Recommended minimum	Additional information
CPU	Quad-core Xeon 2.8 GHz or equivalent. Use the Contact Center CapTool to determine the appropriate CPU required.	Quad-CPU systems are supported with or without Hyperthreading enabled. AMD processors of the same or higher specification are also supported. Unsupported processors include Intel Celeron, and Intel Itanium (IA 64) processors.
Maximum number of physical CPUs	4	—
RAM	8 GB	—
Hard disk size	81 GB of logical disk space (162 GB with RAID-1)	—
Hard disk partitioning See Disk partitioning requirements (page 122).	—	—
Hard disk type	SCSI, SATA, or SAS > 7200 RPM	A Storage Area Network (SAN) configuration is not supported.
(1 of 2)		

Communication Control Toolkit server hardware requirements

Hardware item	Recommended minimum	Additional information
DVD ROM	One dual layer DVD ROM	
Network interface	One network interface card for Contact Center/ Self Service Installation One network interface card with the ELAN subnet router connected to the contact center subnet. When deploying in Self Service Installation mode with non-Avaya PBXs, check network interface requirements with the appropriate PBX vendor.	ELAN subnet must be 10/100 Mb/s Ethernet. The contact center subnet facing network interface card must be 100 Mb/s Ethernet or higher. The binding order of the network interface cards is important. The contact center subnet card is first, and then ELAN subnet.
(2 of 2)		

CPU use

CPU use with all applications running and under peak traffic load must not exceed an average of 70 percent. This CPU limit applies to both stand-alone and co-resident configurations.

RAID controller

For RAID requirements, see Redundant Array of Independent Disks (page 56).

Uninterruptible Power Supply

For Uninterruptible Power Supply (UPS) requirements, see Uninterruptible Power Supply (page 56).

Server operating system requirements

This section describes the operating system requirements for the Communication Control Toolkit server.

The following table shows the operating system versions on which support is available for Communication Control Toolkit.

Communication Control Toolkit server operating system requirements

Operating system	International versions supported	Minimum service pack
Windows Server 2008 Release 2, Standard Edition and Enterprise Edition, 64-bit	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	—

Microsoft hotfixes

You must operate your server with the most current Microsoft patches.

- Review the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* (available from Technical Support Web site) for the list of applicable Microsoft security hotfixes that you should apply.
- Back up the entire server, then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Disk partitioning requirements

The following table lists the disk partitioning requirements for Communication Control Toolkit.

Communication Control Toolkit disk partitioning requirements

Drive letter	Recommended size	Notes
Operating system partition (usually C)	60 GB	NTFS partition on disk 0. This must be partitioned as the primary partition. Windows 2008 Release 2 Server is installed here.
Application partition (usually D)	20 GB	—
DVD ROM drive (usually E)	N/A	DVD ROM
(1 of 2)		

Communication Control Toolkit disk partitioning requirements

Drive letter	Recommended size	Notes
Database partition (usually F)	1 GB	—
Total disk size	81 GB	—
(2 of 2)		

Client hardware requirements

The application developer must specify the requirements of the Communication Control Toolkit client PC.The Communication Control Toolkit client must meet the minimum requirements of the operating system.

Port requirements

Communication Control Toolkit clients use a single port for communication with the Communication Control Toolkit server. By default, this port is 29373; however, the port number is configurable. For instructions, see *Avaya Aura™ Contact Center Server Administration* (NN44400-610). If you use a firewall, ensure that this port is open.

Client operating system requirements

The following table lists the operating system requirements for Communication Control Toolkit clients.

Communication Control Toolkit client operating system requirements

Operating system	International versions supported (See Note)	Minimum service pack
Windows XP Professional	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	Service Pack 2 or later
Windows Vista Business Edition	English	Service Pack 1 or later
Windows Vista Enterprise Edition	English	Service Pack 1 or later
(1 of 2)		

Communication Control Toolkit client operating system requirements

Operating system	International versions supported (See Note)	Minimum service pack
Windows 7 (32-bit and 64-bit)	English	—
Note: The client operating system must be of the same language family as the Communication Control Toolkit server.		
(2 of 2)		

Third-party software requirements

This section describes the third-party software requirements for the Communication Control Toolkit server and clients.

Antivirus software

For antivirus software requirements, see Additional guidelines for the use of anti-virus software (page 53).

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in <Install_Directory>:\Avaya\Cache\CacheSys. Databases and journal files are installed in <Install_Directory>:\Avaya\Contact Center\Databases.

.NET Framework

The Communication Control Toolkit software development kit is based on .NET 3.5 and uses Microsoft Windows Communication Foundation (WCF) technology. Therefore, you must install .NET 3.5 on all Communication Control Toolkit client PCs.

Remote support access tool

You must configure a remote support access tool on the server to provide remote support. You can use LogMeIn Rescue from LogMeIn (www.logmein.com). LogMeIn Rescue supports remote systems over the Web without installing software.

You can use the Remote Desktop Connection feature in Windows as an alternative for remote support access tool instead of LogMeIn Rescue. Remote Desktop Connection is supported in console or admin mode only. Refer to the Microsoft Web site for details about how to verify that you are connected to the console/admin session (session 0).

Communication Control Toolkit port requirements

The following table shows the port numbers required for Communication Control Toolkit (CCT).

Communication Control Toolkit port usage

Communication Control Toolkit port number	Functionality
1972	Caché database, and Caché shadowing High Availability solutions.
29373	Listens for requests from CCT client applications.
29374	Data Access Layer Service listens for requests from CCT Remote Administration Console.
3000	For TAPI switch connection through MLS (CCMA server). This port is required for the contact center subnet.
3998	License Manager (LM) destination port, which is the first of 10 consecutive ports required for license management.
3999 - 4007	LM client source ports.
8081	CCT Web Administration.
8085	For CCT services to access the CCT database.
8098	For the Contact Management Framework on the CCT server.
8099	For the Contact Management Framework on the CCT server.
8888	For the TAPI switch connection using direct-connect. This port is required only for the ELAN subnet.
5000	To connect to the server in CCMS.
8087	For CCT CMF component.
9010	For CCT CMF component.

Network configuration

This section describes network configuration information for Communication Control Toolkit.

Network interface card binding order

Configure the binding order of the network interface cards so that the NIC connected to the contact center subnet is first, followed by others such as the virtual adapters for remote access.

Communication Control Toolkit and Avaya Communication Server 1000 Telephony Manager on the ELAN subnet

In situations where both Communication Control Toolkit and Communication Server 1000 Telephony Manager are present, take extra care in the treatment of the ELAN subnet. When connecting the ELAN subnet to a router, follow the Communication Server 1000 Telephony Manager strict guidelines for filtering and routing. Your configuration must meet the requirements for the Communication Server 1000 Telephony Manager. *Communication Server 1000M and Meridian 1 Large System Planning and Engineering* (NN43021-220) prescribes ELAN engineering details for Contact Center application engineering.

The ELAN subnet is designed and tested for inter-Avaya product communications. These external communications over the ELAN subnet, therefore, present an unknown factor and thereby potential negative impact to the overall operation of the telephone switch and auxiliary processors.

Maximum acceptable use

Total usage of the Enterprise IP network must not exceed 30 percent in a shared network environment. Communication Control Toolkit use of the Enterprise IP network can be as high as 9 percent for a system with 500 agents. Ensure that the Enterprise IP network has enough spare capacity to accommodate Communication Control Toolkit traffic in addition to your traffic.

Knowledge worker environment requirements

In a knowledge-worker environment, Communication Control Toolkit communicates on the contact center subnet and, in turn, the ELAN subnet to the switch.

Contact modeling limitations in a network environment

Some limitations exist in the information you can model the Communication Control Toolkit when you deal with networked call scenarios.

Contact modeling

Conference calls that involve parties from more than one networked switch cannot be completely represented on each Communication Control Toolkit (CCT) system. Each CCT system can model only the parties that it has direct visibility with. For instance, consider a conference call involving parties A, B, and C, where A and B are on CCT 1 and party C is on CCT 2. If party B is the conference controller (initiated the conference with party C), then from the

perspective of CCT 1 shows a three-party call with parties A, B, and C involved. However, the perspective of CCT 2 shows only a two-party call with B and C involved with B as the calling address and C as the called address.

Security Framework configuration requirements

This section provides the configuration requirements for the Security Framework server.

Security Framework is not supported co-resident with Media Application Server (MAS).

Navigation

- Server hardware requirements (page 129)
- Server operating system requirements (page 131)
- Third-party software requirements (page 131)

Server hardware requirements

This section describes hardware requirements for Security Framework.

Server hardware requirements

The following table lists the hardware requirements for a stand-alone Security Framework server. You can install Security Framework co-resident with Contact Center Manager Administration. For more information, see Server hardware requirements (page 85).

Attention: The hardware specifications in this section are for general guidance only.
Carefully analyze your contact center capacity requirements using the Capacity Assessment Tool (CapTool) before you decide the specifications for your PVI server.
You can download the CapTool software utility from the support Web site (www.avaya.com/support).

Security Framework server hardware requirements

Hardware item	Recommended minimum	Additional information
CPU	Quad-Core Xeon 2.8 GHz or equivalent. Use the Contact Center CapTool to determine the appropriate CPU required.	Quad-CPU systems are supported with or without Hyperthreading enabled. AMD processors of the same or higher specification are also supported. Unsupported processors include Intel Celeron, and Intel Itanium (IA 64) processors.
Maximum number of physical CPUs	4	—
RAM	8 GB	—
Hard disk space	60 GB of logical disk space (120 GB of physical disk space with RAID-1)	—
Hard disk partitioning	No specific partitioning requirements	—
Hard disk type	SCSI, SATA, or SAS	At this time, a SAN (Storage Area Network) configuration is not supported.
Hard disk speed	> 7200 RPM	—
DVD ROM	One dual layer DVD ROM drive	—
Network interface	One network interface card	The server subnet facing network interface card must be 100 Mb/s Ethernet or higher.
Video card	One video card and monitor	1024 x 768 minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—
Note: All hardware devices must be on the Microsoft Hardware Compatibility List for Windows Server 2008. For a complete list of compatible hardware devices, see the Microsoft Web site (www.microsoft.com).		

CPU use

For optimal performance, average CPU use on the Security Framework server must not exceed 70 percent over a 15 minute interval.

RAID controller

For RAID requirements, see Redundant Array of Independent Disks (page 56).

Uninterruptible Power Supply

For Uninterruptible Power Supply (UPS) requirements, see Uninterruptible Power Supply (page 56).

Server operating system requirements

The following table provides the operating system requirements for the Security Framework server.

Security Framework server operating system requirements

Operating system	International versions supported	Minimum service pack
Windows Server 2008 Release 2, Standard Edition and Enterprise, 64-bit	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	

Microsoft security hotfixes

You must operate your server with the most current Microsoft patches.

- Review the Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List (available from Technical Support Web site) for the list of applicable Microsoft security hotfixes to apply.
- Backup the entire server, then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Third-party software requirements

This section describes the third-party software requirements for the Security Framework server.

Antivirus software

For antivirus software requirements, see Additional server requirements (page 51).

Remote support access tool

You must configure a remote support access tool on the server to provide remote support for the Security Framework. You can use LogMeIn Rescue from LogMeIn (www.logmein.com). LogMeIn Rescue supports remote systems over the Web without installing software.

You can use the Remote Desktop Connection feature in Windows as an alternative for remote support access tool instead of LogMeIn Rescue. Remote Desktop Connection is supported in console or admin mode only. Refer to the Microsoft Web site for details about how to verify that you are connected to the console/admin session (session 0).

Co-resident configuration requirements

This section lists the requirements for a co-resident installation. You can install multiple Avaya Aura™ Contact Center applications co-resident on one server. The more applications you install on a server the fewer agents that server will support. Use the Capacity Assessment Tool (CapTool) to determine the number of agents your server supports.

You can install the following Avaya Aura™ Contact Center applications co-resident on a single server:

- Contact Center Manager Server
- License Manager
- Contact Center Manager Administration
- Communication Control Toolkit
- Contact Center Multimedia
- Server Utility
- Media Application Server
- Service Creation Environment

If you install all the Avaya Aura™ Contact Center applications on a single server, then Avaya Aura™ Contact Center supports up to 200 agents and a call rate of less than 12 000 calls per hour.

Navigation

- Server hardware requirements (page 134)
- Server operating system requirements (page 136)
- Disk partitioning requirements (page 137)
- Third-party software requirements (page 138)
- Co-residency and your network (page 139)
- Supported configurations (page 140)
- Installation order and supported combinations (page 143)
- Limitations of a co-resident server (page 144)
- Security requirements (page 145)
- Server backup requirements (page 145)
- Remote support for a co-resident server (page 145)

Server hardware requirements

This section describes the server hardware requirements for co-residency scenarios.

Attention: The hardware specifications in this section are for general guidance only. Carefully analyze your contact center capacity requirements using the Capacity Assessment Tool (CapTool) before you decide the specifications for your PVI server.
You can download the CapTool software utility from the support Web site (www.avaya.com/support).

A co-resident server with Windows Server 2008 Release 2 64-bit Standard Edition supports the following applications with limited capacity and features:

- Contact Center Manager Server (CCMS)
- License Manager (LM)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Server Utility (SU)
- Media Application Server (MAS)
- Service Creation Environment (SCE)
- Security Framework

Security Framework is not supported co-resident with Media Application Server (MAS).

Co-resident server hardware requirements

Hardware item	Recommended minimum	Additional information
CPU	Dual Quad-Core Xeon 2.5 GHz or equivalent. Use the Contact Center CapTool to determine the appropriate CPU required.	Quad-CPU systems are supported with or without Hyperthreading enabled. AMD processors of the same or higher specification are also supported. Unsupported processors include Intel Celeron and Intel Itanium (IA 64).
RAM	8 GB	—
Hard disk space	506 GB of logical disk space (1012 GB of physical disk space with RAID-1) if CCMM is installed co-resident with CCMS. 206 GB if CCMM is not installed co-resident with CCMS.	RAID-1 is recommended for all disks on the shared SCSI bus to eliminate disk drives as a potential single source for hardware failures.
Hard disk type	SCSI, SATA, or SAS >15 000 RPM required if MAS is co-resident.	IDE drives not supported. At this time, a SAN (Storage Area Network) configuration is not supported.
Hard disk speed	> 7200 RPM > 15 000 RPM if MAS is co-resident.	—
DVD ROM	One dual layer DVD ROM drive	
Network interface	One network interface card (Network Control Center requires only one network interface card)	ELAN subnet must be 10/100 Mb/s Ethernet. The contact center subnet facing network interface card must be 100 Mb/s Ethernet or higher. Only Ethernet is supported. A Token Ring is not supported.
Note 1: All hardware devices must be on the Microsoft Hardware Compatibility List for Windows 2008 Server. For a complete list of compatible hardware devices, see the Microsoft Web site (www.microsoft.com).		

CPU use

For optimal performance, steady state CPU consumption must not exceed 70 percent over a 15 minute interval. Use the CapTool application to engineer a platform with a processor that is a suitable size for your configuration.

RAID controller

For RAID requirements, see Redundant Array of Independent Disks (page 56).

Uninterruptible Power Supply

For Uninterruptible Power Supply (UPS) requirements, see Uninterruptible Power Supply (page 56).

Server operating system requirements

The following table provides operating system requirements for a co-resident installation.

Co-resident server operating system requirements

Operating system	International versions supported	Minimum service pack
Windows Server 2008 Release 2, Standard Edition and Enterprise Edition, 64-bit	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	

Operating system installation and configuration

See the specific requirements for Contact Center Manager Server, Contact Center Multimedia, and Communication Control Toolkit stand-alone configurations in this document.

The Contact Center Manager Administration requirement for IIS takes precedence over the Contact Center Manager Server requirement because IIS is a core part of the Contact Center Manager Administration implementation. The updated preinstallation compliancy utility tests for IIS and for the other required components before installation.

Microsoft security hotfixes

You must operate your server with the most current Microsoft patches.

- Review the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* (available from the Technical Support Web site) for the list of applicable Microsoft security hotfixes to apply.
- Back up the entire server, then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.

- Apply Microsoft security updates on a timely basis.

Disk partitioning requirements

The section describes partitioning a server to meet the requirements of Platform Vendor Independence. This information covers all co-residency scenarios. The following table shows minimum and maximum partition sizes.

Attention: In a co-residency scenario, for Contact Center Manager Server and Communication Control Toolkit, if the space in your dynamic database drive is full, you can expand the database drive. To avoid database expansions, Avaya recommends that you have at least 300 GB on you disk. For more information about expanding the dynamic disk, see *Avaya Aura™ Contact Center Installation* (NN44400-311).

Co-resident server disk partitioning requirements

Drive letter	Recommended size	Notes
Operating system drive (usually drive C)	60 GB	NTFS partition on disk 0. This must be partitioned as the primary partition. The Windows Server 2008 Release 2 operating system is installed here.
Application drive (usually drive D)	80 GB if CCMM is install co-resident with CCMS 20 GB if CCMM is not installed co-resident with CCMS.	Additional NTFS partition on disk 0 or an NTFS partition on a different disk. This must be partitioned as a logical drive within an extended partition because this partition is not used for startup. Contact Center Manager Server is installed here.
DVD drive (usually drive E)	N/A	DVD ROM drive.
CCMS database partition (usually drive F)	60 GB if CCMM is installed co-resident with CCMS. 120 GB if CCMM is not installed co-resident with CCMS.	—
CCT database partition (usually drive F)	1 GB	—
CCMM database partition	300 GB	—
Trace logs partition (optional)	5 GB	—

- Partitioned sizes on all database drives must be in increments of 1 GB (equivalent to 1024 MB).

- You must partition all Contact Center software drives as logical drives within extended partitions because these partitions are not used for starting.
- You can locate the C drive, D drive, and database partitions on the same hard disk, if required, if sufficient disk space is available. However, you may want to keep the database and the Contact Center Manager Server application on different hard disks for optimal system performance and reliability.
- Avaya does not guarantee the support for future Windows 2008 Server Service Packs, which may require larger disk space.

See *Avaya Aura™ Contact Center Installation* (NN44400-311) for additional information regarding disk partitioning.

Note the following for precise size definitions:

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

Third-party software requirements

See the specific requirements for Contact Center Manager Server, Contact Center Manager Administration, and Communication Control Toolkit stand-alone configurations in this document.

Antivirus software

For antivirus software requirements, see Additional guidelines for the use of anti-virus software (page 53).

Remote access support tool

You must configure a remote support access tool on the server to provide remote support. You can use LogMeIn Rescue from LogMeIn (www.logmein.com). LogMeIn Rescue supports remote systems over the Web without installing software.

You can use the Remote Desktop Connection feature in Windows as an alternative for remote support access tool instead of LogMeIn Rescue. Remote Desktop Connection is supported in console or admin mode only. Refer to the Microsoft Web site for details about how to verify that you are connected to the console/admin session (session 0).

If Communication Control Toolkit is included in the co-resident installation, you can use pcAnywhere to connect to the co-resident server in the following ways:

- through an Ethernet connection over a LAN

- through a dial-up connection into another non-Communication Control Toolkit server on the domain that provides access to the Communication Control Toolkit server through a LAN

Problems occur if you attempt to connect directly to the TAPI server through a modem because of a potential conflict when a modem driver is on the same server as the TAPI driver. (TAPI is a subcomponent of Communication Control Toolkit.)

Co-residency and your network

When you enable the networking feature and one Contact Center Manager Server co-resides with the Contact Center Manager Administration server, then you can use this Contact Center Manager Administration server to administer the Contact Center Manager Server server with which it resides.

Additionally, if you have a stand-alone Contact Center Manager Administration server and a co-resident Contact Center Manager Administration server, you can use the stand-alone Contact Center Manager Administration server to administer the co-resident Contact Center Manager Server/Contact Center Manager Administration server. Do not use the co-resident Contact Center Manager Administration server to administer other Contact Center Manager Servers in the network. The administration of other non-co-resident Contact Center Manager Servers places an additional load on the CPU of the co-resident server (which can affect the contact center operation).

If Active Directory Lightweight Directory (AD-LDS) replication is enabled on the co-resident Contact Center Manager Administration server, then this server shares Contact Center Manager Administration data with all other replication-enabled Contact Center Manager Administration AD-LDS instances in your network. For example, if you have a stand-alone Contact Center Manager Administration server that has a number of Contact Center Manager Servers configured, then when this server replicates with a co-resident Contact Center Manager Administration server, all Contact Center Manager Servers are also visible on the co-resident server. However, even though the co-resident Contact Center Manager Administration server displays these multiple Contact Center Manager Servers, you can use this Contact Center Manager Administration server to administer only the Contact Center Manager Server with which it resides.

A further consideration is the extra bandwidth used by co-resident Contact Center Manager Administration servers that have multiple Contact Center Manager Servers configured. Each Contact Center Manager Administration server receives unicast or multicast data from each Contact Center Manager Server on the network. This data is then consolidated and retransmitted to the network, which can result in sending duplicate data over the network.

On a co-resident Contact Center Manager Administration server that is not replicating, Avaya recommends that you configure only the co-resident Contact Center Manager Server that it administers. This configuration minimizes the amount of multicast data retransmitted by Contact Center Manager Administration to the network by using the multicast filtering feature. This feature allows Contact Center Manager Administration to transmit multicast data only for the configured Contact Center Manager Server. This is not possible in a scenario where replication is enabled and more than one Contact Center Manager Server is configured on any replicating Contact Center Manager Administration server.

The following conditions apply:

- You must install the NCC server on a stand-alone server; it cannot co-reside with Contact Center Manager Administration on one server.
- If you have multiple Contact Center Manager Administration servers in your network, the data that you create and store on one server (such as partitions) is available only on this server; it is not reflected on all Contact Center Manager Administration servers on your network.

Supported configurations

The following table shows which Contact Center applications are supported in a co-resident configuration.

Contact Center co-resident configurations

	CCMS	CCMA	CCT	CCMM	License Manager	Server Utility	AAAD	SCE	MAS
CCMS	N/A	Yes	Yes (see Note 3)	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 (see Note 2)	Yes	Yes
CCT	Yes (see Note 3)	Yes (see Note 1)	N/A	Yes (see Note 4)	Yes (see Note 1)	Yes	Yes (see Note 2)	Yes	Yes
CCMM	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	N/A	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)
License Manager	Yes	Yes (see Note 1)	Yes (see Note 1)	Yes (see Note 4)	N/A	Yes	Yes (see Note 2)	Yes (see Note 1)	Yes
Server Utility	Yes	Yes	Yes	Yes (see Note 4)	Yes	N/A	No	Yes	Yes
Security Framework	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
AAAD	Yes (see Note 2)	Yes (see Note 2)	Yes	Yes	Yes (see Note 2)	Yes (see Note 2)	N/A	Yes (see Note 2)	Yes
SCE	Yes	Yes	Yes (see Note 1)	No	Yes (see Note 1)	Yes	No	N/A	Yes
MAS	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	Yes (see Note 5)	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 on the same server for the 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. CCMM and CCMS co-residency is supported to a 200-agent limit. The agent limit is 100 with an Essential license.

Note 5: CCMS, CCMA, CCT, and CCMM must be installed on the same server for MAS to co-reside with CCMS. MAS is supported only in SIP enabled contact centers. If the 200-agent limit is reached for a SIP-enabled single server installation with MAS and CCMM, you must remove MAS and CCMM be from the server at the same time.

Note 6: In SIP-enabled contact centers, for CCMM to co-reside with CCMS, MAS must also be installed co-resident.

Network Control Center is configured only in stand-alone mode and cannot be installed co-resident with Contact Center Manager Administration or Communication Control Toolkit.

The following configurations are not supported:

- Contact Center Manager Server and Communication Control Toolkit, without Contact Center Manager Administration
- Contact Center Manager Administration and Communication Control Toolkit, without Contact Center Manager Server
- Media Application Server without Contact Center Multimedia.
- Contact Center Multimedia without Contact Center Manager Server, Contact Center Manager Administration, and Communication Control Toolkit.

Attention: All requirements in this document for stand-alone installations are valid for a co-resident installation unless they are explicitly superseded by alternative requirements in the following sections of the document.

The following conditions apply:

- You can install the Communication Control Toolkit only on a server on which you already installed Contact Center Manager Server and Contact Center Manager Administration.
- If you installed Contact Center Manager Server and Server Utility on the same computer, and then you install Contact Center Manager Administration, you must uninstall the Server Utility before you install Contact Center Manager Administration, and then reinstall it after you install Contact Center Manager Administration.
- For migrations, you must select the same switch type on the new server that was associated with the old server. For example, if you configured a co-resident 7.0 with an Avaya Communication Server 1000 switch, you cannot migrate to a co-resident configuration with a SIP switch.
- Media Application Server is supported only in SIP-enabled contact centers.

Installation order and supported combinations

This section provides the sequence in which you should install Contact Center components as well as the various supported component combinations.

Co-resident matrix—supported combinations and installation order

Contact Center Manager	License Manager	CCMA	CCT	CCMM	Server Utility	Media Application Server
X					X	
X	X					
X	X				X	
X		X				
X		X			X	
X	X	X				
X	X	X			X	
	X	X				
	X	X			X	
X	X	X	X			
X	X	X	X		X	
X	X	X	X	X		X
X	X	X	X	X	X	X
Attention: X = Supported Combination **Attention:** You must install the Contact Center components in order from left to right.						

Three servers

If you are limited to three servers and want to use Contact Center Multimedia (CCMM) server functions, or if you expect your contact center traffic to be below a special threshold, install Contact Center Manager Server (CCMS), Contact Center Manager Administration (CCMA), License Manager, Security Framework, and Server Utility on the same server. Install Communication Control Toolkit (CCT) and Contact Center Multimedia (CCMM) each stand-alone on the other two servers.

Install the preceding Contact Center components in the following sequence:

- CCMS
- License Manager
- Server Utility

- CCMA
- Security Framework

Two servers

If you are limited to two servers and want to use Contact Center Multimedia (CCMM) server functions, or if you expect your contact center traffic to be below a special threshold, install Contact Center Manager Server (CCMS), Contact Center Manager Administration (CCMA), License Manager, Server Utility, Security Framework, and Communication Control Toolkit (CCT) on the same server.

Install these Contact Center components in the following sequence:

- CCMS
- License Manager
- CCMA
- CCT
- Server Utility
- Security Framework

You can install co-resident applications at the same time by using the Contact Center Installer.

Limitations of a co-resident server

The following sections describe the limitations of a co-resident server.

Capacity

The capacity supported by a co-resident server is less than the capacity of a stand-alone server running on the same hardware platform.

You can use the CapTool application to determine the hardware requirements for a co-resident server.

Contact Center Manager Administration

You can access Contact Center Manager Administration (CCMA) two different ways.

Accessing from an external client PC

When you use an external client PC to access Contact Center Manager Administration on a co-resident server, Avaya recommends that you limit the number of on-demand and scheduled historical reports run on the co-resident server. Running historical reports can increase the CPU usage on the server.

Accessing from a browser on the co-resident server

When you access Contact Center Manager Administration from a browser on the co-resident server, Avaya recommends that you limit the number of on-demand and scheduled historical reports run on the co-resident server. Running historical reports can increase the CPU usage on the server.

In addition, Avaya recommends that you limit the number of real-time displays that you start. Viewing real-time displays also increases the CPU usage on the server.

Network Skill-Based Routing

In a networking environment, a co-resident Contact Center Manager Administration can administer only the co-resident Contact Center Manager Server.

Security requirements

You must operate your server with the most current Microsoft patches.

- Review the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* (from the Technical Support Web site) for the list of Microsoft security hotfixes to apply.
- Back up the entire server, then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Server backup requirements

To keep data synchronized between Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit and Contact Center Multimedia on a co-resident server, ensure that whenever you back up one application, you back up the other at the same time.

When you perform a full offline backup of the server, the entire server is backed up, including all applications. This backup method ensures that the data between the applications is always synchronized. Furthermore, you must store a set of backups in the same location.

For information about backing up Contact Center Manager Administration, see *Avaya Aura™ Contact Center Server Administration* (NN44400-610).

Remote support for a co-resident server

This section describes remote support using VPN and direct-connect modem in both stand-alone mode and co-resident mode.

Remote support for Contact Center Manager

If you require remote technical support, your distributor or Avaya technical support staff must be able to connect remotely to your server. Virtual Private Network (VPN) is more secure than directly connected modems. While many VPN technologies and configurations are available, for remote support of Enterprise voice equipment, Avaya supports a standard with a technology based on the VPN Router 1100 (as a minimum) in a particular host-to-gateway configuration.

Avaya recommends this configuration for both stand-alone mode and co-resident mode.

Remote support over a direct-connect modem

If VPN is not available, you can provide remote support over a direct-connect modem (however, many enterprises view this as a security risk).

To facilitate remote support through a direct-connect modem the following is required:

- a modem connected to each Contact Center Manager Server
- Remote Access Services (RAS) configured on each server

Attention: Due to the operating system communication-layer issues, you cannot configure Contact Center Manager Administration and the Communication Control Toolkit to use RAS (and thereby the direct-connect modem) for remote support.

Therefore, if Contact Center Manager Server is configured 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 direct-connect modem access through an external RAS device on the data-network, as indicated in the following examples:

- a corporate RAS server with modem to the PSTN and a connection to the LAN
- a computer with modem to the PSTN, RAS enabled, and a connection to the LAN
- A third-party remote-maintenance product with modem to the PSTN and a connection to the LAN

With the listed alternatives, the end user assumes the responsibility for setup on their premises and the risks to their equipment associated with this pass-through type of connection.

You can use the Remote Desktop Connection feature in Windows as an alternative for remote support access tool instead of pcAnywhere.

Guidelines for the remote support VPN

When you set up your VPN for remote support, follow these guidelines:

- Create a dedicated subnet for Avaya 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 access to other subnets in your LAN/WAN. As usual, ensure that the Avaya application servers have unrestricted access to the enterprise LAN/WAN.
- Ensure that the ELAN subnet connects to the contact center subnet through a router. Take the additional precaution of configuring the network router to allow 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.

VPN configurations

This section describes configurations that meet the needs of most users. However, because every network is different, the exact configurations may not be practical in all environments. Use these recommendations as a starting point and building block when you create your Remote Support VPN.

The remote support configurations recommended by Avaya provide the following benefits:

- Protection for your network from unauthorized external users.
- Any location is accessible, even through an analog line, but are still protected by the VPN.
- Flexible designs exist that can extend to non-Avaya products and that can accommodate customer-specific network requirements.
- VPN equipment is local to the equipment it serves, resulting in network and management simplicity, while allowing for central security authentication management.
- Solution is cost-effective.

The recommended configuration is a starting point for designing your Remote Support VPN. However, when you deviate from the recommended configurations, you may sacrifice some benefits.

Configuration types

Avaya recommends a host-to-gateway configuration for the Remote Support VPN.

SIP Contact Center configuration requirements

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

Navigation

General requirements

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

Dependent platform and switch compatibility

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

Switch compatibility

Platform	Release	Requirement
Avaya Communication Server 1000 + Signaling Server + NRS	5.0, 5.5, 6.0, 7.0	Converged Office
Avaya Communication Server 1000 Call Server	5.0, 5.5, 6.0, 7.0	Converged Office—SIP CTI
Media Application Server (MAS)	6.4	—
Avaya Aura™ Unified Communications platform	5.2.1 or later	For patch details, see *Avaya Aura™ Contact Center Configuration – Avaya Aura™ Unified Communications Platform Integration* (NN44400-521).

Switch integration

When you install Contact Center Manager Server, you can select the Microsoft Office Communications Server (SIP) option to install a SIP-enabled contact center.

Engineer the Avaya Communication Server 1000 system so it is capable of supporting SIP, in particular DSP hardware resources to support TDM/IP transcoding. Incoming PSTN calls will require one DSP per call. Agents with TDM phones will each require another DSP. For more information, see *Communication Server 1000M Large System Planning and Engineering* (NN43021-220) and *Communication Server 1000E Planning and Engineering* (NN43041-220).

You can install two Contact Center Manager Server configurations on the same Avaya Communication Server 1000 switch with an AML connection, with one instance being a SIP-enabled Contact Center and the second instance being a regular (non-SIP) Contact Center.

Co-residency

SIP Contact Center can co-reside with Contact Center Manager Administration and Communication Control Toolkit, Contact Center Multimedia, and Media Application Server with support for a limited number of active agents.

Upgrade path

Avaya does not support migrations and upgrades from AML-based (non-SIP) Contact Center products.

MAS requirements

Avaya Aura™ Contact Center uses the media processing capabilities of the Contact Center Services for MAS (CCSM) component to support conferencing, announcements and dialogs in SIP-enabled contact centers.

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

Each MAS 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 MAS 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 on-hold must be provisioned in order for MAS to provide meaningful media to the customer. When adding this additional media, the Media Content Name in MAS must match the Local SIP Subscriber Domain Name in Contact Center Manager Server–Server Configuration.

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

A SIP-enabled Contact Center solution must contain one or more MAS server. Each MAS server in a SIP-enabled Contact Center solution must be licensed and configured to provide media services.

Server hardware requirements

This section contains the server hardware requirements for stand-alone and co-resident configurations that use SIP.

Server requirements

SIP Contact Center Manager Server requires the same hardware as AML configurations.

For more details about the hardware requirements for a stand alone SIP Contact Center Manager Server see Contact Center Manager Server configuration requirements (page 75).

The supported maximum configuration supports a contact center with less than 1500 active agents and less than 30 000 calls per hour.

For more details about the hardware requirements for a co-resident SIP Contact Center Manager Server see Co-resident configuration requirements (page 133).

CPU use

For optimal performance, average CPU use on the SIP Contact Center Manager Server must not exceed 50 percent over an interval of 15 minutes.

RAID controller

For RAID requirements, see Redundant Array of Independent Disks (page 56).

Additional requirements for SIP Contact Center Manager Server

You can implement RAID-5 with SIP Contact Center Manager Server; however, RAID-1 is an Avaya recommended solution because the RAID-1 provides maintenance personnel with extra flexibility in providing technical support. Other RAID levels are not supported. Any RAID-specific issues must be addressed by the RAID vendor.

Uninterruptible power supply

For Uninterruptible Power Supply (UPS) requirements, see Uninterruptible Power Supply (page 56).

Server operating system requirements

The following table lists the operating system requirements for a SIP Contact Center Manager Server.

SIP Contact Center operating system requirements

Operating system	International versions supported	Minimum service pack
Windows Server 2008 Release 2, Standard Edition and Enterprise Edition, 64-bit	English French German LA Spanish Brazilian Portuguese Russian Simplified Chinese Traditional Chinese Japanese	

Microsoft security hotfixes

You must operate your server with the most current Microsoft patches.

- Review the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* (available from the Technical Support Web site) for the list of applicable Microsoft security hotfixes to apply.
- Back up the entire server, then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Third-party software requirements

This section describes the third-party software requirements for the SIP Contact Center Manager Server.

You can perform two types of backup on SIP Contact Center Manager Server:

- Full (offline) Backup
- Database (online) Backup

Third-party backup software

Use third-party backup software only for full (offline) backups. To create a full backup, you must use a third-party backup utility such as Microsoft backup utility. See the third-party documentation for information about the full backup procedure, and *Avaya Aura™ Contact Center Server Administration* (NN44400-610) for information about procedures that you must perform before a full backup. If you use a third-party backup utility, it must comply with the general third-party software guidelines specified in Third-party software requirements (page 52).

Shut down all SIP Contact Center Manager Server services before you perform a full backup. Even though some third-party backup utilities can provide an online backup of all files, including the database, SIP Contact Center Manager Server does not support an online backup from these third-party backup utilities.

You must use the utility included with SIP Contact Center Manager Server to perform all other database backups due to proprietary functions called upon during the backup routine. See *Avaya Aura™ Contact Center Server Administration* (NN44400-610).

Avaya recommends that you back up your database daily.

Antivirus software

Several maintenance tasks are automatically activated on SIP Contact Center Manager Server at 12:00 midnight. Therefore, you must schedule virus scans at an off-midnight time. Similarly, you must disable active virus scans when you perform diagnostic traces or logs on the server.

For Contact Center Manager Server, Avaya recommends that you exclude the following files and folders from scans (both real-time and scheduled):

- F:\Avaya\Database\
- <additional database drive>:\Avaya\Database\
- TSM_OAM log folder location
- D:\Avaya\Contact Center\Manager server\iccm\bin\data
- D:\Avaya\Contact Center\Manager server\iccm\data
- D:\Avaya\Contact Center\Manager server\iccm\sdm\log
- OAMContainer*.log located at D:\Avaya\Core\CMF
- D:\Avaya\CCM\BIN\Tools2.exe—File access errors occur in the Scan Activity log if you do not exclude this file from scanning.
- D:\Avaya\Contact Center\Manager server\iccm\logs (SIP logs)
- D:\Avaya\Contact Center\Manager server\iccm\sgm\config\ (SIP log configuration files)

- D:\Avaya\Contact Center\Core\CMF\(current version of CMF)

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in <Install_Directory>:\Avaya\Cache\CacheSys. Databases and journal files are installed in <Install_Directory>:\Avaya\Contact Center\Databases.

For MAS, Avaya recommends that you exclude the following files and folders from scans (both real-time and scheduled):

- D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\ConfMP
- D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\CStore
- D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\IvrMP
- Profile\(username)\AppData\Roaming\Avaya\Agent Desktop\Logs

Simple Network Management Protocol (SNMP) alerting on virus confirmation

Avaya does not recommend that you activate this feature.

Remote support access tool

You must configure a remote support access tool on the server to provide remote support. You can use LogMeIn Rescue from LogMeIn (www.logmein.com). LogMeIn Rescue supports remote systems over the Web without installing software.

You can use the Remote Desktop Connection feature in Windows as an alternative for remote support access tool instead of LogMeIn Rescue. Remote Desktop Connection is supported in console or admin mode only. Refer to the Microsoft Web site for details about how to verify that you are connected to the console/admin session (session 0).

Office Communications Server 2007 hardware requirements

The following table provides the hardware requirements of the Office Communications Server (OCS) network portion of the SIP Contact Center solution and details the OCS server types required to achieve the corresponding agent capacity. These values are based on scaling down the Microsoft-issued statistics for user capacity in an OCS configuration. The Microsoft figures in the third column are based Microsoft-stated 5 percent usage level.

This table does not account for non-Contact Center activity on the part of the OC client users. (for example, if other users use the OCS network and servers for non-Contact Center activity).

OCS server requirements

Topology	Servers	Number of OC users (Microsoft numbers)	Scaled maximum number of Contact Center agents
Standard Edition (SE)	1 SE Front End server 1 Access Edge server	< 5000	< 200
Enterprise Edition (EE) Consolidated	4 Front End servers 1 Backend SQL server 1 Access Edge server	< 30 000	< 1500
Enterprise Edition Expanded Mid-range SQL	4 Front End servers 2 IIS servers 1 Backend SQL server 1 Access Edge server	< 50 000	< 1500
Enterprise Edition Expanded High-end SQL	8 Front End servers 2 IIS servers 1 Backend SQL server 1 Access Edge server	< 125 000	< 1500

The following table describes the reference hardware for the servers in the OCS network.

OCS server hardware requirements

Component	Front End servers (SE or EE), Access Edge, or IIS server	EE Backend SQL server (mid-range)	EE Backend SQL server (high-end)	A/V Access Edge Conferencing
CPU	Dual processor, dual core 2.6 GHz	Dual processor, dual core 2.6 GHz	Quad processor, dual core 2.6 GHz	Dual processor, dual core 2.6 GHz
Disk	2 x 18 GB For collocated Standard Edition server, add 2 x 36 GB, 15K RPM, RAID 0 for database log files and 2 x 36 GB, 15K RPM, RAID 0 for database data.	2 x 18 GB For collocated Standard Edition server, add 2 x 36 GB, 15K RPM, RAID 0 for database log files and 2 x 36 GB, 15K RPM, RAID 0 for database data.	Drive 1 (2 x 18 GB) for OS and Page File Drive 2 (4 x 36GB, 15K RPM, RAID 0+1) for database log file Drive 3 (4 x 36GB, 15K RPM, RAID 0+1) for database log file Drive 4 (8 x 36GB, 15K RPM, RAID 0+1) for database files	2 x 18 GB
Cache	1 MB Layer 2 for each core	1 MB Layer 2 for each core	2 MB Layer 2 for each core	1 MB Layer 2 for each core
Memory	2 GB (4 GB for Standard Edition Server or Consolidated Enterprise Edition Server)	2 GB (4 GB for Standard Edition Server or Consolidated Enterprise Edition Server)	16 GB	4 GB
Network	GBit NIC	GBit NIC	GBit NIC	2 x GBit NIC

SIP installation and configuration order

The following table lists the high-level steps specific to a new SIP installation and which book to refer to for each step.

SIP installation and configuration

Contact Center component	Procedure	Contact Center book
1. SIP proxy server and OCS 2007	Install and configure SIP proxy server and OCS 2007 server.	*Avaya Aura™ Contact Center SIP Commissioning* (NN44400-511)
2. Media Application Server (MAS)	Install and configure Media Application Server (MAS).	*Avaya Aura™ Contact Center Installation* (NN44400-311)
3. Contact Center Manager Server	Follow instructions for SIP installation.	*Avaya Aura™ Contact Center Installation* (NN44400-311)
4. Contact Center Manager Administration -Configuration component	Configure CDNs. • Enter SIP URI parameter	Contact Center Manager Administration online help
5. Contact Center Manager Administration - Contact Center Management component	Configure Agents. • Enter SIP URI parameter. • Enter SIP Address for agent.	Contact Center Manager Administration online help
6. Contact Center Manager Administration - Configuration component	Configure DNIS. • Enter URI parameter. DNIS URI should not include prefix sip.	Contact Center Manager Administration online help
7. Contact Center Manager Administration - Configuration component	Configure Routes. • Configure new routes that were created in Step 2: MAS Server.	Contact Center Manager Administration online help
8. Contact Center Manager Administration - Configuration component	Configure Media Servers and Services.	Contact Center Manager Administration online help
9. Contact Center Manager Administration - Scripting component	Configure TFE Script Commands. • Create or edit scripts for SIP intrinsics.	*Avaya Aura™ Contact Center Configuration – Service Creation Environment Application Development* (NN44400-510)
At this point you can make a test SIP call, but you cannot route it to an agent yet.		
10. Communication Control Toolkit server	Install Communication Control Toolkit. • Select the Contact Center installation section to install CCT in a SIP environment.	*Avaya Aura™ Contact Center Installation* (NN44400-311)

(1 of 2)

SIP installation and configuration

Contact Center component	Procedure	Contact Center book
11. Communication Control Toolkit server	Install Agent Desktop.	*Avaya Aura™ Contact Center Installation* (NN44400-311)
12. Communication Server 1000	Communication Server 1000 configuration. • Configure ports for virtual agent phones.	*Avaya Aura™ Contact Center Configuration – Avaya CS1000 Integration* (NN44400-512)
(2 of 2)		

SIP building blocks

This section describes Session Initiation Protocol (SIP), an application-layering control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include internet telephone calls, multimedia distribution, and multimedia conferences. SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP uses elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers. SIP runs on top of several transport protocols.

For more information about configuring the SIP switch, see *Avaya Aura™ Contact Center SIP Commissioning* (NN44400-511).

SIP user agent

SIP user agents (UA) are endpoints. For Content Center application, UAs can be considered as intelligent stateful entities, consisting of a SIP user agent client (UAC) and SIP server (UAS). SIP endpoints can terminate or originate SIP sessions, which can contain user-to-user information (for example, Instant Messaging) or negotiation messaging to set up other parallel information streams or redirect these streams to other entities through the SIP session negotiation information (SDP).

A SIP UA

- terminates (SIP UAS) or originates (SIP UAC) SIP sessions.
- addressed through logical address of record, such as pat@cc.nn.com.
- registers (generally) the current position with a central proxy server or registrar at initiation so that the proxy knows how to resolve the Address of Record (AOR) to an actual IP address.

An example of a SIP UA is the Media Application Server (MAS).

SIP proxy server

The SIP proxy server provides location services (resolves SIP AOR to actual IP addresses or resolves them to a proxy closer to the target endpoint).

If the proxy does more than simple address resolution (for example, call services), it is referred to as the application server, call server, or similar label.

SIP registrar server

The SIP registrar server

- accepts SIP REGISTER sessions from end points who announce their location
- can challenge and authenticate the user

SIP presence server

The SIP presence server

- accepts SIP PUBLISH sessions from endpoints that announce thee current state (such as Busy, Away from Desk, or On the Phone)
- allows interested parties to SUBSCRIBE for the user's presence
- sends state updates to interested parties using SIP NOTIFY

SIP media server

The SIP media server

- acts as a SIP endpoint that can perform special media features
- provides functions such as IVR, RAN, Conference, and Media Mixing
- is not a formal entity but is a special type of end user application
- terminates and originates RTP, and SIP signaling

An example of a SIP media server is the MAS.

SIP BBUA

The SIP Back to Back User Agent (BBUA) is two user agents (UAS and UAC) twinned. A session terminates on the incoming user agent and passes to the application for modification or decision tree.

A new session originated on the outgoing user agent is twinned with the incoming user agent for the duration of the call.

The SIP BBUA provides a mechanism for applications to sit in the middle and influence SIP sessions. (for example, SIP Contact Center).

SIP gateway

The SIP gateway acts as a SIP Protocol Converter:

- SIP to H.323
- SIP to ISDN
- SIP to Analog Trunk
- SIP to 3G324M

Examples of SIP gateways include Communication Server 1000, Audiocodes ISDM Gateway, and Radvision 3G Gateway.

Avaya Communication Server 1000 configuration requirements

This section provides configuration requirements for the Avaya Communication Server 1000. For more information about Avaya Communication Server 1000 integration, see *Avaya Aura™ Contact Center Configuration – Avaya CS1000 Integration* (NN44400-512).

Navigation

- Configure CDNs (page 161)
- Configure Communication Control Toolkit phones (page 162)
- Engineer the telephone switch for multimedia (page 163)

Configure CDNs

Controlled Directory Numbers (CDN) are specialized ACD-DNs or queues on the telephone switch. Contact Center Manager Server can control CDNs. Only one application can control a CDN at a time. However, Contact Center Manager Server can monitor CDNs controlled by other applications.

You must configure CDNs on the telephone switch, and in the Contact Center Manager Server. This section describes how to configure CDNs on the telephone switch.

Prerequisites

- You know the user ID and password to log on to the telephone switch administration terminal.
- You are familiar with telephone switch Change and Diagnostics overlays.
- You have a list of available CDNs (LD 23).

Attention: Do not enter a VSID definition on CDNs.

Configuring a CDN with LD 23

Use these prompts and responses in Overlay 23. For prompts that are not specified in the following table, press Enter.

Prompt	Response	Description
REQ	NEW	Add a CDN.
TYPE	CDN	Control DN data block.
	(1 of 2)	

Prompt	Response	Description
CUST	0–99	Customer number.
CDN	xxxx	Controlled Directory Number.
RPRT	NO	Deactivate the report control option.
DFDN	xxx(xxxx)	Default ACD-DN (DN to which calls are routed if a problem occurs with Contact Center Manager).
CNTL	YES	DN is controlled by Contact Center Manager.
REQ	END	Exit from overlay.
	(2 of 2)	

After you configure the CDNs, continue with the following steps:

- If you use a non-SIP contact center, configure the CDN using Contact Center Manager Administration. See *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611). Ensure that you select DN Monitored.
- Configure the CDNs. For more information about configuring CDNs, see *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).
- When you develop the application, use the appropriate API call to acquire the CDN.

Configure Communication Control Toolkit phones

Use Overlay 11 to configure phones for use with Contact Center Manager Server. Follow these guidelines:

- Configure the AST value for the phone to the key to be monitored by Communication Control Toolkit and Contact Center Manager Server. For example, if the keys you choose to control are 00 and 03, set the values for 00 and 03.
- Assign a value of 1 to IAPG.
- To have other Contact Center Manager Server call control features, such as transfer and conference, program these features on the phone.

Attention: Limitations in the Meridian Link Services (MLS) protocol prevent the Service Provider from supporting the following keys: Call park/unpark, No-hold conference call, and Pickup.

Next steps

- Configure the phone using Phoneset and Voice Ports in Contact Center Manager Administration. See *Avaya Aura™ Contact Center Manager*

Administration – Client Administration (NN44400-611). Ensure that you select DN Monitored.

- Configure the phone in Communication Control Toolkit (CCT) using the CCT Web Administration. For more information about configuring CCT, see *Avaya Aura™ Contact Center Commissioning* (NN44400-312)

Engineer the telephone switch for multimedia

This section provides an overview of the Contact Center Multimedia telephone switch requirements.

Before you install the Contact Center Multimedia components, you must ensure that the telephone switch is configured properly with:

- agent phones configured with for Communication Control Toolkit control
- ACD and DN keys on agent phone configured for Communication Control Toolkit control

An e-mail agent with a telephony toolbar needs at least one ACD key configured.

This section provides samples of the setup of the agent TNs on the telephone switch to allow Communication Control Toolkit control.

Complete the checklists in this section to ensure that your telephone switch meets all the requirements for Contact Center Multimedia.

Supported telephone switches

Contact Center Multimedia relies on Communication Control Toolkit for switch support. For more information, see Communication Control Toolkit configuration requirements (page 113).

For more information about which telephone switches are supported, see Telephone switch comparison (page 41).

Configuring agent phones

Contact Center Multimedia requires Communication Control Toolkit on all of the agent computers so the agent user interface can control the status of the phone. This configuration is the same as the standard Communication Control Toolkit configuration for the agent phone.

See the following table for a checklist of tasks that you need to perform when you engineer phones (TNs) for use with Communication Control Toolkit (CCT).

Avaya Communication Server 1000 checklist for agent phones

Avaya Communication Server 1000 for the agent	X
Ensure Open Queue feature is enabled on Contact Center Manager Server.	
Create a TN entry for each contact center agent, following the instructions in the Contact Center Manager documentation.	
Ensure that key 0 has ACD functionality.	
If you enable Outbound, ensure that you create a personal DN key on the contact center agent phone.	
Enable Associated Set Assignment (AST) for the ACD key and for one of the other personal DN keys. You can configure a maximum of 2 AST keys	
Ensure that IAPG is enabled.	

Avaya Communication Server 1000 voice processing system configuration requirements

This section describes how to determine the number of voice ports required to provide voice processing services to Contact Center Manager Server as well as the requirements for Avaya CallPilot™.

Navigation

- Voice Port usage (page 165)
- ACCESS requirements (page 166)
- Contact Center Voice Services on Avaya CallPilot requirements (page 166)

Voice Port usage

The number of voice ports required depends on:

- the rate of port requests
- the duration of voice sessions
- the Grade of Service (GOS)

Grade of Service refers to the probability that requests are delayed by more than a certain number of seconds. For Avaya CallPilot, the standard GOS used is 5 percent probability that the calls are delayed for more than six seconds, and 95 percent of the calls incur a delay of less than six seconds.

Voice ports must be dedicated to Contact Center Manager Server. They cannot be shared with other services.

ACCESS port usage

Contact Center Manager Server can support a single ACCESS connection to control voice processing. A single ACCESS connection supports up to 191 voice ports. This can limit Contact Center Manager Server performance by limiting the rate of calls that require Contact Center Manager Server control of voice processing. The following conditions apply:

- Avaya CallPilot supports a maximum of 191 voice ports. However, one voice port must be reserved for messaging. Therefore, 191 voice ports provide voice services for Contact Center Manager Server.
- None of the predefined applications (and, therefore, workloads) require controlled voice services; therefore, none result in ACCESS traffic.

Non-ACCESS port usage

Contact Center Manager voice services that do not require local voice port control (such as Give IVR) do not result in ACCESS usage and, therefore, are not subject to the 192-port limitation. Additional voice ports may be required, however, to support these services.

ACCESS requirements

Contact Center Manager Server generates ACCESS traffic when it communicates with the integrated voice processing system (Avaya CallPilot) to obtain the following controlled voice services:

- Give Controlled Broadcast command
- Collect Digits command
- Open/Close Voice Session commands

For Contact Center Voice Services on Avaya CallPilot, ACCESS traffic travels on the ELAN subnet.

Contact Center Voice Services on Avaya CallPilot requirements

The following sections detail requirements for Contact Center Voice Services on Avaya CallPilot.

Avaya CallPilot platforms

Contact Center Voice Services requires Avaya CallPilot Release 3.0 or later. Avaya CallPilot Release 5.0 supports the following platforms;

- 201i IPE
- 202i IPE
- 703t Tower
- 1002rp Rackmount
- 600r Rackmount
- 1005r Rackmount

The following table shows some of the Avaya CallPilot platforms, the number of channels available on each of these platforms, and the maximum centum call seconds (CCS). Centum call seconds are equivalent to 100 call-seconds.

Avaya CallPilot resources

Avaya CallPilot platform	Maximum voice channels	Maximum CCS Erlang C	Maximum CCS Erlang B
201i	40	1183	1116
703t	96	3120	3028
1002rp	192	6515	6417

Avaya CallPilot and multiple servers on the same telephone switch

If you use Avaya CallPilot to provide front-end IVR, the same Avaya CallPilot can support all of the up to three Contact Center Manager Server systems connected to the same telephone switch.

If you use Contact Center Voice Services on Avaya CallPilot—that is, if Avaya CallPilot is providing Give IVR or ACCESS voice services (Open/Close Voice Session, Collect Digits, and Give Controlled Broadcast)—Avaya CallPilot can serve only one Contact Center Manager Server. Therefore, each Contact Center Manager system must connect to a separate Avaya CallPilot.

On a Communication Server 1000E switch, Give Controlled Broadcast requires additional media card ports in the MG 1000E hosting the Avaya CallPilot server. For more information, see the *Avaya Aura™ Contact Center Configuration – Avaya CS1000 Integration* (NN44400-512).

CPU impact

Contact Center Voice Services on Avaya CallPilot uses MLS for communication between Avaya CallPilot and Contact Center Manager. To estimate the additional CPU load generated by Contact Center Voice Services on Avaya CallPilot, use the CapTool application.

ELAN subnet impact

For Contact Center Voice Services on Avaya CallPilot, ACCESS traffic is carried on the ELAN subnet or over the contact center subnet. In the embedded LAN (ELAN) subnet situation, the CapTool application automatically determines the additional load on the ELAN subnet.

Contact center subnet impact

Contact Center Voice Services on Avaya CallPilot results in additional MLS traffic on the contact center subnet. When you use CapTool to assess capacity in an environment with Contact Center Voice Services on Avaya CallPilot, the application automatically calculates the impact of the additional MLS traffic on bandwidth.

Contact center e-mail server configuration requirements

You can use Contact Center Manager Administration to configure mailboxes, general settings, and rules that are required and optional for routing e-mail messages.

This section provides an overview of the e-mail server requirements, including the use of aliases. Contact Center Multimedia pulls e-mail from any POP3/SMTP compatible e-mail server. It polls the mailboxes at specified intervals.

Navigation

E-mail server requirements

Contact Center Multimedia uses the POP3/SMTP protocols to retrieve and send e-mail. You must enable these protocols on your mail server. Contact Center Multimedia can support SMTP Authentication, POP3/SMTP over SSL, and the use of nonstandard ports for these protocols. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).

Configure the e-mail settings

Use the E-mail General Settings window to configure the following settings:

- The Mailbox Scan Interval is the interval between the scans made to the E-mail server to check for new e-mail messages. The default value is 60 seconds.
  - — Configure the specific intervals in the Contact Center Multimedia Administrator application.
- The Attachment Files are the locations on the Contact Center Multimedia server where the attachments to e-mail messages are stored. A URL is provided for agents to access the folder on the Web server. These values are provided by default.

  To change these folder names, you must ensure that the new folder exists on the file system with the correct path to the folders, the folder is shared, a parallel IIS virtual folder is created, and that all of the permissions are correct. No verification is performed in the Contact Center Multimedia

Administrator application to ensure that the new values are correct, so the values need to checked carefully. The default values for the folder, where <Server name> is the name of the Contact Center Multimedia server, are:

— Inbound URL: http://<Server name>/inboundattachment

— Inbound Share: \\<Server name>\inboundattachment

— Outbound URL: http://<Server name>/outboundattachment

— Outbound Share: \\<Server name>\outboundattachment

CAUTION:

CAUTION

Risk of backup failure

Avaya recommends that you use the default attachment locations defined during installation. If required, you can choose a different location for the inbound and outbound shared e-mail folders. If you choose a different location, you must ensure that you perform the following activities: 1) Create the inbound e-mail attachment folder with the path MailAttachment/Inbound. 2) Create the Outbound folder with the path MailAttachments/Outbound. 3) Share the inbound and outbound folders with the users CCMMOPSUSR and IUSR_<Servername>. 4) Configure the folders in the E-mail attachment locations in the Contact Center Multimedia Administrator application.

- The AutoNumber Outgoing Email is the customer identification number and can optionally be included in the message subject of all e-mail messages.
- The Include E-Mail Body in Keyword Search specifies the keyword search for rules is applied to both the subject and the body of the e-mail message. You can also select the number of characters in the e-mail message to search.

Using aliases

An alias is an alternative name for a mailbox. Sending an e-mail to either an alias or the mailbox itself has the same result; that is, the e-mail is stored in the same place.

For example, if you have a mailbox named sales@avaya.com. This mailbox has two aliases—contactcentersales@avaya.com and mcssales@avaya.com. If you send an e-mail to either one of these addresses (sales@avaya.com, contactcentersales@avaya.com, mcssales@avaya.com), the e-mail is sent to the same destination, which is sales@avaya.com.

Why use an alias?

Aliases are useful for e-mail filtering. For example, if an alias address is defined for only a short promotion period, you can discard any e-mail that arrive at that alias after the promotional time has passed.

What is the impact of alias addresses on Contact Center Multimedia?

Alias addresses are a useful pre-routing tool for e-mail. Given the example in the previous section, you can configure three e-mail routing rules. E-mail arriving with an address contactcentersales@avaya.com can be routed to the skillset EM_ContactCenterSales. E-mail arriving with the address mcssales@avaya.com can be routed to the skillset EM_MCSSales. If an e-mail arrives at the address sales@avaya.com, you may not be sure of its content (at least without further keyword searching); therefore, route it to a general skillset such as EM_DefaultSales.

Configuring an alias within Contact Center Multimedia

As an alias is only an alternative name for a mailbox, it is not polled. Therefore, Contact Center Multimedia must be aware of all possible aliases to ensure powerful routing. Define an alias in the same way as a physical mailbox. The only difference is you select the alias radio button rather than the enabled button. This informs Contact Center Multimedia that this is an alias address and there is no physical mailbox to poll. The e-mail itself is retrieved from the physical mailbox the alias is associated with. When you define all the possible aliases (as well as the physical mailboxes) in this list, the aliases become available to the Rules Wizard to selectively apply keyword searching, including address matching and other criteria to make routing decisions.

For more information about defining an alias, see *Avaya Aura™ Contact Center Server Administration* (NN44400-610).

Outgoing e-mail

Configure outgoing e-mail mailbox settings to identify who responds to the customer's e-mail message.

The response can contain the e-mail address to which the customer sent the original e-mail message, or a general corporate e-mail address that is configured for each skillset.

Agent-initiated messages are always sent from an e-mail address associated with a skillset.

After you define the rules for e-mail routing, all e-mail are routed to a skillset. To determine the mailbox that is set as the originator, map the skillset to a mailbox. For detailed information, see *Avaya Aura™ Contact Center Commissioning* (NN44400-312).

Mailbox requirements

Contact Center Multimedia logs onto nominated mailboxes on your mail server and retrieves e-mail at defined intervals. E-mail is then routed to agents. To route an e-mail, Contact Center Multimedia requires the mailbox name and password. In addition, Contact Center Multimedia requires the possible alias names used for a mailbox to ensure correct routing of e-mail.

Determining capacity requirements

Your contact center infrastructure must meet the minimum requirements specified in this section before you attempt to install the Avaya Aura™ Contact Center software.

Navigation

Contact Center Manager Server Call load

Call complexity and call rate determine the CPU or memory resources required to process the call load.

Call complexity

Call complexity is the number of each type of service used by a call.

Expected resource consumption

Over a period of time, you can use the average number of each type of service for each call to estimate the expected resource consumption. For example, if a typical call queues to an average of two skillsets, the expected resource cost for each call is two times the cost of queueing a call to one skillset (provided that the costs are a linear function of call rate).

Cost of call services

To estimate the resource consumption on Contact Center Manager Server for different call rates, you must define the cost of a basic call, as well as the costs associated with the most typical call operations. These costs are measured and are incorporated in the Capacity Assessment Tool (CapTool) calculations.

The following conditions apply:

- The cost of a basic call is the resource consumption incurred due to basic call processing (assuming that the agent answers immediately).
- The default value for call rate is based on a holding time of three minutes. For example, if you enter 500 logged-on agents in the CapTool, the default value for call rate equals 180, which is 10 000 CPH.

The following table lists common call services and indicates the typical cost used for each call in the hybrid or typical call model for the Avaya Communication Server 1000 and SIP.

Call service and cost per call

	Avaya Communication Server 1000	**SIP**
Parameter	Services for each call	Services for each call
Basic Call	1	1
Queue to Skillset	2	2
Queue to Agent	0	0
Give Controlled Broadcast (S/S)	1	N/A (see Notes)
Voice Services Collect Digits	0	0
Give IVR	1	2
Give RAN	2	2
Give Music	1	1
HDX Send Info	1	1
Voice Services Collect Digits	0	0
Give IVR	1	2
Give RAN	2	2
Give Music	1	1
HDX Send Info	1	1
HDX Request/Response	1	1
Intrinsics	5	6
If/Then’s Executed	5	5
If/Then’s Executed	5	5

(1 of 2)

Call service and cost per call

	Avaya Communication Server 1000	SIP
Proportion of Calls Transferred	5%	5%
Proportion of Calls Conferenced	5%	5%
Proportion of Calls Transferred to a DN	N/A	N/A
MLS Screen Pops	1.2	N/A
MLS Messages	0	N/A
Queue to Network Skillset	2	N/A (see Notes)
(2 of 2)		

Call load table notes:

- The number of services for call is an average value taken over all inbound calls (or outbound calls, if that is the context). See the examples presented in Contact Center Manager Server services performance impact (page 197).
- Give Controlled Broadcast (S/S) and Queue to Network Skillset for SIP are not supported in this release.

Call rate

Call rate is the average rate of calls processed by the server. The call rate is measured in Calls Per Hour (CPH) and is a function of the average Call Arrival Rate and Mean Holding Time (MHT).

Mean Holding Time is the time the agent spends serving a call. MHT is the sum of:

- average talk time
- time required for post-call processing, when the agent is not available to handle other calls
- inter-call interval (including union break time, if any)

Under heavy call loading, or during the busy time, when there is no agent idle time, Mean Holding Time is equal to Mean Time Between Calls (MTBC). (These definitions apply to both inbound and outbound calls.)

Call rate, number of active agents, and MHT are related. Given the same call rate, the more agents there are, the longer the MHT can be. For example, if the call rate is 60 CPH and only one agent is available, the MHT cannot be more than 1 minute. On the other hand, if there are 60 agents for the same call rate, then each agent can take up to an hour, on average, for a call.

The values used in the CapTool to estimate capacity are based on successful call terminations (for example, treatment, available agent, call servicing, call termination), and do not take into account agent activity other than call handling. Use this information to estimate combinations of call rates and reasonable workloads. For example, 20 agents handling 25 000 CPH spend, on average, no more than three per call. This is probably unreasonable for a human agent but may be acceptable for an automated voting application.

Contact Center Manager Server Capacity estimation

This section shows how the Contact Center Manager Server capacity varies with different call loads and standard workloads on a stand-alone server. The performance metrics are the outputs from the capacity models (the same ones used in the CapTool), which are based on controlled measurements (calibration measurements), as well as high-capacity testing validation results.

Rated capacity for call processing for different processors

Rated capacity is the maximum load that can be sustained at steady state, such that the average CPU use does not exceed 50 percent. The capacity limits for different hardware platforms and different Mean Holding Times (MHT) are shown in the following table.

This information applies to Avaya Communication Server 1000, but does not apply to SIP.

For these calculations, the following assumptions are made:

- There is one Web client for 10 agents logged onto the system. For *n* agents logged onto the system, the number of Web clients is equal to Ceiling(n/ 10).
- The Contact Center Manager Server networking is not enabled
- The RSM is on
- There is no Standby Server available
- There is no networking available
- There are no Real-time API applications
- The call complexity model is the standard one given in Contact Center Manager Server Call load (page 173).
- All parameters are scaled according to number of agents logged on to the system.

Rated capacity for call processing

Processor	MHT (minutes)	Agents	Peak call rate (CPH)
Dual Xeon 2.8 GHz	2	2454	73 620
	3	2719	54 380
	4	2868	43 020
Dual Xeon 3.4 GHz	2	2846	85 280
	3	3128	62 560
	4	3286	49 290

Peak sustainable capacity

The following table shows the upper limit on processing calls with the same standard call model and assumptions used in the previous section.

Peak sustainable call rates

	Peak sustainable call rates for different standard workloads at 50 percent CPU use (CPH)		
Processor	**1000 active agents**	**2000 active agents**	**3000 active agents**
Dual Xeon 2.8 GHz	120 000	97 500	28 125
Dual Xeon 3.4 GHz	No practical upper limit	135 000	67 500

Contact Center Multimedia disk storage requirements

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

For more information about database requirements, see *Avaya Aura™ Contact Center Installation* (NN44400-311).

Required database files

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

- CACHE.DAT in the Avaya\Contact Center\Databases\CCMM\MULTIMEDIA\DATA folder. This stores the Contact Center Multimedia data.
- Avaya\Contact Center\Journals folder is created during installation. This folder contains the Database Journal Files, which are used for Geographic Redundancy.

- Avaya\Contact Center\ShadowJournals folder is created during installation. This folder is used if Geographic Redundancy is configured and this server is running as the Redundant server.

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

The CACHE.DAT file grows dynamically as the volume of data in the database grows. Initially it is just under 45 MB. One million contacts take approximately 20 GB of space.

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

E-mail attachment storage

E-mail attachments are stored in the attachment folder. The disk space required to store attachments is calculated as

Disk space for e-mail attachments in MB
= number of e-mail messages per day
* percent with attachment
* average attachment size in MB
* number of days before purging

Example

Following is the disk storage calculation for a contact center that receives 9000 e-mail messages every day, where 30 percent of the e-mail messages have an attachment averaging 0.5 MB in size, and attachments are stored for 10 days before they are deleted.

Disk space for e-mail attachments in MB
= 9 000 * 0.3 * 0.5 * 10
= 13500 MB

Maximum number of days before purging or archiving

The maximum number of days before you must purge or archive the database can be determined given the total amount of disk space in GB available (TGA):

$$ndp_{Max} = \left\lceil \frac{2\,000\,000 * TGA}{5 * ntx + 12 * nts + 12 * nemd} \right\rceil$$

where

- ndp_{Max} is the maximum number of days before you must purge or archive the database
- *ntx* is the number of transaction records each day
- *nts* is the number of text chat sessions each day
- *nemd* is the number of e-mail sessions each day, which is calculated as (# of e-mail/agent/day)*(# of agents)
- $\lceil\ \rceil$ is the ceiling function (least integer greater than or equal to the expression

Attention: When you purge the database, you permanently remove the information from the database. Also, you can use the Dashboard utility to monitor the services in your system. For more information, see *Avaya Aura™ Contact Center Server Administration* (NN44400-610).

Example

If, on an average daily basis, there are 20 000 transaction records, 4000 text chat sessions, and 5000 e-mail sessions with no attachments, the maximum number of days that can be tolerated before purging for a 10 GB (10.24) disk space availability is given as

$$ndp_{Max} = \left\lceil \frac{2\,000\,000 * 10.24}{5 * 20\,000 + 12 * 4000 + 12 * 5000} \right\rceil = \lceil 98.5 \rceil = 99$$

Communication Control Toolkit capacity

The call capacity is 100 000 simple calls per hour (CPH) with data for a maximum of 5000 agents. Self service supports an additional 16 000 CPH running on the IVR lines.

Agent counts are 5000 agents (5000 terminals, 10 000 addresses) if call data is not required or 1600 agents (1600 terminals, 3200 addresses) if call data is used. Self Service supports an additional 1000 IVR lines.

The performance of a standalone Communication Control Toolkit server depends on a number of factors, including:

- number of resources (terminals, addresses, and users)
- number of clients
- number of calls per hour, call duration, and call complexity—transfers, conferencing, and attached caller-entered data all increase call complexity, and, therefore, the resources required to process a call

- amount of call-attached data (see the following section)
- hardware configuration (processor speed, memory, and disk space available)
  - For more information about hardware platforms, see Server hardware requirements (page 119).
- type of solution (Communication Control Toolkit, CCT-IVR, or both)
  - A system running both Communication Control Toolkit and CCT-IVR requires more system resources than a system running only Communication Control Toolkit or CCT-IVR.

To calculate the hardware requirements for your environment, use the CapTool application. For more information, see the *CapTool User's Guide*.

You can download the CapTool software utility from the support Web site (www.avaya.com/support).

CTI application performance impact

Meridian Link Services (MLS) can be used in a contact center environment. It is an intelligent signaling link offering computer-telephony integration (CTI) applications access to Avaya Communication Server 1000 call processing functions.

If you use MLS with Communication Control Toolkit, there is an impact on Contact Center Manager Server performance.

Single server capacity

The capacity (in terms of logged-on agents and calls per hour) supported by a single server is less than the capacity of a stand-alone server running on the same hardware platform.

The following restrictions apply to single servers.

- A single server with Contact Center Manager Server, Contact Center Manager Administration and Communication Control Toolkit has an agent limit of 1000 active agents.
- A single server with a SIP-enabled Contact Center Manager Server, Contact Center Manager Administration and Communication Control Toolkit has an agent limit of 200 active agents.
- A single server with Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit and Contact Center Multimedia has an agent limit of 600 active agents.
- A single server with a SIP-enabled Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit and Contact Center Multimedia has an agent limit of 200 active agents.

- A single server supports 20 000 calls per hour.
- A single server SIP-enabled Contact Center supports 4000 calls per hour.

You can use the CapTool application to determine the hardware requirements for a single server.

Maximum capacity values

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

The following conditions apply to the table:

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

Contact Center capacity

Parameter	SIP maximum	AML maximum
General parameters		
Number of logged-on voice agents: Configurations with greater than 1500 agents require special consideration for contact center subnet bandwidth and disk requirements. The maximum of 5000 logged on agents is only applicable for the Communication Server 1000 Release 5.0 (or later) with Pentium IV CPUs.	Avaya Communication Server 1000 based SIP: 1500 Avaya Aura™ Unified Communications platform based SIP: 1000 Avaya Aura™ Solution for Midsize Enterprises based SIP: 300	5000
Number of logged-on multimedia agents. (No voice agents on AACC in this configuration)	Avaya Communication Server 1000 based SIP: 1500 Avaya Aura™ Unified Communications platform based SIP: 1000 Avaya Aura™ Solution for Midsize Enterprises based SIP: 300	3000

Contact Center capacity

Parameter	SIP maximum	AML maximum
Number of agents defined in the system	6000	10 000
Number of phones: Communication Server 1000	 10 000	 10 000
Number of supervisors logged on	150	600
Number of supervisors defined in the system The number of configured supervisors defined in the system is not limited, but Avaya tests only up to 300 configured supervisors.	600	600
Number of scripts The number of scripts defined in the system is not limited, but Avaya tests only up to 1500 scripts.	1500	1500
Number of active scripts The product contains three predefined scripts. Therefore, you can create 997 scripts.	1000 (997)	1000 (997)
Maximum script size—Master_Script (characters)	100 000	100 000
Maximum script size—other scripts (characters)	50 000	50 000
Number of applications (that is, exit points from the Master_Script) The product contains five predefined applications. Therefore, you can create 800 applications for Release 6.0 or 1000 applications for the current release.	805 (800)	1005 (1000)
Number of call variables	100	100
(2 of 7)		

Contact Center capacity

Parameter	SIP maximum	AML maximum
Number of skillsets The maximum includes both local skillsets and network skillsets.	1500 (1496) The product contains four predefined skillsets. Therefore, you can create 1496 skillsets.	1500 (1493) The product contains up to seven predefined skillsets, depending on what is licensed on your server. Therefore, you can create 1493 skillsets.
Number of skillset priority levels	48	48
Number of skillsets for each call	20	20
Number of activity codes The product contains three predefined activity codes. Therefore, you can create 9997 activity codes.	10 000 (9997)	10 000 (9997)
Inbound voice calls per hour The number of inbound calls per hour at 33000 and 100000 assumes a hold time of three minutes. For shorter call durations, higher call rates can be supported. See the CapTool to optimize the engineering of your configuration.	Avaya Communication Server 1000 based SIP: 24000 Avaya Aura™ solution based SIP: 6000	100 000
Inbound Multimedia contacts per hour	12 000	12 000
Number of waiting calls	3000	3000
Call resources parameters		
Number of IVR queues (Communication Server 1000)	150	150
Number of IVR ports	1000	1000
Number of ACCESS ports (Avaya Communication Server 1000)	NA	191
Number of routes	513	513
Number of trunks (Avaya Communication Server 1000) Avaya only tested 1000 trunk members. Avaya has no plans to test the 4400-trunk limit.	4400	4400
Number of CDNs	750	750

Contact Center capacity

Parameter	SIP maximum	AML maximum
Number of RAN and music routes	512	512
Number of DNISs	10 000	10 000
Assignment parameters		
Number of agents in an agent-to-supervisor assignment	1000	1000
Matrix size for agent-to-skillset assignments This parameter is the supported matrix size for displaying agent-to-skillset assignments. An agent-to-skillset assignment contains a matrix with a row for each agent in the assignment, and a column for each skillset to which the agents belong. The matrix size is the number of agents multiplied by the number of skillsets. This parameter works in conjunction with the Number of agent-to-skillset reassignments in an agent-to-skillset assignment parameter. Even though this window allows a 5000 element matrix to be displayed, non-blank elements in the matrix should not exceed the parameter Number of agent-to-skillset reassignments in an agent-to-skillset assignment (that is, the maximum number of agent-to-skillset reassignments in a single agent-to-skillset assignment is 1000).	5000	5000
(4 of 7)		

Contact Center capacity

Parameter	SIP maximum	AML maximum
Number of agent-skillset reassignments in an agent-to-skillset assignment In an agent-to-skillset assignment, you can change an agent's status for multiple skillsets. For example, you can put the agent James Jones on Standby for the skillset Bookings, and give him priority 1 for the skillset European Vacations. Thus, you have two reassignments for the agent James Jones in the agent-to-skillset assignment.	1000	1000
Networking parameters		
Number of call processing nodes in the network (including local node) The number of configured nodes is 30; however, only 20 nodes can be configured in the routing table.	30	30
Number of network skillsets The maximum includes the predefined skillsets, local skillsets, and network skillsets.	1000	1500
Number of skillsets per agent	150	150
Number of sites in the routing table for a network skillset	20	20
Number of network skillsets to which a call is queued	10	10
Number of agent reservation requests per call	30	30
Number of remote applications (applications accessible over the network)	6000	6000
Network calls per hour for which CBC data is collected	10 000	10 000
Number of target nodes	20	20
Real-time display parameters		
Number of RTD screens	4	N/A

Contact Center capacity

Parameter	SIP maximum	AML maximum
Database parameters		
Number of client PCs and RTI applications connected to the database	100	100
Number of other applications connected to the database	100	100
Number of Fault Management messages in database	7500	7500
Maximum number of report clauses The database server supports a maximum of 255 clauses on a single SQL statement.	255	255
Third-party interface parameters		
Number of MLS applications	16	16
Number of MLS DN registrations across all MLS applications	5000	5000
Number of MLS calls per hour The number of MLS calls per hour at 58,000 and 68,000 assumes a hold time of three minutes. For shorter call durations, higher call rates can be supported. Refer to the CapTool to optimize the engineering of your configuration.	58 000	58 000
Number of HDX connections When configured, Database Integration Wizard (DIW) uses a single HDX connection.	10	10
Number of RTI client systems/ applications	100	100
Other parameters		
(6 of 7)		

Contact Center capacity

Parameter	SIP maximum	AML maximum
Number of scripts activated under load Script activation supports activation cascading, where the activation of a parent script forces activation of all lower level scripts. Do not use this feature on a system under load. Under load, activate scripts from the lowest level up, with the Master script activated last.	1	1
Steady state CPU	70%	70%
Number of servers per Communication Server 1000 Number of AML-based application servers per Communication Server 1000	3 16	3 16
(7 of 7)		

Access from an external client PC

When you use an external client PC to access Contact Center Manager Administration (CCMA) on a single server, Avaya recommends that you limit the number of on-demand and scheduled historical reports run on the co-resident server. Running historical reports can increase the CPU use on the server.

Access from a browser on the single server

When you access Contact Center Manager Administration from a browser on the single server, Avaya recommends that you limit the number of ad hoc and scheduled historical reports run on the single server. Running historical reports can increase the CPU use on the server.

In addition, Avaya recommends that you limit the number of real-time displays that you start. Viewing real-time displays also increases the CPU use on the server.

SIP capacity estimation

The following table shows the peak sustainable capacity, or upper limit, on processing calls using the standard call model.

SIP capacity

	Peak sustainable call rates for different standard workloads at 50 percent CPU use (CPH)		
Processor	**100 active agents**	**500 active agents**	**1500 active agents**
Quad Xeon 2.8 GHz	100 000	50 000	25 000

Avaya Communication Server 1000 telephone switch capacity

The capacity of Contact Center Manager Server is a factor of both Contact Center Manager Server and the physical capacity of the telephone switch. The call throughput of Contact Center Manager Server depends on several factors, including the following:

- rated capacity of the telephone switch
- call complexity
- Contact Center Manager Server hardware platform and configuration
- LAN speed
- total LAN traffic

You can use the Networks Enterprise Configurator (NEC) to calculate call throughput for the Avaya Communication Server 1000 telephone switch. It is used to perform Avaya Communication Server 1000 CPU calculations for users in North America and the Caribbean and Latin America (CALA).

How switch capacity is calculated

Trunks normally operate at 28 CCS (busy for 2800 seconds during an hour) and ACD Agents typically operate at 33 CCS (3300 seconds busy during an hour). Therefore, more trunks than agents are required to keep the agents busy (approximately 18 percent more trunks than agents). The number of trunks a site provisions depends on what the busy hour (incoming calls) volume is and how full queues become, for example, do you want customers in a queue getting music or getting a busy signal from the Central Office because the trunks are busy. The model suggests the use of 50 percent more trunks than agents. You can use a different ratio.

Because agents are busy for 3300 seconds during an hour and call duration is an average of 3 minutes (180 seconds), that means each agent handles 3300/180=18.3 calls an hour. This implies that for 5000 agents (the maximum number currently supported), there are 91 500 agent handled calls an hour.

Each trunk can handle 15.6 calls an hour (2800/180). Therefore, to handle the 91 500 agent calls requires conservatively 3930 trunks. Thus a site with a trunk/agent ratio of 1.5 needs (5000 x 1.5)-3930=3570 trunks to queue calls. In the worst case, this means treating queued calls at the rate of 15.6 x 3570 or 55 692 CPH).

The CPU calculation must take into account the treatment that the extra trunks generate (the total number of calls depends on how long the queue wait time is, so this becomes difficult to determine). It is up to you to determine what treatment these calls receive, what load factor is used for them, and are how they are handled by Contact Center Manager.

The worst case is that the extra trunks queue calls at the maximum rate. This means there are a total of 78 387 calls on system at full capacity.

If you use the hybrid treatment, with a load factor of 8.78 and include the trunking factor of 1.6 and a misc. load of 0.25, you have a load factor of 10.63 per call. So for 5000 agents with a 1.5 trunk ratio, there are 78 387 x 10.63=833 254. This results in a total CPU load of (833 254/880 000) of 95 percent, hence the hybrid solution of 5000 agents at 100 percent CPU usage.

Rated capacity of the telephone switch

The capacity of the telephone switch is specified as the number of Equivalent Basic Calls (EBC) per hour. An EBC is a measure of the telephone switch CPU real-time required to process a basic call. For an IP system (Communication Server 1000E), a basic call is defined as a simple unfeatured call between two phones, on the same telephone switch, using a four-digit dialing plan.

The EBC capacity of the telephone switch depends on the processor type, as shown in the following table.

Telephone switch capacity

Telephone switch	Capacity
SSC (Communication Server 1000M, Communication Server 1000S)	42 000 (no IP expansion) 35 000 (with IP expansion)
CP3 (Communication Server 1000M)	72 000
CP4 (Communication Server 1000M)	100 900
CP-PII (Communication Server 1000M))	315 000
CPP4 (Communication Server 1000M)	1 006 000
(1 of 2)	

Telephone switch capacity

Telephone switch	Capacity
CP-PII (Communication Server 1000E, Communication Server 1000M pure IP)	210 000
CPP4 (Communication Server 1000E, Communication Server 1000M pure IP)	880 000
(2 of 2)	

Quoted EBC or BHCC capacity for Communication Server 1000M configurations are for TDM solutions and for Communication Server 1000E are for IP solutions.

Call complexity

The complexity of a Contact Center Manager call is defined as the number of each type of service used by the call. All calls have an EBC cost, with calls of greater complexity (that is, using a greater number of services) costing more EBCs.

For example, a basic call costs 2.40 EBC; Give Music costs 0.25 EBC; Give IVR (including transfer) costs 2.29 EBC. Therefore, a call that receives IVR and Music treatments costs

2.40 + 0.25 + 2.29 = 4.94 EBC

To quantify levels of call complexity, Avaya has defined several call models, which represent simple, complex, and front-end IVR systems. You can calculate the EBC cost using the Enterprise Configurator (EC).

Simple model: Front-end IVR system

In this call model, the IVR system handles IVR processing. Therefore, the cost of IVR processing is removed from the telephone switch. The following table shows the number of each type of treatment per call in this model.

Treatments per call

Service name	Number of treatments per call
Queue to Skillset	2
Give RAN	0
Give Music	1
Intrinsics Accessed	5
If-Then-Else Executed	5
(1 of 2)	

Treatments per call

Service name	Number of treatments per call
Intrinsics Accessed	5
If-Then-Else Executed	5
(2 of 2)	

Attention: The EBC cost of this call is 3.28 EBC. If Avaya CallPilot™ is used, it adds an additional EBC cost because of MLS processing.

Average complexity model: typical (hybrid complexity model)

This call model uses features from both Contact Center Manager and the telephone switch. The following table shows the number of each type of treatment per call.

Treatments per call

Service name	Number of treatments per call
Queue to Skillset	2
Give Controlled Broadcast Start/Stop	1
Give IVR	1
Give RAN	2
Give Music	1
HDX Send	1
HDX request/Response	1
Intrinsics Accessed	5
If-Then-Else Executed	5

Attention: The EBC cost of this model is 8.78 EBC. If Avaya CallPilot is used, the EBC cost is 15.49 due to MLS processing.

Complex model: Contact Center Voice Processing

The following table shows the number of each type of treatment per call under this model.

Treatments per call

Service name	Number of treatments per call
Queue to Skillset	2
Give Controlled Broadcast Start/Stop	3
Collect Digits Voice Session	1
Give IVR	1
Give RAN	1
Give Music	1
HDX Send	1
HDX Request/Response	1
Intrinsics Accessed	5
If-Then-Else Executed	5

Attention: The EBC cost of this model is 13.84 EBC. With Avaya CallPilot, the EBC value is 27.37

Maximum achievable call rates

To determine the maximum achievable call rates for different telephone switch models, all contributions resulting from the following parameters must be considered:

- the call complexity
- the MLS commands issued by CTI applications
- any other applications that are communicating with the telephone switch over the ELAN subnet

You can determine the call rate by calculating the total Equivalent Basic Call (EBC) value for all incoming traffic per telephone switch type.

Sample calculations using Enterprise Configurator

The calculations in this section are performed using the Enterprise Configurator (EC).

CPU use greater than 100 percent is not supported. Running a system at 100 percent CPU use does not leave room for growth in phones or adding new features.

The following tables show sample calculations based on these parameters:

- 1.5 trunks per agent

- using published EBC for call type and CPU
- call duration of three minutes or 20 calls per hour per agent

Attention: The numbers in brackets in the following tables are the EBC load factors for the script model. The numbers in brackets in the following tables are the EBC load factors for the script model.

Avaya Communication Server 1000E/
Avaya Communication Server 1000M IP agents - CPP4

	100 percent rated CPU	80 percent rated CPU
Contact Center Voice Processing (13.84)	2300	1850
Hybrid (8.78)	5000	2650
IVR (5.42)	5000	3350
Attention: Assume 1.5 V-trunks per agent is EBC = 880 000 for IP calls.		

Avaya Communication Server 1000M TDM agents - CPP4

	100 percent rated CPU	80 percent rated CPU
Contact Center Voice Processing (13.84)	2200	2150
Hybrid (8.78)	2200	2200
IVR (5.42)	2200	2200
Attention: Assume 1.5 PRI trunks per agent is EBC = 1 006 000 for TDM calls.		
Attention: The Communication Server 1000M (MG) is limited by the number of TDM talkslots, therefore it can support a maximum of 2200 TDM agents.		

Avaya Communication Server 1000E /
Avaya Communication Server 1000M IP agents - CP-PII

	100 percent rated CPU	80 percent rated CPU
Contact Center Voice Processing (13.84)	560	450
Hybrid (8.78)	790	630
IVR (5.42)	1100	875
Attention: Assume 1.5 V-trunks per agent, is EBC = 210 000 for IP calls.		

Avaya Communication Server 1000M TDM agents - CP-PII

	100 percent rated CPU	80 percent rated CPU
Contact Center Voice Processing (13.84)	1200	970
Hybrid (8.78)	1725	1375
IVR (5.42)	2200	1925
Attention: Assume 1.5 PRI trunks per agent is EBC = 315 000 for TDM calls.		

Landing Pads

The Avaya Aura™ Contact Center Web Service Open Interfaces enable self-service systems and third-party applications to transfer a call into a contact center by reserving a Landing Pad on the target contact center; it also allows custom data to be passed with the call. When the Landing Pad is reserved, the call must be transferred to the contact center within 20 seconds.

Typically the time between a successful Landing Pad reservation and actual call arriving at the Landing Pad is between 2 and 4 seconds, depending on the call setup-time over your network.

If one call takes 4 seconds to setup, then the theoretical maximum for equally spaced calls is 900 calls per hour for each Landing Pad.

3600/4 = 900 calls per hour for each Landing Pad.

You must also consider the peak call rate and configure the number of Landing Pads in your Contact Center to handle the anticipated peak call rate. Avaya recommends that you configure one Landing Pad per simultaneous call, if you want to handle 70 simultaneous calls then configure at least 70 Landing Pads.

Configure at least one Landing Pad per simultaneous call.

If the peak call rate increases above the rate configured for, calls are not lost, but your customers may experience delays in service.

Outbound capacity

Contact Center Outbound components have the following capacity:

- Outbound Campaign Management Tool monitors a maximum of 100 simultaneous outbound campaigns with a maximum of 20 000 contacts (e-mail or outbound) per campaign.
- Agent Desktop processes a maximum of 2500 contacts (e-mail or outbound) per hour to a maximum of 600 agents.

- InterSystems Caché database server and its associated Web services store information for 1 000 000 contacts in a database that is saved on a 20 GB disk.
- Open queue can queue up to 30 000 contacts at one time for routing and reporting.

Using Erlang B

If you have the traffic in centum call seconds (CCS) and the Grade of Service (GOS), you can calculate the number of required lines using the Erlang B formula. The GOS is the probability of finding all lines busy. The standard practice is to take the probability of finding all lines busy as 0.001.

When you have non-blocking cases, the GOS is 0; therefore, lines are always available. To calculate this with Erlang B, use 0.000000001 instead of 0.

Use the following formula to calculate the number of lines you require.

$$Prob = \frac{\frac{erlangs^{M}}{M!}}{\sum_{j=0}^{M} \frac{erlangs^{j}}{j!}}$$

where:

- erlangs is the # CCS/36 (1 erlang = 3600 call seconds or 36 CCS)
- M is the number of lines
- Prob is the probability of a lost call

To use this formula, iterate on M = 1, 2, and so on, until Prob is less than or equal to the GOS. The first M found where Prob is less than or equal to the GOS is the number of required lines.

Alternatively, you can also use a table of Erlang B. (A table of Erlang B is found in most traffic engineering texts.)

Performance optimization

This section provides information about performance optimization.

Navigation

Contact Center Manager Server services performance impact

Contact Center Manager Server services Meridian Link Services (MLS) and Host Data Exchange impact performance. This section describes the performance of these two services, for which many contact centers require detailed information.

Meridian Link Services

Meridian Link Services (MLS) is an intelligent signaling link offering computer-telephony integration (CTI) applications access to Avaya Communication Server 1000 call processing functions.

CTI applications

Many contact center customers require third-party CTI applications that use MLS. Examples of these applications include software phones, Outbound Predictive Dialing, Host Enhanced Routing, and CTI applications such as Agent Desktop.

CPU impact

CapTool helps determine the impact of MLS on Contact Center Manager Server performance. CapTool calculates the CPU impact of issuing passive screen pops, as well as the general impact of MLS usage by applications.

Every CTI application that interfaces with MLS sends messages to and receives messages from the telephone switch. The MLS software on the server takes messages from the application en route to the telephone switch and translates them into the protocol understood by the telephone switch, namely the Application Module Link (AML) protocol. Conversely, messages from the telephone switch en route to the application are translated from the AML protocol

to the Meridian Link Service (MLS) protocol by the MLS software. The Contact Center Manager Server CPU impact, therefore, depends on the rate of exchange of messages between the telephone switch and the application. This message rate is a function of the application and you need it to calculate the CPU usage. When you use CapTool, determine the average number of MLS messages per call for the MLS application.

Example

Consider a predictive dialing application having the following message profile:

Message number	From application to telephone switch	From telephone switch to application
1	MakeCall	
2		Progress (Trunk seized)
3		Progress (Answered)
4	InitiateTransfer	
5		Progress (Ringing)
6		CallOffered
7	Answer	
8		Progress (Answered)
9		AnswerIndication
10		Answer Response
11	CompleteTransfer	
12		Progress (Transfer complete)
13	Release	
14		Release Response

If all outbound calls use this application, the number of MLS messages processed per outbound call is 14. To include the impact due to this application in the CapTool model, enter 14 in the Number of MLS messages per outbound call box on the MLS Services input page.

If only 75 percent of the outbound calls use this application, and the remaining 25 percent use another MLS application with an average of 20 messages per call, the overall average number of MLS messages per call is

(0.75 x 14) + (0.25 x 20) = 15.5

In this case, enter 15.5 in the Number of MLS messages per outbound call box.

Contact center subnet impact

To calculate the network traffic that MLS contributes on the contact center subnet, CapTool requires the average message length. (If you do not know the average message length, use 50 bytes per message.) To calculate the average message length for the preceding example, consider the following table.

Message type	Message length (bytes)	Number per call	Effective length (bytes)
MakeCall	46	1	46
Progress (Trunk seized)	52	1	52
Progress (Answered)	49	2	98
InitiateTransfer	50	1	55
Progress (Ringing)	54	1	54
CallOffered	36	1	42
Answer	28	1	41
Complete Transfer	52	1	52
Progress (Transfer complete)	52	1	52
Release	51	1	51
Release Response	50	1	52
Total		12	595
Average			49

The message lengths in this example do not represent real data.

The average length per call serviced by MLS is 49 bytes. If all calls receive MLS service, enter this value into the MLS message size box on the MLS Services input page.

Host Data Exchange

The host data exchange (HDX) server enables the values of script variables to be sent to or received from a third-party provider application.

The following conditions apply:

- Third-party provider applications reside on a third-party host computer, and, therefore, are often referred to as host applications.
- Avaya provides a provider application that can co-reside with Contact Center Manager Server. The Database Integration Wizard (DIW) provides an

easy-to-use tool for configuring and customizing the Avaya provider application. (Using the Database Integration Wizard can result in additional contact center subnet traffic, so use the CapTool application to help analyze your contact center subnet bandwidth requirements.) For more information, see the *Avaya Aura™ Contact Center Server Administration* (NN44400-610).

For example, a script can

- obtain a credit card number from a caller using IVR
- query the provider application using the HDX API to determine the account balance of the caller
- use the account balance as a variable in the script

An API known as the service provider API enables a Contact Center Manager user to write custom applications (provider applications) that register with the HDX server to handle back-end processing for the script elements.

Two service elements can be invoked in the script:

- Send Info
- Send Request/Get Response

The Send Info command sends data to the provider application or the HDX server. The Send Request/Get Response command sends information to and receives information from the provider application. The Send Request/Get Response operation uses approximately twice as much CPU resources as the Send Info operation.

CapTool can estimate the CPU and contact center subnet load. On the Call Complexity input page, enter the average number of Send Info and Send Request/Get Response commands issued for each call.

This is the average value taken over all incoming calls.

Example

Suppose that the call rate is 20 000 CPH during the peak hour. If 40 percent of incoming calls are treated with the HDX service, and of these calls

- 20 percent use one Send Info command
- 20 percent use two Send Info commands
- 30 percent use one Send Info and one Send Request/Get Response command
- 30 percent use one Send Request/Get Response command

The average number of Send Info commands issued per incoming call is
0.4 x (0.2 + 0.2 x 2 + 0.3) = 0.36

The average number of Send Request/Get Response commands issued per incoming call is
0.4 x 0.3 x 2 = 0.24

Enter these values into the appropriate boxes on the Call Complexity property sheet.

Cautions

If the provider application runs on a slow platform, or if it runs on the same platform as other CPU-intensive applications, the provider application may not be able to handle the Send Request commands quickly enough. As a result, a high volume of messages may become queued in the HDX server. If the queue reaches its size limit, the HDX server terminates the provider session. When this situation occurs, the provider application receives a DXM_SERVER_SHUTDOWN message from the API.

A DXM_SERVER_SHUTDOWN message means either of the following:

- The session is terminated because the provider application is too slow to respond.
- Communication is down because the HDX server is terminated.

If the provider application is too slow, either reduce the incoming Contact Center Manager Server call rate or run the provider application alone on a faster computer.

Guidelines to minimize capacity requirements

The engineering models used to calculate the capacity requirements of your contact center assume that you follow certain guidelines to minimize the load on your server. These guidelines apply to both stand-alone and co-resident servers.

Steady state operation

Steady state refers to an operational state in which average values of the capacity parameters do not change with time. For example, CPU use can vary widely; however, if you examine the average values of CPU use measured at consecutive intervals of 20 minutes, during a period of steady state operation, these average values are approximately the same.

Guidelines for steady state operation

To ensure trouble-free operation of the server, adhere to the following guidelines for steady state operation:

- Processor CPU—Average CPU usage for any interval of 20 minutes during the peak hour under steady state operation must not exceed 50 percent.

- Server RAM memory—Average pages per second (found in the Memory Object of the Performance Monitor) for any interval of 20 minutes during the peak hour under steady state operation must not exceed five.
- Server virtual memory—Committed Bytes (found in the Memory Object of the Performance Monitor) must not exceed 90 percent of the Commit Limit (also found in the Memory Object of the Performance Monitor).
- Physical and virtual memory—The Microsoft recommendations for physical RAM and virtual memory sizing must be adhered to for optimal performance. For more information, see Co-resident configuration requirements (page 133).

Guidelines for non-steady state operation

A number of non-steady state processes can impact the steady state call processing activity of the server. To minimize their impact, Avaya recommends a number of restrictions:

- All non-steady state processes
  - Run only one non-steady state process at any given time.
  - Do not run other applications between 12:00 midnight and 12:30 a.m. During this time, the Historical Data Manager (HDM) service performs data consolidation for monthly, weekly, and daily data. CPU usage for this activity is high.
- Activation of the Master script
  - Do not activate the Master script during a busy period.
  - If you must activate the Master script during a busy period, activate all primary and secondary scripts first.

Attention: If the server is not processing calls, you can activate the Master script without first activating the primary and secondary scripts.

- Validation of large scripts
  - Do not validate the Master script or any large script during a busy period.
- Agent-to-supervisor assignments
  - Do not run multiple agent-to-supervisor assignments concurrently.
- Agent-to-skillset assignments
  - Do not run multiple agent-to-skillset assignments concurrently.
- Generation of large reports
  - Generate large reports one after the other rather than concurrently.
- Extraction of large amounts of data from the database

  - — Generation of large data extractions one after the other rather than concurrently.
- Mass logon and logoff of agents
  - — Spread agent logon/logoff activity over a period of 5 to 15 minutes, and do not perform this activity during the peak busy hour.
- Database backup
  - — Perform online (for example, database) backups during off-peak hours.
- Checking files for viruses
  - — Perform this activity during off-peak hours.

Contact Center Manager Administration performance

This section describes performance impacts to Contact Center Manager Administration server.

Contact Center Manager Administration CPU impact

The analysis in this section applies to a stand-alone system only.

For optimal performance, average CPU use on both the Contact Center Manager Administration server and the client must not exceed 70 percent over an interval of 15 minutes.

CPU Model

The CPU model implemented in the CapTool consists of four sub-models to account for the major consumers of CPU resources on the Contact Center Manager Administration server:

- IIS CPU load
- Partitioning CPU load
- Unicast traffic transmission CPU load
- RTD CPU load from a co-resident Web Client

CPU Model assumptions

For this model assume the following:

- Average CPU utilization does not exceed 70 percent over an interval of 20 minutes during peak usage loads.
- The average request rate from each user to Contact Center Manager Administration does not exceed 17 per minute.

To determine the processor required for a Contact Center Manager Administration in your environment, use the CapTool. The CapTool recommends a processor and predicts the CPU impact.

To determine the processor required for a client PC, use CapTool. Based on the amount of real-time display traffic, CapTool recommends a processor and predicts the CPU impact.

Additional factors affecting CPU consumption

Refresh rates—The minimum refresh rate for real-time statistics on Contact Center Manager Administration is 0.5 seconds. You can adjust this rate to achieve optimal balance between latency and CPU consumption.

Historical reports—The combined number of on-demand or scheduled reports that you can generate simultaneously is limited to five. You can schedule as many historical reports as required; however, only five scheduled reports are processed simultaneously while the others wait in queue. Likewise, for on-demand reports, only five reports can be generated at the same time. For example, five supervisors can generate an on-demand report, but the sixth supervisor to do so receives a message saying the system cannot process the request. This supervisor must try to generate the ad hoc report again later after the first five reports are generated (or schedule the report to run later). This limitation applies to the total of the on-demand and scheduled reports that can be generated at a particular time. For example, if two reports are scheduled to be completed at noon, then only three ad hoc reports can be generated at this time, bringing the total to five.

Parameters not included in the model

The CPU use on Contact Center Manager Administration may be impacted by the following parameters, which are not accounted for in the preceding model:

- scheduled historical reports
- antivirus scanning
- backup and restore procedures

Multiple Contact Center Manager Administration systems

It is possible to split Contact Center Manager Administration users across multiple platforms. When using the CPU model, each Contact Center Manager Administration must be analyzed individually to determine the CPU loading on each one.

Contact Center Manager Administration contact center server network impact

The network impact from Contact Center Manager Administration on the Contact center LAN or WAN can be divided into two parts:

- RSM multicast data sent from Contact Center Manager Server to Contact Center Manager Administration.

Attention: RSM compression is a new option that can now be configured on the Contact Center Manager Server. However, Contact Center Manager Administration does not support RSM compression. If the compression is configured, Contact Center Manager Administration real-time displays will not work.

- Consolidated Real-Time Display (CRTD) data
  Contact Center Manager Administration consolidates multicast traffic into a single stream, and sends it to the client PCs in either multicast or unicast format.

  Attention: Because the unicast option has a significant impact on network bandwidth requirements and CPU usage, Avaya recommends that you use multicast mode of network communication where possible.

In a network Contact Center Manager Server environment, Contact Center Manager Administration can consolidate traffic from multiple contact center servers. The RSM multicast data streams can originate at local and remote sites, and may be directed to both local clients and remote clients. In this environment, the consolidated display data is known as Network Consolidated Real-Time Display (NCRTD) data.

NCRTD multicast characterization

The inputs required to characterize the NCRTD multicast traffic are:

- send rates (time intervals in seconds) for each of the following statistics:
  - Agent
  - Application
  - Skillset
  - Nodal
  - IVR
  - Route
- the number configured for the following parameters:
  - Active agents
  - Applications
  - Skillsets
  - IVR queues
  - Routes

Attention: Number of nodes is always equal to 1.

- the number of data streams sent for each of the listed statistics. This value is 0, 1, or 2 for each type of statistic. The two types of data streams are Moving Window and Interval-to-date.

NCRTD unicast characterization

The inputs required to characterize unicast traffic are the same as those for multicast traffic, with the following additional input: number of unicast connections for each type of statistic (Agent, Application, Skillset, Nodal, IVR, and Route). A separate unicast data stream is required for each unique unicast display on each client. The number of possible unique displays for each client is 12— six for Moving Window statistics and six for Interval-to-date statistics. If more than one identical display for a particular statistic type is required on a given client, then only one unicast stream is sent for both.

For example, if two Agent/Moving Window displays are opened by the same client, only one Agent/Moving Window data stream is sent. However, if another client PC opens an Agent/Moving Window data stream, a new unicast stream is sent from the server. Two identical streams are open at this point.

Contact Center Manager Client performance

The following section describes performance impacts to Contact Center Manager Administration client.

Contact Center Manager Client CPU impact

The real-time displays have the largest impact on CPU performance on Contact Center Manager Client. The input parameters used to calculate Contact Center Manager Client CPU requirements are:

- the refresh rate (assumed identical for each display)
- the number of lines displayed (overall displays, including fixed header rows)

Contact Center Manager Administration CPU load reduction

There are several ways to reduce CPU load on the Contact Center Manager Administration server and client.

Contact Center Manager Administration server

To minimize CPU load, make the following adjustments in Contact Center Manager Administration:

- Reduce real-time display refresh rates.
- Stagger scheduled historical reports so that they are not scheduled to run at the same time.
- Schedule large reports to run at off-peak hours.
- Schedule antivirus scanning to occur at off-peak hours.
- Perform backup and restore procedures at off-peak hours.

Contact Center Manager Administration client

To minimize CPU load, make the following adjustments in Contact Center Manager Client:

- Reduce real-time display refresh rates.
- Configure the client to display less data by using data partitioning and filtering.

If the parameters are exceeded, you can use more than one Contact Center Manager Administration, and you can split Contact Center Manager Administration users across the multiple Contact Center Manager Administration servers.

Contact Center Multimedia bandwidth recommendations

Avaya recommends that the average contact center subnet usage not exceed 30 percent of the total bandwidth. This includes all the traffic (even customer traffic).

The e-mail servers can be remote, but, if they are, the latency and bandwidth of the connection to these servers result in slower throughput of the overall system.

Communication Control Toolkit guidelines to minimize capacity requirements

The engineering models used to calculate the capacity requirements of your contact center assume that you follow certain guidelines to minimize the load on your server.

Steady state operation

Steady state refers to an operational state in which average values of the capacity parameters do not change with time. For example, CPU use may vary widely at different consecutive time intervals; however, if you examine the average values of CPU use taken over consecutive 20-minute intervals, during a period of steady state operation, these average values are approximately the same.

Guidelines for steady state operation

To ensure trouble-free operation of the server, adhere to the following guidelines for steady state operation:

- Processor CPU—Average CPU use over an interval of 20 minutes during the peak hour under steady state operation must not exceed 70 percent.
- Server RAM memory—Average pages per second (found in the Memory Object of the Performance Monitor) over an interval of 20 minutes during the peak hour under steady state operation must not exceed 5.

- Server virtual memory—Committed Bytes (found in the Memory Object of the Performance Monitor) must not exceed 90 percent of the Commit Limit (also found in the Memory Object of the Performance Monitor).
- Physical and virtual memory—For optimal performance, you must adhere to the Microsoft recommendations for physical RAM and virtual memory sizing.

Guidelines for non-steady state operations

Non-steady state processes can impact the steady state call processing activity of the server. To minimize their impact, Avaya recommends a number of restrictions:

- Database backup
  Perform database backups during off-peak hours.
- Checking files for viruses
  Perform this activity during off-peak hours.

Network Traffic

Communication Control Toolkit uses remote method calls between the client PC and the Communication Control Toolkit server. Avaya recommends that you design and develop the applications to minimize the number of remote calls and, therefore, reduce the demands on the underlying network and increase the application responsiveness.

The following network traffic measurements were taken using the Full API Reference Client and logging on to the Communication Control Toolkit server as a user with a single AgentTerminal assigned (representing the normal deployment of a Communication Control Toolkit application).

The following table provides a measurement of the network traffic generated by various call scenarios using the Full API Reference Client. These network traffic statistics provide a representation of what load the Communication Control Toolkit should impose on the network.

Network traffic statistics

Scenario	Rx by server (bytes)	Tx by server (bytes)	Total (bytes)
Connect to the CCT server (does not include traffic required to perform user authentication)	8227	7090	15 317
Disconnect from the CCT server	1629	1243	2872
Answer and drop an incoming call	4171	7324	11 495
Make and drop an outgoing call	4332	6726	11 058

Server virtualization support

Avaya Aura™ Contact Center supports the use of server virtualization. Virtualization essentially enables you to share the resources of a single computer across multiple environments. You can host multiple operating systems and multiple applications locally and in remote locations, removing the constraints of physical and geographical limitations. The benefits of more efficiently using your hardware resources through virtualization include the following:

- energy savings
- cost reduction
- increased security
- high availability of resources
- enhanced desktop management
- improved disaster recovery

Virtualization allows one large server to replace multiple smaller servers. Contact Center supports:

- VMWare vSphere Release 4.0
- Microsoft Hyper-V

This section provides the information needed to determine whether your contact center meets the requirements associated with virtualization.

Attention: Media Application Server (MAS) does not support virtualization. Do not install Media Application Server using VMWare or Microsoft Hyper-V.

Navigation

- VMWare support (page 209)
- Hyper-V support (page 210)
- Virtual Machine hardware requirements (page 210)

VMWare support

Contact Center supports VMWare vSphere Release 4.0. Each Contact Center server application is supported stand-alone in its own single Virtual Machine instance on VMware. Three instances of Contact Center server applications per Avaya Communication Server 1000 are supported.

Hyper-V support

Contact Center supports Microsoft Hyper-V. Each Contact Center server application is supported stand-alone in its own single Virtual Machine. Three instances of Contact Center server applications for each Avaya Communication Server 1000 are supported.

Virtual Machine hardware requirements

Provision the Virtual Machine with the same (or higher) specification as is listed for the physical server, plus an additional CPU overhead of 15 percent over the recommended value in the physical server specification.

The Virtual Machine must have the same amount of allocated memory as the equivalent physical server.

The Virtual Machine must have the same amount of allocated hard disk space as the equivalent physical server and the hard disk must have the same size partitions as the equivalent physical server.

Networking

The networking requirements in Contact Center is the same as the networking requirement of each virtual machine. Use the Capacity Assessment Tool to determine the networking requirement of each virtual machine hosted on the server.

High Availability server requirements

Avaya Aura™ Contact Center supports hot standby resiliency for Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), Contact Center Multimedia (CCMM), and Contact Center Manager Administration (CCMA).

The Avaya Aura™ Contact Center High Availability feature is supported on Avaya Communication Server 1000 Release 6.0 or later. If using an Avaya Communication Server 1000 Release 6.0 PABX, patch MPLR30010 must be applied to the PABX to support Avaya Aura™ Contact Center High Availability functionality.

This section provides information about Standby server and Remote Geographic Node server requirements.

Navigation

Overview

One set of Contact Center applications (a CCMS, a CCT, a CCMA, 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. Configuration changes made to the active system during normal operation are automatically copied to the standby applications and the standby applications are configured to take over processing from the active system. Statistical data is also automatically copied to the standby applications.

Standby server 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.

Attention: In a SIP-enabled contact center using an Avaya Aura™ Unified Communications platform and High Availability resiliency, the active and standby CCMS servers must both have TLS certificates in place to communicate securely with the Avaya Aura™ Unified Communications platform and to support High Availability switch-over.

Network requirements

In a Campus High Availability environment the standby and active servers are in the same location, typically they are both on the same network subnet (LAN). In a campus environment the active and standby server have different static IP addresses, but share a common virtual Managed IP address.

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 needs the Contact Center Manager Server name), no requirements are required to reconfigure the contact center system.

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

Remote Geographic Node server requirements

The High Availability feature supports Remote Geographic Nodes. Remote Geographic Nodes are similar to the standby servers but they are used only to shadow data from the active server—they have no other responsibility. Remote Geographic Nodes do not automatically take over if the active system fails. If the standby server and active server are in the same building, then a Remote Geographic Node on remote site provides additional data protection by maintaining a remote copy of the configuration and statistical information.

The Remote Geographic Node server must match the active server. The Remote Geographic Node server must have 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 standby servers must have the same patch level and the same operating system updates.

Managed IP address

Contact Center provides a mechanism by which the IP address of the active Contact Center server does not change after switchover to minimize impact on other Avaya and third-party applications. A switchover from the active to the standby server in a campus environment 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.

A mechanism is also provided by which the IP address information of the primary and secondary servers are different for geographic redundancy solutions. Communication Control Toolkit can publish APIs to allow the clients to retrieve the active and standby servers. Contact Center Manager Server can publish database views to display the active and standby information.

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.

Trusted IP address

The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have a server to ping regularly to verify the network connection. Avaya recommend that you use the IP address of some part of your IT infrastructure as the trusted IP address.

Switch over behavior in Avaya Communication Server 1000-based contact centers

Avaya Communication Server 1000 resources acquired by the Contact Center Manager Server are not released at the time of a failure, and the logon state of voice agents is maintained when the backup Contact Center Manager Server (CCMS) comes online. Therefore, if a CCMS outage occurs, agents need not cycle their voice logon state. The standby CCMS starts up and shows the correct state of every agent’s voice terminal as they were at the time of the active CCMS outage. Calls in progress between a customer and an agent are not affected. The logon state of multimedia-enabled agents is not preserved when a failover to a standby application occurs. These agents must logon again.

For an Avaya Communication Server 1000-based contact center system with 5000 active agents, it takes about 30 seconds for the standby Contact Center Manager Server to begin processing new incoming calls in the script. During this short period, calls are given default ACD by the Avaya Communication

Server 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 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 pop-ups are used at the time of a CCT server outage, then the agents will observe that the pop-ups start again seamlessly in less than 30 seconds.

Switch over behavior in SIP-enabled contact centers

For a SIP-based contact center system agents must manually log back on again if a Contact Center Manager Server switches over. The switch-over time is longer in SIP-enabled contact centers, typically less than 5 minutes.