Avaya Contact Center Select Solution Description

Release 7.0.3
Issue 02.05
July 2018

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Contents

Chapter 1: Introduction

Purpose

This document describes an Avaya solution from a holistic perspective focusing on the strategic, enterprise, and functional views of the architecture. This document also includes a high-level description of each verified reference configuration for the solution.

Intended audience

This document is intended for personnel who want to understand how the solution and related verified reference configurations meet customer requirements.

Related resources

Avaya Contact Center Select Documentation

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

Title	Use this document to:	Audience
Overview		
Avaya Contact Center Select Solution Description	This document provides a technical description of Avaya Contact Center Select. It describes the product features, specifications, licensing, and interoperability with other supported products.	Customers and sales, services, and support personnel
Avaya Contact Center Select Documentation Catalog	This document describes available Avaya Contact Center Select documentation	Customers and sales, services, and support personnel

Table continues…

Title	Use this document to:	Audience
	resources and indicates the type of information in each document.	
Contact Center Performance Management Data Dictionary	This document contains reference tables that describe the statistics and data in the historical and real-time reports generated in Contact Center.	System administrators and contact center supervisors
Implementing		
Deploying Avaya Contact Center Select DVD	This document contains information about Avaya Contact Center Select DVD installation, initial configuration, and verification. This document contains information about maintaining and troubleshooting the Avaya Contact Center Select server.	Implementation personnel
Deploying Avaya Contact Center Select Software Appliance	This document contains information about Avaya Contact Center Select Software Appliance (VMware) preparation, deployment, initial configuration, and verification. This document contains information about maintaining and troubleshooting the software appliance.	Implementation personnel
Deploying Avaya Contact Center Select Hardware Appliance	This document contains information about Avaya Contact Center Select Hardware Appliance (physical server) installation, initial configuration, and verification. This document contains information about maintaining and troubleshooting the hardware appliance.	Implementation personnel
Avaya Contact Center Select Business Continuity	This document contains information about deploying Avaya Contact Center Select Business Continuity.	Implementation personnel
Upgrading and patching Avaya Contact Center Select	This document contains information about upgrading and patching Avaya Contact Center Select.	Implementation personnel and system administrators
Administering		
Administering Avaya Contact Center Select	This document contains information and procedures to configure the users, skillsets, and contact center configuration data. This document contains information about creating Avaya Contact Center Select real-time and historical reports.	System administrators and contact center supervisors
Avaya Contact Center Select Advanced Administration	This document contains information about managing the Avaya Contact Center Select	System administrators

Table continues…

Title	Use this document to:	Audience
	server, licensing, and multimedia configuration.	
Using Contact Center Orchestration Designer	This document contains information and procedures to configure script and flow applications in Contact Center Orchestration Designer.	System administrators
Maintaining		
Contact Center Event Codes	This document contains a list of errors in the Contact Center suite and recommendations to resolve them. This document is a Microsoft Excel spreadsheet.	System administrators and support personnel
Using		
Using Agent Desktop for Avaya Contact Center Select	This document provides information and procedures for agents who use the Agent Desktop application to accept, manage, and close contacts of all media types in Contact Center.	Contact center agents and supervisors
Using the Contact Center Agent Browser application	This document provides information and procedures for agents who use the Agent Browser application to log on to Contact Center and perform basic tasks.	Contact center agents

Finding documents on the Avaya Support website

Procedure

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

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

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

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

Chapter 2: Changes in this release

This section describes the new features and changes in Avaya Contact Center Select Release 7.0.

Feature changes in the Release 7.0 base build

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

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

In Contact Center Release 7.0, administrators can configure a setting that gives agents the ability to automatically add a leading digit before dialing of any number using Agent Desktop Phonebook. If administrators enable this feature, the plus sign (**+**) before the phone numbers in Phonebook is replaced with a trunk access code. The trunk access code is added before the phone number. Therefore, agents do not need to manually add a leading digit to call externally or forward a call using Phonebook.

Avaya Contact Center Select supports Microsoft Windows Server 2012 R2

Avaya Contact Center Select Release 7.0 is supported on the Microsoft Windows Server 2012 R2 operating system. Avaya Contact Center Select Release 7.0 is not supported on Microsoft Windows Server 2008 R2. Customers upgrading to Avaya Contact Center Select Release 7.0 must migrate to a new Microsoft Windows Server 2012 R2 server.

Avaya Media Server changes

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

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

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

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

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

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

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

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

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

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

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

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

Contact Center Agent Browser application

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

Contact Center Manager Administration password expiry

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

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

Contact Center Manager Administration support for Caché database

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

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

Contact Center services secured by default

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

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

- Contact Center Manager Administration (CCMA)
- Contact Center Multimedia (CCMM) Administration
- Agent Desktop
- Multimedia Services
- Orchestration Designer
- Outbound Campaign Management Tool
- Contact Center Web Services

- Communication Control Toolkit (CCT) Web Administration

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

Emergency license expiry notification

When an emergency license is provided to a customer, a daily Windows event is generated. The Windows event warns the customer of the number of days left for the emergency license to expire. Customers can then address the situation in which the Avaya customer service representative provided the emergency license, before the emergency license expires. For example, if your Avaya customer service representative activates the emergency license file on your system because the connection between Contact Center License Manager and Contact Center Manager Server cannot be fixed within the 30-day grace period, then you can use the emergency license to re-establish the connection between Contact Center License Manager and Contact Center Manager Server.

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

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

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

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

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

New Avaya Contact Center Select Hardware Appliance

Avaya Contact Center Select Release 7.0 is offered as a Hardware Appliance.

The Avaya Contact Center Select Release 7.0 Hardware Appliance specification has improved to meet the increased requirements of the included Microsoft Windows Server 2012 R2 operating system. The Release 7.0 Hardware Appliance new hard disks support increased multimedia offline data retention.

New Avaya Contact Center Select minimum hardware specifications

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

New Avaya Contact Center Select minimum virtual machine specifications

Avaya Contact Center Select Release 7.0 continues to support VMware and virtualization. Avaya Contact Center Select Release 7.0 defines three new minimum levels of virtual machine specification; a new Entry-level, a new Mid-range, and a new High-end virtual machine specification. For virtualized Avaya Contact Center Select Release 7.0 installations on virtual machines, only the new virtual machine specifications are supported.

Password aging in Contact Center Manager Administration

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

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

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

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

Report Creation Wizard

Avaya Contact Center Select Release 7.0 now supports Report Creation Wizard (RCW). RCW is a Web-based interface in which you can create and edit reports. You can import and schedule the reports in Historical Reporting. You can access RCW from the Historical Reporting component of Contact Center Manager Administration.

Serviceability enhancements in Contact Center 7.0

The following are the serviceability enhancements in Contact Center 7.0:

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

Support for adding company images and logos to signatures

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

Support for copying the CLID of a customer using Agent Desktop

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

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

Note:

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

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

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

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

Support for forced Not Ready reason codes

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

Note:

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

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

Support for scripting using CLID and Wild CLID in SIP environments

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

Temporary lock out of Contact Center Manager Administration users

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

In Contact Center Release 7.0, the temporary lock out feature is disabled by default,. If administrators enable the temporary lock out feature, by default users can incorrectly enter the password three times before CCMA locks the user account for three minutes. Administrators can

configure both the number of times that the users can enter an incorrect password and the lock out period using the CCMA Security Settings dialog.

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

Feature changes in Release 7.0 Feature Pack 1

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

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

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

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

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

Avaya Contact Center Select supports IP Office Release 10

Avaya Contact Center Select supports IP Office Release 10. Avaya Contact Center Select solutions that use IP Office Release 10 can benefit from an increase in agent counts by enabling Direct Media on the IP Office lines (IP Office Line or IP Office SIP Line) that target inbound calls at Avaya Contact Center Select.

Contact Control Service SDK

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

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

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

File extension restrictions for attachments

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

Improved operational performance for Business Continuity

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

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

Instant Messaging feature supports Microsoft Skype for Business 2015

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

New application for installing Feature Packs and Service Packs

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

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

Multimedia account passwords must meet minimum complexity criteria

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

Passwords must fulfill the following complexity criteria:

- Must be between 8 to 20 characters
- Must contain a number
- Must contain at least one uppercase letter and at least one lowercase letter
- Must not contain spaces
- Must not contain any of these characters: \ & : < > |

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

Provision of adding a friendly name for a web chat agent

From Release 7.0 Feature Pack 1, Contact Center administrators can add a friendly name or nickname for a web chat agent. If administrators configure the Friendly Name label, the nickname

of the web chat agent is displayed in agents' responses to web chat messages. Administrators can also choose that the friendly name is displayed in welcome messages.

Removal of the default Agent Desktop Dashboard password

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

Skillset list sorted when creating a billboard display

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

Support for the Open Queue Open Interface

From Release 7.0 Feature Pack 1, Avaya Contact Center Select (ACCS) supports the Open Queue Open Interface.

The Open Queue Open Interface delivers existing Open Queue functions to third-party applications that use a Web service. Third-party applications can add and remove contacts of a specific type in Contact Center.

VMware 6.0 support

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

Whisper Coaching

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

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

Feature changes in Release 7.0 Feature Pack 2

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

Agent Desktop integrated login

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

Agent skillset assignment guardrails

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

Increased CCMM customer contact ratio

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

Offline Security Store

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

Remote Desktop Services support for Agent Desktop

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

Removal of default security configuration

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

REST API integration

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

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

Synchronization of accssync user changes to IP Office

From Release 7.0 Feature Pack 2, Avaya Contact Center Select synchronizes accssync user password changes to IP Office. When you change the accssync user password, Contact Center Manager Administration automatically updates the password on IP Office.

VMware 6.5 support

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

Feature changes in Release 7.0 Feature Pack 3

See the following sections for information about new features in Release 7.0 Feature Pack 3.

Ability to store email attachments in the database

From Release 7.0 Feature Pack 3, there is an option to save new email attachments in the MULTIMEDIA database instead of on the file system. You can configure this option using the Multimedia Administration utility.

Contact Center database encryption

From Release 7.0 Feature Pack 3, you can encrypt and decrypt the Contact Center database using Security Manager. To encrypt the database, you must create and activate an encryption key and use it to encode the files in the Contact Center Caché database.

Data Management - customer privacy

From Release 7.0 Feature Pack 3, you can use the Multimedia Data Management utility to act on privacy requests from contact center customers. For example, if a customer exercises their right to access information or their right to be forgotten, you can use the Multimedia Data Management utility to satisfy these requests.

REST API Enhancements

From Release 7.0 Feature Pack 3, the Contact Center REST API supports GET, POST, PUT, or DELETE request methods. Using the TFE REST Configurator, you can now add environments which enable the use of environment variables in REST requests.

Contact Center workflows now support the CONVERT and JSON GET ELEMENT command.

Security Manager support for chained certifcates

From Release 7.0 Feature Pack 3, Security Manager supports importing chained certificates.

Support for applying a restriction flag to a customer

From Release 7.0 Feature Pack 3, you can apply a restriction flag to a customer using Agent Desktop. This can help your Contact Center to comply with General Data Protection Regulation (GDPR). For example, add a restricted flag to indicate to agents not to initiate unsolicited email messages to customers without consent.

Other changes in Release 7.0

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

Agent Desktop no longer supports deployment as a thick client

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

Avaya Contact Center Select OVA file no longer available

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

IP Office supported versions

Avaya Contact Center Select Release 7.0 does not support integration with IP Office 9.0.3 or 9.0.4.

Avaya Contact Center Select Release 7.0 supports integration with IP Office 9.1.x, minimum 9.1.4 or later. For more information about the supported IP Office versions, refer to the Avaya Contact Center Select Release Notes.

Microsoft Exchange Server supported versions

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

Microsoft Internet Explorer releases no longer supported

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

Secure Sockets Layer communications is no longer supported

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

Third-party or custom applications connecting to Contact Center must support TLS 1.0 or later. Removal of support of SSL can have implications for existing third party or custom applications. Before migrating from a previous Release, check third-party or custom applications that connected securely to Contact Center, to ensure that these applications support TLS.

Windows Server 2008 is no longer supported

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

Other changes in Release 7.0 Feature Pack 1

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

Contact Center security improvements

From Release 7.0 Feature Pack 1, Contact Center introduces additional security improvements to keep current with the latest standards in the industry. These improvements include restrictions to web services access, locking down of user accounts, and changes to the way Contact Center manages passwords and keys. Many of these improvements are internal to Contact Center operation and have no impact on end-user operations.

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

Server Message Block signing enabled on Windows Server 2012

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

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

Third-party components updated

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

The Release Pack Installer automatically updates these components.

Other changes in Release 7.0 Feature Pack 2

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

CCMA users must login before changing password

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

Installation account for Contact Center install

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

Third-party components updated

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

The Release Pack Installer automatically updates these components.

Other changes in Release 7.0 Feature Pack 3

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

Avaya Aura® Media Server update

Contact Center Release 7.0 Feature Pack 3 supports Avaya Aura® Media Server Release 7.8.

From Contact Center Release 7.0 Feature Pack 3, installing the Windows version of Avaya Aura® Media Server co-resident with a Voice and Multimedia Contact Server is no longer supported. When you deploy a Voice and Multimedia Contact Server with Avaya Aura® Media Server, Contact Center installs the Linux version of Avaya Aura® Media Server on a Hyper-V instance on your Voice and Multimedia Contact Server.

This process is fully automated by the Contact Center software installer for fresh installs, and by the Contact Center Release Pack Installer (RPI) for upgrades. In both cases, you can use the Update Configurator utility to update Avaya Aura® Media Server to the latest supported version and apply all necessary configuration. After a reboot following an install or upgrade, the Update Configurator utility launches.

Contact Center backwards compatibility with previous version of Agent Desktop

From Release 7.0 Feature Pack 3, Contact Center supports backwards compatibility with the previous Feature Pack or Service Pack version of Agent Desktop. This allows you to upgrade the Contact Center server without the requirement to upgrade Agent Desktop in a single maintenance window. For example, if you upgrade to Release 7.0 Feature Pack 3, you can use the Release 7.0 Feature Pack 2 version of Agent Desktop.

New Agent Desktop features added in the latest Contact Center release are not available until you upgrade Agent Desktop to that release.

Backwards compatibility is not supported for major or minor releases. For example, if you upgrade to Release 7.1, you cannot use the Release 7.0 version of Agent Desktop.

IP Office supported versions

Avaya Contact Center Select Release 7.0 Feature Pack 3 does not support integration with IP Office 9.1.

Avaya Contact Center Select Release 7.0 Feature Pack 3 supports integration with IP Office 10.1 and 11.0. For more information about the supported IP Office versions, refer to the Avaya Contact Center Select Release Notes.

Third-party components updated

Release 7.0 Feature Pack 3 upgrades a number of third-party components to recent versions, such as Caché, Contact Center Tomcat, and .NET Framework. This improves security and ensures that Contact Center remains current with recent updates.

The Release Pack Installer automatically updates these components.

Chapter 3: Avaya Contact Center Select overview

Avaya Contact Center Select is a context-sensitive, collaborative, voice and multimedia customer experience solution that allows small to midsize enterprises to anticipate, accelerate, and enhance customer interactions. Avaya Contact Center Select uses the Avaya IP Office telephone system to provide a real-time telephony platform. Avaya IP Office is a flexible and scalable phone system designed specifically for small and midsize enterprises. IP Office supports a wide range of phones and devices for use in contact centers.

Avaya Contact Center Select uses SIP and CTI interfaces to communicate with the IP Office platform. This integration gives Avaya Contact Center Select access to and control of a wide range of IP Office phones and features. Customers integrating Avaya Contact Center Select with the IP Office platform gain skill-based routing, call treatments, reporting, unified agent management, and the graphical Orchestration Designer utility. Agent Desktop supports specified IP Office phones and also supports multimedia contact types.

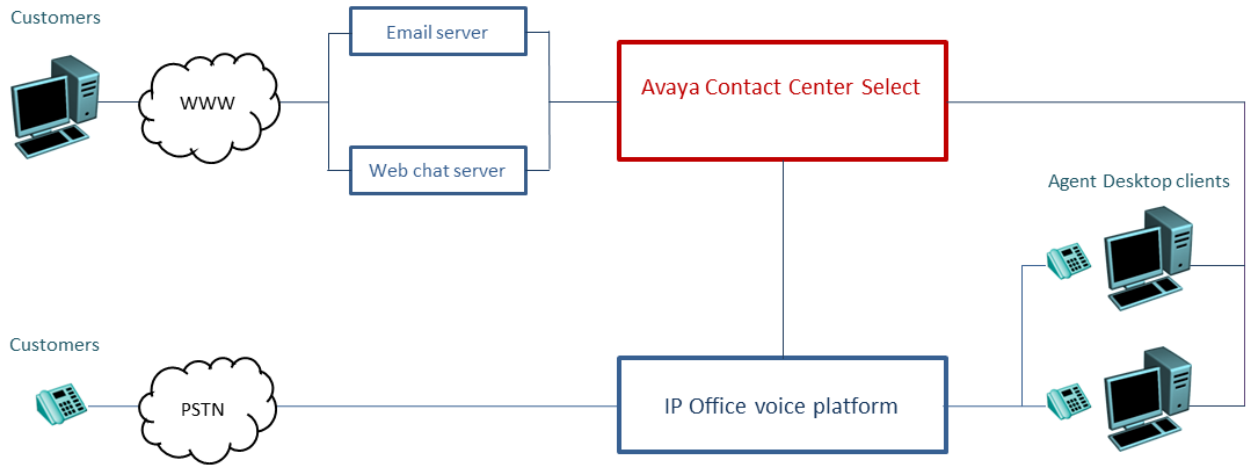


Figure 1: Typical contact center solution using voice and multimedia enabled Avaya Contact Center Select and the Avaya IP Office voice phone system

Avaya Contact Center Select provides a feature rich voice and multimedia solution with integrated routing and reporting for the small to midsize enterprises. Avaya Contact Center Select provides unified contact center and IP Office phone user account management for agents and supervisors.

Voice-enabled agents and supervisors created in Avaya Contact Center Select are automatically added to the IP Office platform. Avaya Contact Center Select synchronizes user (agent and supervisor) information between Avaya Contact Center Select and the IP Office platform.

Avaya Contact Center Select is offered in the following deployment types:

- **Avaya Contact Center Select DVD**; The Avaya Contact Center Select DVD contains the application software. The Avaya Contact Center Select DVD deployment option supports Platform Vendor Independence (PVI). The customer supplies the Microsoft Windows 2012 R2 operating system license and server hardware that meets one of the Avaya Contact Center Select PVI server specifications.
- **Avaya Contact Center Select software appliance**; The Avaya Contact Center Select software appliance is a set of VMware virtualized servers; an Avaya Contact Center Select virtual machine, an Avaya Aura® Media Server OVA, and a WebLM OVA. The customer supplies the VMware resources and operating system license for the VMware virtual machine (guest).
- **Avaya Contact Center Select hardware appliance**; The Avaya Contact Center Select hardware appliance is a physical server with the application software already loaded and partially preconfigured. Avaya supplies the server hardware and a license for the Microsoft Windows 2012 R2 operating system.

Avaya Contact Center Select supports the following routed contact types:

- Voice
- Email
- Outbound
- Web communications (Web chat)
- SMS text messages
- Fax messages
- Scanned documents
- Voice mail messages

Avaya Contact Center Select also supports peer-to-peer Instant Messaging and Presence Notifications. To support the email-based contact types, you must add an email server to your solution. To support the Web communications contact type, you must add a Web communications server to your solution.

The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.

Avaya Contact Center Select is quick to deploy and offers a feature rich voice and multimedia solution. Avaya Contact Center Select provides sample configuration data to support rapid deployment and integration with IP Office. You can modify the sample data to meet your solution's requirements and add to the data as your solution expands. You can also use the sample data to learn more about Avaya Contact Center Select. The sample data includes the following data:

- Supervisors and agents

- Skillsets
- Orchestration Designer voice flow applications
- Activity codes
- CDN (Route Points)
- Multiplicity Presentation Classes
- Real-time reports
- Historical reports
- User data synchronization account for IP Office

Avaya Contact Center Select provides a simplified voice prompt management utility. The contact center supervisor can perform prompt management work without requiring administrator access to the Avaya Aura® Media Server server. Avaya Contact Center Select provides a number of status monitoring utilities to monitor the integration points with the IP Office platform. Avaya Contact Center Select also provides an always-on graphical troubleshooting dashboard running on the server.

Licensing

Avaya Contact Center Select supports the following licensed agent packages:

Name	Description	Notes
Agent licenses	Agent licenses determine the number of agents that can log on to Contact Center. Licensing is available for the following types of agents: • voice agent • outbound agent • email agent (covering FAX messages, SMS text messages, voice mail messages, and scanned document messages) • Web communications agent (or Web chat agent)	

Avaya Contact Center Select supports the following licensed features:

Name	Description	Notes
Multiplicity	Multiplicity is the ability of an agent to handle multiple concurrent multimedia contacts. At any one time an agent can be active on a voice and multimedia contact. However, when one contact is active; the others automatically are on hold. The maximum number of concurrent multimedia or non-voice contacts that an agent can be assigned is five.	

Table continues…

Name	Description	Notes
Web Based Statistics	If Web Reporting server is enabled, agents and supervisors can use Agent Desktop to view real-time reports for call handling, skillset data, and state information on Agent Desktop.	
Remote Agent	Remote Agent is a solution that extends a Contact Center to an agent's preferred environment, allowing them to handle skillset calls regardless of location. Remote Agent solutions connect contact center calls to the agent's telephone (home telephone or mobile), without the agent needing special hardware.	
Outbound	Use the Multimedia server and the Outbound Campaign Management Tool in Contact Center Manager Administration to create progressive outbound campaigns on which calls are passed to agents and made from the Contact Center.	

For Avaya Contact Center Select (ACCS) integration with IP Office Server Edition, IP Office Server Edition requires the following licenses:

- One Avaya IP Endpoint license for Avaya Contact Center Select integration.
- One Power User license for every ACCS agent or supervisor agent that is configured for any of the following:
  - configured to use IP Office Avaya Communicator for Windows.
  - configured to operate as an ACCS Remote Agent.
  - configured to use an IP Office physical phone with IP Office remote worker functionality. Only IP Office physical phones using IP Office remote worker functionality require a Power User license; other physical phone users do not require a Power User license.
- One Server Edition license. One license for each node in the Small Community Network (SCN).
- IP Endpoint licenses – either Avaya or Third-Party depending on the IP phones used in your solution. Provision one IP Endpoint license for each configured endpoint.
  - IP Office Avaya Communicator for Windows users do not require an IP endpoint license, only an IP Office user license.
  - If your solution uses digital phones only from an IP Office 500V2 Expansion then you do not require endpoint licenses.
- One CTI Pro license or Third Party API license for IP Office.
- One ACCS license for IP Office.
- Voicemail Pro Additional Voicemail Channels, up to a maximum of 350.
- SIP Trunk licenses or channels to support the trunks used in your solution.
- Voicemail Pro Recording Administrators. One instance on each node of the SCN that calls are recorded from. If all recording is to be done on the Primary node then one instance is required. This license enables Contact Recorder.

For Avaya Contact Center Select (ACCS) integration with IP Office 500V2 (non-Server Edition), IP Office 500V2 requires the following licenses:

- One Avaya IP Endpoint license for Avaya Contact Center Select integration.
- One Power User license for every ACCS agent or supervisor agent that is configured for any of the following:
  - configured to use IP Office Avaya Communicator for Windows.
  - configured to operate as an ACCS Remote Agent.
  - configured to use an IP Office physical phone with IP Office remote worker functionality. Only IP Office physical phones using IP Office remote worker functionality require a Power User license; other physical phone users do not require a Power User license.
- Preferred Edition License.
- Essential Edition License.
- IP Endpoint licenses – either Avaya or Third-Party depending on the IP phones used in your solution.
  - IP Office Avaya Communicator for Windows users do not require an IP endpoint license, only an IP Office user license.
  - If your solution uses only digital telephones then you do not require endpoint licenses.
- One CTI Pro license.
- Voicemail Pro Additional Voicemail Channels.
- SIP Trunk licenses or channels licenses to support the trunks used in your solution.
- Voicemail Pro Recording Administrators. One instance on each node of the Small Community Network (SCN) that the calls are recorded from. If all recording is to be done on the Primary node then one instance is required. This license enables Contact Recorder. Contact Recorder requires a separate Application Server.

When Avaya Contact Center Select is deployed with an IP Office Resilience pair, ensure the IP Office Secondary system contains the following licenses to enable Avaya Contact Center Select connectivity:

- One Avaya IP End point license
- One CTI Pro license

This applies to both Avaya Contact Center Select standalone and Avaya Contact Center Select Business Continuity configurations. The IP Office Secondary system does not require the inclusion of Voicemail Pro Recordings Administrators license system or Voicemail Pro licenses, because the Call Recording functionality is licensed from the IP Office Primary system.

The Avaya Contact Center Select base software bundle provisions one Contact Recorder system license plus 1 Voicemail Pro port for every voice agent for Call Recording.

An Avaya Contact Center Select voice agent license provisions one Voicemail Pro port for Call Recording.

Avaya Contact Center Select uses Avaya WebLM as the license provider. Each Avaya WebLM instance supports a single Avaya Contact Center Select.

Hotdesking / Free-seating

Hot desking / Free-seating environments are supported with ACCS and IP Office physical phones and softphones.

Hotdesking with physical phones

Each physical IP phone requires an IP Endpoint license.

Power User licenses are not required to use IP Office physical phones unless using the IP Office remote worker functionality.

Example:

Requirement: 100 seat ACCS with 100 IP physical phones and 200 possible agents:

- Order 100 ACCS voice agents + 100 IP Endpoint licenses.
- If all agents require IP Office remote worker functionality also order 200 Power User licenses.

Hotdesking with softphones

Each ACCS agent requires a Power User license.

IP Endpoint licenses are not required for the softphones.

Example:

Requirement: 100 seat ACCS with 100 softphones and 200 possible agents:

- Order 100 ACCS voice agents + 200 Power User licenses.

Maximum number of supported nodes

Avaya Contact Center Select supports the following maximum number of IP Office nodes:

- For IP Office 10.x or 11.0 Select (Server Edition) Switch R630 or OVA, ACCS supports 150 nodes in total, consisting of a Primary, a Secondary, and 148 expansions.
- For IP Office 10.x and 11.0 Select (Server Edition) with any hardware other than R630/OVA, ACCS supports 32 nodes in total, consisting of a Primary, a Secondary, and 30 expansions.

User Data Synchronization

Avaya Contact Center Select provides unified administration for contact center agents and IP Office users. The users (agents and supervisors) that you configure in Avaya Contact Center Select are automatically mirrored to the connected IP Office.

When you create an agent in Contact Center Manager Administration, you can choose to create a local Windows user account on the Avaya Contact Center Select server or map to an existing Windows domain user account. Avaya Contact Center Select automatically creates a matching user account in IP Office.

When you modify agent details in Avaya Contact Center Select, the corresponding IP Office user details are automatically updated. If you delete an agent in Avaya Contact Center Select, the corresponding IP Office user is not deleted.

The data synchronization mechanism works in one direction; from Avaya Contact Center Select to IP Office. The Avaya Contact Center Select administrator can manually force data synchronization from Avaya Contact Center Select.

Topology

In a contact center solution using Avaya Contact Center Select and an IP Office telephone system, the following network and connectivity topology considerations apply.

Avaya Contact Center Select (ACCS) supports the following deployment options:

- Avaya Contact Center Select DVD
- Avaya Contact Center Select Software Appliance
- Avaya Contact Center Select Hardware Appliance

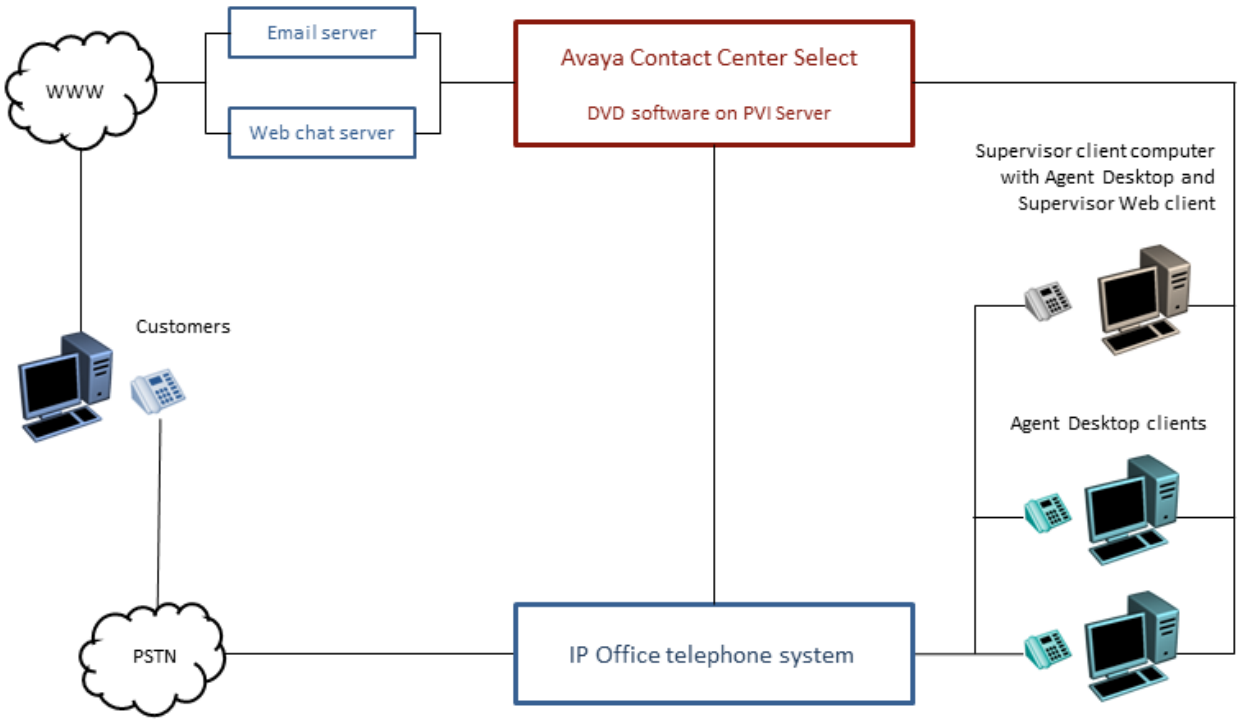


Figure 2: Typical Avaya Contact Center Select DVD deployment

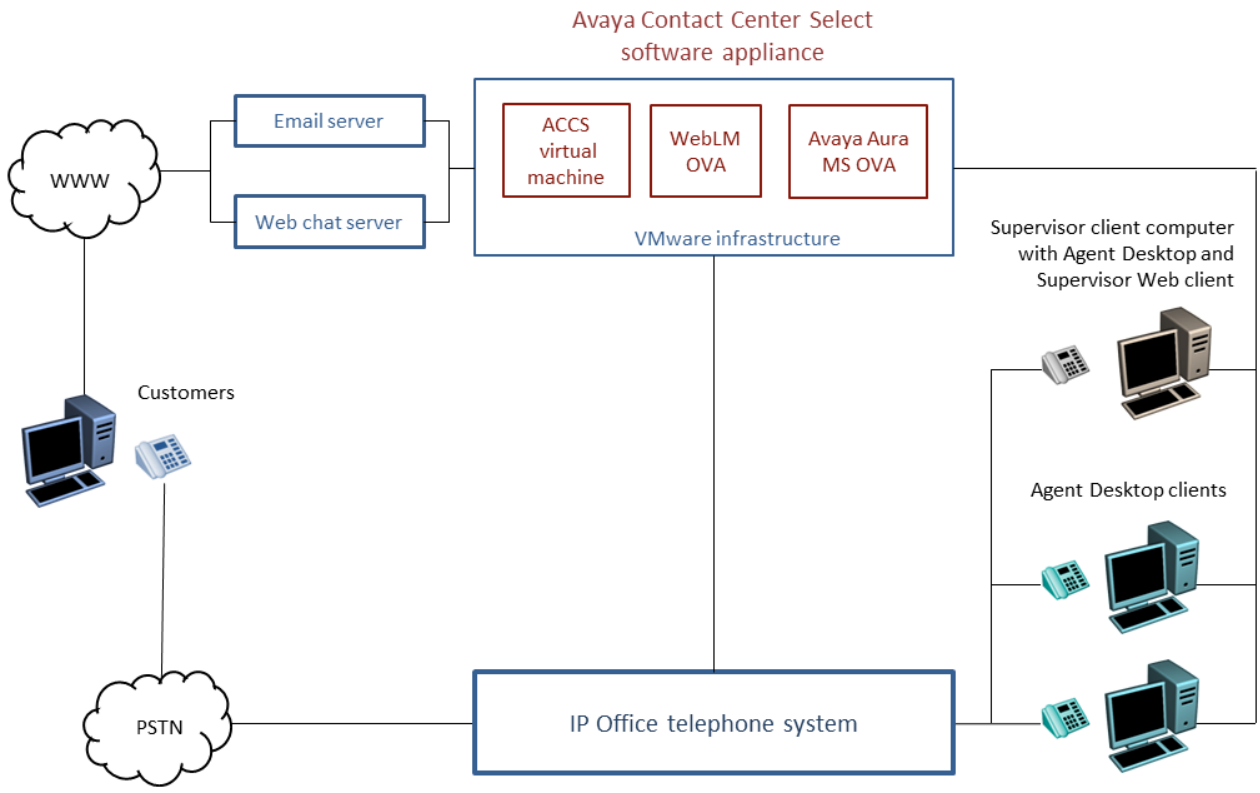


Figure 3: Typical Avaya Contact Center Select software appliance solution

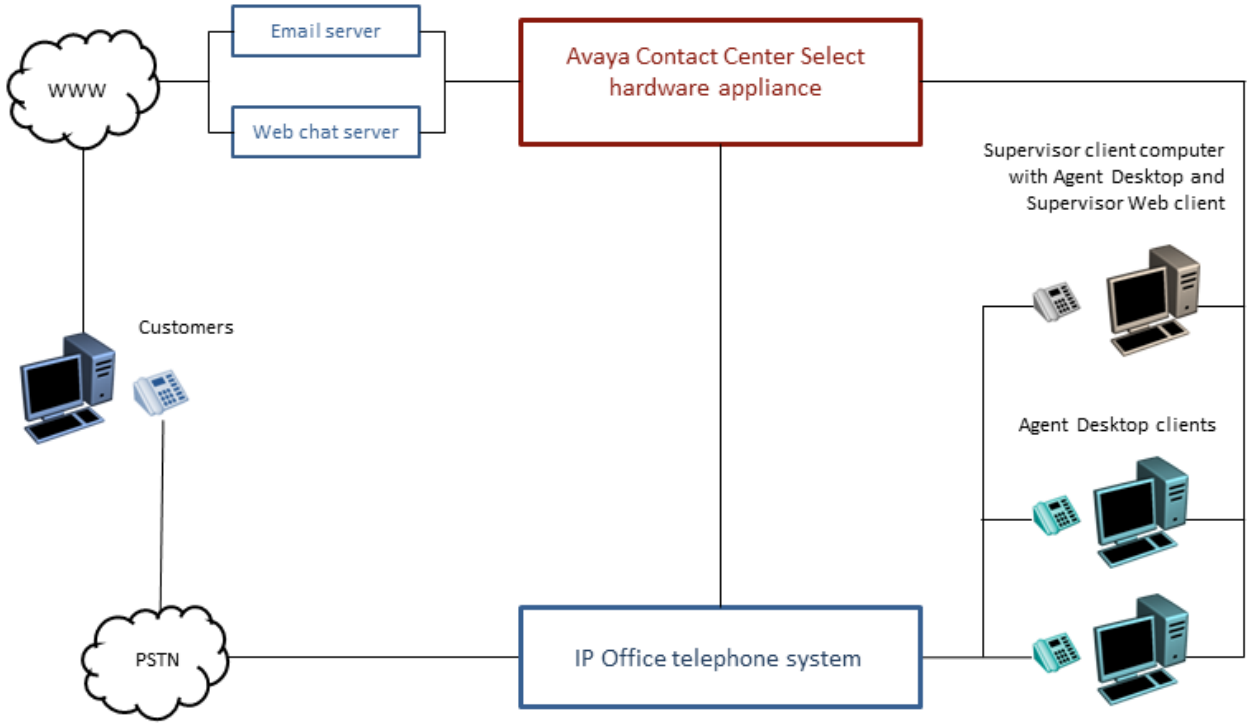


Figure 4: Typical Avaya Contact Center Select hardware appliance solution

The following connectivity and network layout conditions apply to all Avaya Contact Center Select solutions:

- The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.
- Each Avaya Contact Center Select connects to a single IP Office Server Edition Primary server. Avaya Contact Center Select does not support connecting to an IP Office Secondary server. Alternatively, each Avaya Contact Center Select can connect to a single IP Office 500V2 Standard Mode with an Advanced Edition license.
- A Small Community Network (SCN) is a system of networked IP Office telephone systems that can, among other features, share extension numbers and user names. Each IP Office SCN supports a single connected Avaya Contact Center Select. Avaya Contact Center Select connects to the IP Office Server Edition Primary server of the SCN.
- To support an IP Office SCN, Avaya Contact Center Select must connect to an IP Office Server Edition Primary server in that SCN network.
- The Avaya Contact Center Select server and the connected IP Office telephone system must be located in the same campus location.
- To support the email-based multimedia contact types, you must install and commission an email server in your solution.
- To support the Web Communications (Web chat) contact type, you must install and commission a Web chat server in your solution.

- Each Avaya WebLM instance supports a single Avaya Contact Center Select.
- Each Avaya Aura® Media Server instance supports a single Avaya Contact Center Select.
- A single instance of Contact Center Manager Administration (CCMA) can manage only a single Avaya Contact Center Select.
- If you are using the Avaya Contact Center Select Software Appliance, the Avaya Contact Center Select virtual machine, the WebLM virtual machine, and the Avaya Aura® Media Server virtual machine must all be hosted on VMware servers located at the same campus location. The Avaya Contact Center Select Software Appliance supports hosting the Avaya Contact Center Select virtual machine, the WebLM virtual machine, and the Avaya Aura® Media Server virtual machine on one VMware host server. The Avaya Contact Center Select virtual machine host server and the connected IP Office telephone system must be located at the same campus location.
- Each Supervisor client computer communicates with the Avaya Contact Center Select server. Each Agent Supervisor client computer has Agent Desktop software and Microsoft Internet Explorer installed on it. The Supervisor uses Internet Explorer to access the Contact Center Manager Administration Web client. The Supervisor uses Contact Center Manager Administration to perform basic agent configuration and to run reports. The Agent Supervisor uses Agent Desktop software to handle customer calls, to accept emergency or supervisor calls from agents and to observe calls or Web communication contacts. Each Supervisor computer with Agent Desktop requires an associated IP Office telephone.
- Each Agent client computer communicates with the Avaya Contact Center Select server. Each Agent computer has Agent Desktop software and Microsoft Internet Explorer installed on it. The Agent uses Internet Explorer to download the Agent Desktop client software. The Agent uses Agent Desktop software to handle customer calls. Each Agent computer requires an associated IP Office telephone.
- Multicast or Unicast must be enabled on the underlying data network between the clients and the Avaya Contact Center Select server for supervisor and agents.
- Avaya Contact Center Select Business Continuity adds additional network connectivity and layout considerations to the solution. For more information, see *Avaya Contact Center Select Business Continuity*.

IP Office supported versions

Each Avaya Contact Center Select connects to a single IP Office Server Edition Primary server. Avaya Contact Center Select Business Continuity-enabled solutions support connecting to an IP Office Secondary server. A Small Community Network (SCN) is a system of networked IP Office telephone systems that can share extension numbers and user names. Each IP Office SCN supports a single connected Avaya Contact Center Select. The Avaya Contact Center Select server and the connected IP Office server must be located at the same campus location.

To support an IP Office SCN, Avaya Contact Center Select must connect to an IP Office Server Edition Primary server in that SCN network.

Avaya Contact Center Select supports only the following versions of IP Office:

- IP Office Server Edition Release 10.1, or 11.0
- IP Office 500V2, Release 10.1, or 11.0 software, Standard Mode, Advanced Edition license

Avaya Contact Center Select does not support other versions of IP Office. For more information about the supported IP Office versions, refer to the Avaya Contact Center Select Release Notes.

Avaya Contact Center Select does not support IP Office 500V2 Basic mode.

Overview of solution configuration

This section provides an overview of how to install and commission an Avaya Contact Center Select and IP Office platform-based solution. By describing the commissioning steps, this section also describes how Avaya Contact Center Select integrates with IP Office.

Avaya Contact Center Select uses the IP Office TAPID interface and SIP open standards to integrate with the IP Office platform. Avaya Contact Center Select uses the IP Office TAPID interface to monitor and control the agent endpoints of the IP Office platform. The IP Office TAPID interface gives Avaya Contact Center Select CTI call control of the IP Office users and extensions representing Avaya Contact Center Select agents. Avaya Contact Center Select uses a *SIP User Extension Number* to register and integrate with IP Office. This gives Avaya Contact Center Select SIP session management of the IP Office voice calls.

IP Office configuration for Avaya Contact Center Select

Configure IP Office to support integration with Avaya Contact Center Select. This configuration overview does not include IP Office basic configuration for system settings, licensing, or networking.

Using the IP Office Manager:

1. Configure the Avaya Contact Center Select Service User account details. On the System > Contact Center tab, configure the *CCMA Address*, *CCMA Username*, and *CCMA Password*.
2. Configure the System Voice over IP (VoIP) Domain Name. The Avaya Contact Center Select server uses this domain name for treatments and contact routing.
3. Add a user with the following specifications. Avaya Contact Center Select uses this SIP User Extension Number to register with IP Office:
    a. Device type set to *All Other Phone Types*.
    b. Extension type set to *SIP Extension*. For example, 6000.
    c. A numerical *Base Extension* number.
    d. On the User, enable *Call Waiting On*.
    e. On the User > Telephony > Supervisor Settings tab, configure the *Login Code*.

4. Configure an IP Office solution short code to map a telephone number to the Avaya Contact Center Select *SIP User Extension Number*. For example, create a short code 6000|>>3000. All customer calls to telephone number 3000 are forwarded to 6000 and routed to Avaya Contact Center Select. If 3000 is configured as a CDN (Route Point), Avaya Contact Center Select treats the customer call and routes it to a contact center agent.
5. Add a H.323 or SIP extension for each Avaya Contact Center Select agent. Avaya Contact Center Select agents use these IP Office extensions to handle voice contacts.

Avaya Contact Center Select installation

During deployment, configure Avaya Contact Center Select to connect to IP Office.

Using the Avaya Contact Center Select Ignition Wizard (configuration utility):

1. Configure the IP Office platform details.
2. Configure the Service User account details.
3. Configure the *Domain Name* to match the IP Office VoIP domain name.
4. Configure a CDN (Route Point) number to match the *Code* number used by the IP Office short code.
5. Configure the *SIP User Extension Number* to match the above IP Office user with a SIP extension.
6. Configure the Avaya Contact Center Select server details, licensing, and optional multimedia settings.
7. Start Avaya Contact Center Select.

At start up, Avaya Contact Center Select uses the SIP User Extension Number details to register itself as a SIP device with IP Office. This registration permits the following functionality:

- Incoming calls destined for an Avaya Contact Center Select Route Point are delivered to the Avaya Contact Center Select server.
- Authorizes the Avaya Contact Center Select server to send outgoing SIP calls to IP Office (for agent routing of Avaya Contact Center Select calls).
- Enables Avaya Contact Center Select specific functionality on the IP Office platform.

Continue to commission Avaya Contact Center Select by adding option features as appropriate. Install Agent Desktop software on all agent computers. Continue to maintain Avaya Contact Center Select by making frequent data backups.

For more information about deploying and configuring Avaya Contact Center Select, including IP Office short codes, refer to:

- *Deploying Avaya Contact Center Select DVD*
- *Deploying Avaya Contact Center Select Software Appliance*
- *Deploying Avaya Contact Center Select Hardware Appliance*

Simple voice call flow example

The following example shows how a customer call to IP Office is treated by Avaya Contact Center Select and then routed to an agent. By describing a sample call flow, this section also describes how Avaya Contact Center Select integrates with IP Office.

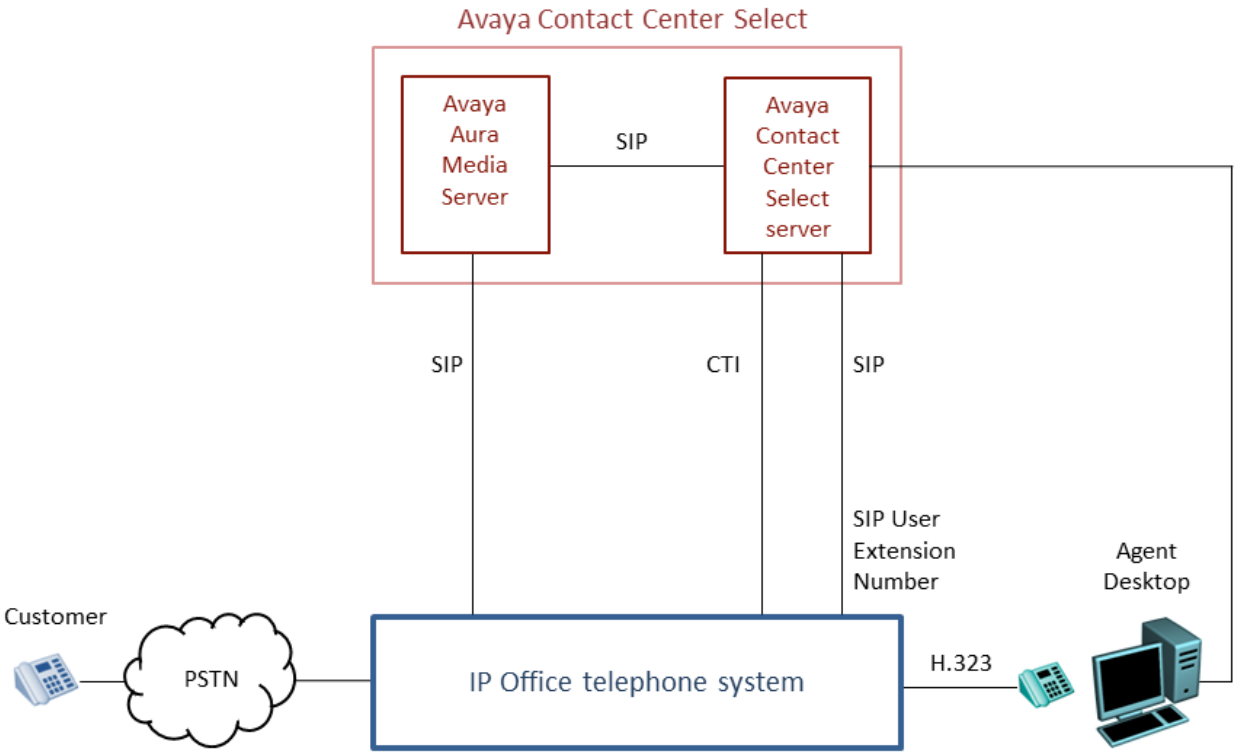


Figure 5: Communication links between Avaya Contact Center Select and IP Office

1. A Customer dials a number and the call arrives at an IP Office platform. For example, the customer dials 3000.
2. An IP Office short code (for example, 6000|>>3000) reroutes the customer call to Avaya Contact Center Select.
3. IP Office sends a SIP INVITE message to Avaya Contact Center Select.
4. When the SIP INVITE message arrives at Avaya Contact Center Select, it matches the call to one of its configured Route Point URIs and then anchors the customer call on an Avaya Aura® Media Server conference port.
5. The Avaya Aura® Media Server establishes a Real-Time Transport Protocol (RTP) media and voice path with the customer. Avaya Contact Center Select treats the customer's call using this conference port for the remainder of the call lifetime.
6. When Avaya Contact Center Select has identified a suitable available agent to handle this call, it sends a SIP INVITE message to IP Office. When the SIP INVITE message arrives at IP Office, it is sent to the destination agent H.323 desk phone.

7. IP Office sends a H.323 request to the agent desk phone to indicate that a new customer call has arrived. The agent phone rings and IP Office sends a SIP 180 Ringing message (and a corresponding TAPID Offering CTI message) back to Avaya Contact Center Select. Avaya Contact Center Select uses this trigger to inform the Agent Desktop that a call is alerting on the desk phone. In this way, both the agent desk phone and the Agent Desktop software client show the customer call as ringing.
8. When the agent answers the customer call using Agent Desktop software, Avaya Contact Center Select sends a TAPID AnswerCall request to IP Office. This causes the agent desk phone to go off hook and answer the call. IP Office sends a SIP 200 OK message (and corresponding TAPID Connected CTI message) to Avaya Contact Center Select. Avaya Contact Center Select uses CTI to notify Agent Desktop that the customer call has been answered.
9. When the call is answered, Real-Time Transport Protocol (RTP) is sent from the agent desk phone to Avaya Aura® Media Server. Avaya Aura® Media Server conferences the agent and the customer, the customer and the agent can now communicate. The agent has answered the customer's phone call.
10. The call remains active until the customer or the agent releases the call.

Sample Orchestration Designer voice flow applications

Avaya Contact Center Select provides a number of sample Orchestration Designer flow applications that treat and route customer voice contacts. Orchestration Designer flow applications contain instructions that determine the sequence of steps that a contact follows after the contact arrives at Avaya Contact Center Select. These steps can include call treatments (such as music or ringback), call routing (such as skill-based routing), or interaction with the caller (entering account numbers).

Applications perform two major functions: they define the path a contact follows, and they provide treatments to a contact as the contact moves through Contact Center. You can also use the applications to track and record information about each step in the progress of a contact, and use this information to analyze how your contact center functions to improve service. Orchestration Designer flow applications are stored in an Avaya Contact Center Select database. Task Flow Executor, a component and service of Avaya Contact Center Select, runs the flow applications to treat customer contacts. A contact is not always answered immediately by an agent. You can provide treatments to the voice contacts while they wait in a queue. These treatments can tell callers the estimated amount of time before their call is answered, or play music to callers while they wait in queue. Additionally, you can use time of day, day of week, or contact center activity to determine how a contact is handled.

Avaya Contact Center Select provides a number of sample voice Orchestration Designer flow applications:

- Customer Service. This is the main application. It welcomes the customer to the contact center, performs some basic boundary checking, and plays a menu offering the customer a

small selection of options (talk to the help desk, talk to support, enter your PIN, or leave a message).

- Voice_Skill1. This application forwards customer calls to voice skillset Skill1.
- Voice_Skill2. This application forwards customer calls to voice skillset Skill2.
- Collect_Digits. This application asks the customer to enter their PIN number using the digits on their phone. The application then plays the number back to the customer and asks them to confirm the PIN number.

Avaya Contact Center Select also provides a number of sample multimedia Orchestration Designer flow applications for the supported multimedia contact types.

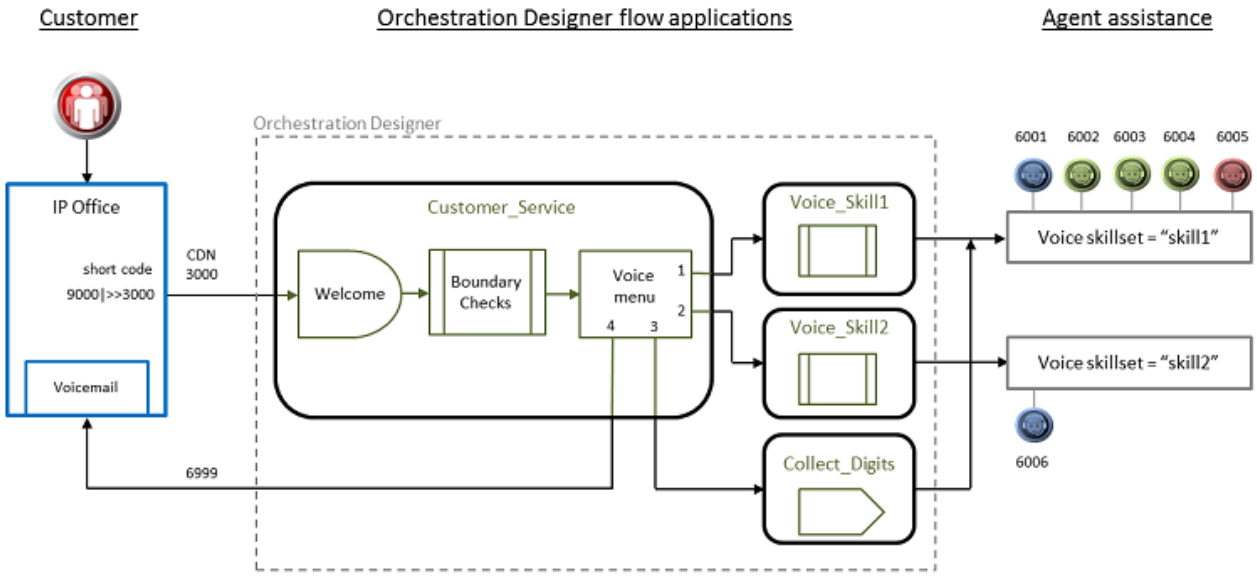


Figure 6: Treatment and routing of customer voice contacts to Avaya Contact Center Select by the sample Orchestration Designer flow applications

Sample Voice Prompt variables

The following table shows the audio media files used by the sample Orchestration Designer flow applications. Orchestration Designer uses these audio .WAV files to play messages (prompts) to the customer. The table shows which Orchestration Designer flow application uses each media file. The table also provides a transcript of the audio in each media file.

Prompt name	Prompt variable name in Orchestration Designer	Prompt transcript	Orchestration Designer flow using this prompt
Welcome_CS	Welcome_CS	"Welcome to the Contact Center."	Customer_Service

Table continues…

Prompt name	Prompt variable name in Orchestration Designer	Prompt transcript	Orchestration Designer flow using this prompt
Menu_Selection_CS	Menu_Selection_CS	• “Press 1 to speak to an agent at the help desk. • Press 2 to speak to an agent in the support center. • Press 3 to Enter your Pin Number or any 8 Digits of your choosing. • Press 4 to leave a voice mail. • Press * to repeat this menu.”	Customer_Service
Voicemail_CS	Voicemail_CS	“Please wait while we direct you to our voice messaging system mailbox.”	Customer_Service
EnterDigits_CD	EnterDigits_CD	“Please enter your pin number or digits up to a maximum of 8 digits followed by the # key.”	Collect_Digits
ConfirmDigits_CD	ConfirmDigits_CD	“The digits you entered were ...”	Collect_Digits
ValidateDigits_CD	ValidateDigits_CD	“If that is correct press 1 followed by the # key or press 2 if you wish to retry followed by the # key.”	Collect_Digits
InvalidEntry_CS	InvalidEntry_CS	“That is an invalid entry please try again.”	Customer_Service
NoData_Entry_CS	NoData_Entry_CS	“You have not entered any data Please try again.”	Customer_Service
Emergency_CS	Emergency_CS	“The contact center is now in emergency mode and closed. We will reopen shortly.”	Customer_Service
OutOfHours_CS	OutOfHours_CS	“The contact center is now closed as it is out of hours.”	Customer_Service

Table continues…

Prompt name	Prompt variable name in Orchestration Designer	Prompt transcript	Orchestration Designer flow using this prompt
Holidays_CS	Holidays_CS	“The contact center is now closed for holidays.”	Customer_Service
OutOfService_CS	OutOfService_CS	“All departments are out of service at this time. Please call back at a later time.”	Customer_Service
PromptSubmenu_CS	PromptSubmenu_CS	“Press 0 to speak to an agent, Press 1 to leave a voice mail, press, Press 9 to return to the main menu.”	Customer_Service – submenu 1 and 2
FirstRAN_CD	FirstRAN_CD	“This is the first announcement. Please wait while we try to connect you to our agents.”	Collect_Digits – Queuing Tab
SecondRAN_CD	SecondRAN_CD	“This is the second announcement. All our agents are still busy please wait.”	Collect_Digits – Iterate Queue Tab

You can use Contact Center Manager Administration (CCMA) *Prompt Management* to replace these media files with your own recordings. You can record your own voice prompts for the customer, or record voice prompts suitable for your locale (language and dialect). Avaya Contact Center Select provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a bit rate of 128kbits/sec.

Multimedia contacts processing

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

Email server contacts

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

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

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

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

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

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

External Web server transactions

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

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

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

Simple email message flow

Avaya Contact Center Select provides routed contact support for email messages. Customers send email messages requesting information or support to a published email address. Avaya Contact Center Select connects to the hosting email server and scans this mailbox (published email address) at regular intervals. Avaya Contact Center Select retrieves the customer's email messages from the email server, processes them (by keywords), and stores them in the database. Avaya Contact Center Select then generates a multimedia (email) contact for each email stored in the database, and routes it to an appropriate and available agent.

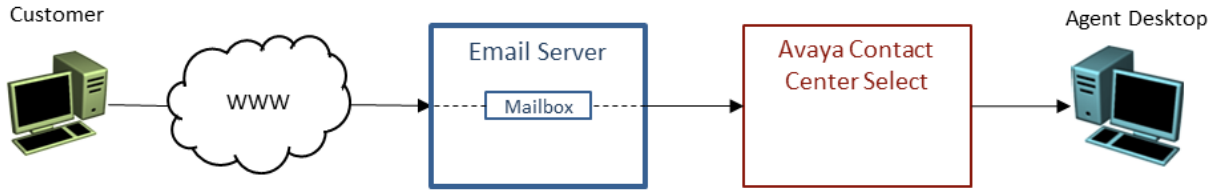


Figure 7: Avaya Contact Center Select process used to retrieve customer email messages and to route the messages as multimedia contacts to contact center agents

When you install Avaya Contact Center Select, you configure the email server and a default recipient mailbox. The default settings ensure email messages go only to an agent with the ability to handle email messages. You can customize your contact center with additional skillsets, rule groups and email servers.

To further enhance your customer service, you can configure routing rules to use in rule groups. Use keyword groups and sender groups to decide how to route contacts. Configure which skillset and priority the email contact is assigned to, based on the input for routing contacts. Use automatic suggestions for the agent to reply quickly to an email or automatic responses to send a reply to the customer without agent interaction. You can close the contact immediately after the automatic response.

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

For more information about configuring Avaya Contact Center Select email contacts and enhancing the customer experience, see *Avaya Contact Center Select Advanced Administration*.

Call Recording

Avaya Contact Center Select supports IP Office Call Recording. IP Office Call Recording provides regulatory type recording, including the option to pause automatic recording for Payment Card Industry (PCI) security compliance. Avaya Contact Center Select supports the Call Recording pause and resume feature when it is initiated from a physical phone set. By default, Avaya Contact Center Select agents have both inbound and outbound call recording enabled.

IP Office Call Recording has two main components:

- Voicemail Pro Voice Recording Library (VRL) records the inbound and outbound agent calls.
- IP Office Contact Recorder stores the recorded calls and associated metadata.

The recorded calls are stored in industry standard .WAV files. When each call is completed, Contact Recorder compresses the audio .wav file and updates the database with a record of the call. These files are stored in a hierarchy of folders on the IP Office server. Each recording results in a .wav file and the associated metadata stored in an XML file:

- Each .wav file contains the actual audio of the recording. Use the Contact Recorder Search and Replay application to locate and playback these recordings.
- Each .xml file contains metadata about the associated .wav recording file. The following are some examples of call recording metadata parameters:
  - Original CLI (P-Asserted-Identity)
  - Agent name
  - Skillset

- Agent number
- conference parties
- start time of the recorded call
- end time of the recorded call

IP Office Call Recording is a licensed feature. Recordings consume Voicemail Pro channel licenses.

Pause Recording when on Hold: If an Avaya Contact Center Select call is being recorded and the agent puts the call on hold, IP Office Call Recording puts the recording in a suspended state (not terminated), adds a short beep to the recording, and when the call is retrieved from hold the recording is resumed. This entire call is stored in a single .wav file.

User Pause recording: If an Avaya Contact Center Select call is being recorded, and if the agent needs to collect payment card details from a customer, the agent can pause the recording to comply with Payment Card Industry (PCI) requirements. IP Office Call Recording puts the recording in a suspended state (not terminated) and adds a short beep to the recording. After collecting the payment card details, the agent resumes call recording. This entire call is recorded and stored in a single .wav file.

The Agent Desktop user interface does not have a pause button. Agents and agent supervisors must use their physical phone to pause and resume voice contact recording.

Remote Agents

Avaya Contact Center Select (ACCS) supports Remote Agents. This feature allows agents at remote locations to use a phone and Agent Desktop software to handle customer voice contacts routed from ACCS.

ACCS supports the following types of Remote Agent:

- Remote Agents using an IPsec compliant Avaya VPN Router and an Avaya IP desk phone. The Internet Protocol Security (IPsec) compliant Virtual Private Network (VPN) router extends the ACCS network across a public network such as the internet, giving the remote agents secure access to the contact center solution. In this solution type, the agent has a computer, an Avaya IP desk phone, and an Avaya VPN Router in their home or at their remote workplace location. The agent's Avaya IP desk phone and Agent Desktop computer connect to the Avaya VPN Router. The VPN Router connects to ACCS using the internet. The agent uses their Avaya IP desk phone and Agent Desktop software to handle customer voice and multimedia contacts.
- Remote Agents using an IPsec compliant Avaya VPN Router and an Avaya IP Office softphone. The Internet Protocol Security (IPsec) compliant Virtual Private Network (VPN) router extends the ACCS network across a public network such as the internet, giving the remote agents secure access to the contact center solution. In this solution type, the agent has a computer and an Avaya VPN Router in their home or at their remote workplace location. The agent's Agent Desktop computer and IP Office softphone connect to the Avaya

VPN Router. The VPN Router connects to ACCS using the internet. The agent uses Agent Desktop software and the IP Office softphone to handle customer voice and multimedia contacts. ACCS Remote Agent supports IP Office Avaya Communicator for Windows.

- Remote Agents using their existing third-party telephones. In this solution type, the agent has a standard residential analog phone and a computer in their home or at their remote workplace location. The agent's phone connects to ACCS using the Public Switched Telephone Network (PSTN) and the Agent Desktop software connects to ACCS using the internet. This type of Remote Agent uses the Telecommuter mode of operation. The agent uses a standard analog phone and Agent Desktop software to handle customer voice and multimedia contacts.

  To enable Remote Agent Telecommuter mode:

  1. Enable the *Offsite Agent* feature in *Server Configuration - Licensing*
  2. For each remote agent, enable *Offsite Agent Allowed* for each remote agent in CCMA.
  3. The agents can then use Agent Desktop to log on from home or another remote location. Agents log on using one of their configured remote phone numbers.

To use Remote Agent, ACCS agents must have a suitable laptop or desktop computer in their home or at their remote workplace location. The agents install Agent Desktop software on this computer. The agents must have a fast and reliable internet connection to the contact center solution. For more information, see *Avaya IP Office Manager*.

Remote Agents log on to Agent Desktop using the *Other Phone* mode. When they log on, the agent telephone rings. This is a nail-up call. Agents must answer this call on their telephone to complete logging on to Agent Desktop. After the logon completes, the agent phone is nailed-up and agents must use Agent Desktop for all subsequent telephony operations. When the agent logs out of ACCS by using the Log Out button on Agent Desktop, ACCS disconnects the nailed-up call. Multimedia contact types appear to a remote agent in exactly the same way as they do to an onsite agent.

Avaya Contact Center Select domain and workgroup support

The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.

After you deploy the Avaya Contact Center Select Hardware Appliance or Software Appliance, you can add the Avaya Contact Center Select server to a Windows domain.

You can add the Avaya Contact Center Select server to a Windows domain before or after you install the Avaya Contact Center Select software using the Avaya Contact Center Select DVD.

In an Avaya Contact Center Select Business Continuity enabled solution, the Avaya Contact Center Select servers must be in the same Windows domain. To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active and standby servers. Avaya Contact Center Select agents are also supported in domains with a two-way trust relationship with

the Avaya Contact Center Select server domain. Avaya Contact Center Select Business Continuity is not supported in a workgroup.

Avaya Contact Center Select domain considerations

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

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

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

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

- Understand the ACCS services, ports, and user account requirements as specified by the ACCS firewall. For more information, see Microsoft Windows Firewall and Advanced Security on your ACCS server to view the inbound/outbound rules.
- Understand the ACCS network ports and transport types. For more information, see Avaya Contact Center Select port matrix on page 189.
- Design or modify your group policy to accommodate these existing ACCS services, ports, user accounts, and transport type requirements.
- Domain group policies and security policies can be configured to automate MS Windows updates, server backups, and password expiry rules for local users. These automated features are not supported by ACCS. If your group policies or security policies implement these automated features, place the ACCS servers in an Active Directory organizational unit (OU) container that protects the servers from these automated features.
- During Avaya Contact Center Select commissioning or during a maintenance window, apply and test your group policy. Ensure Avaya Contact Center Select call control, administration and maintenance capabilities are preserved. Do not apply an untested group policy to an Avaya Contact Center Select production environment. If necessary, modify your group policy to preserve Avaya Contact Center Select functionality.
- After successful testing, place ACCS back into production, and continue to monitor the contact center for adverse side effects of your group policy.

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

Avaya Contact Center Select servers do not support Dynamic Host Configuration Protocol (DHCP). All Avaya Contact Center Select servers must have a static IP address. Agent Desktop client computers support both DHCP and static IP addresses.

Avaya Security Advisories

Avaya Security Advisories are posted on the Avaya Security Support website at https://support.avaya.com/security. From the Avaya Support website, you can register to receive email notifications of Avaya Security Advisories.

The amount of time it takes to receive an Avaya Security Advisory varies depending on the vulnerability classification of the advisory. For more information about vulnerability classifications, responses, and maintenance policies, refer to the following documents:

- *Avaya's Product Security Vulnerability Response Policy*
- *Avaya's Security Vulnerability Classification*
- *Avaya's Maintenance Contract Requirements for Product Support*
- *Avaya Product Security Support Flow*

Avaya Contact Center Select Business Continuity

Business Continuity is an Avaya Contact Center Select (ACCS) licensed feature. ACCS solutions that support Business Continuity have two ACCS servers. One server, called the active server, processes customer contacts. The other ACCS server (standby or Remote Geographic Node) shadows the active server. If the active server fails, the other ACCS server can take over contact processing. This feature therefore provides ACCS redundancy, data resiliency, and disaster recovery.

For more information about Avaya Contact Center Select Business Continuity, see *Avaya Contact Center Select Business Continuity*.

Upgrades and migrations

Avaya Contact Center Select Release 7.0 is supported only on the Microsoft Windows Server 2012 Release 2 operating system. The Microsoft Windows Server 2012 R2 operating system and server must meet the requirements specified in *Avaya Contact Center Select Solution Description*. Avaya Contact Center Select supports only Microsoft Windows Server 2012 R2 Standard or Data Center editions.

Avaya Contact Center Select Release 6.4.2 is supported only on the Microsoft Windows Server 2008 R2 operating system. You cannot upgrade directly from Avaya Contact Center Select Release 6.4.2 on Windows Server 2008 R2 to Avaya Contact Center Select Release 7.0 on Windows Server 2012 R2. You can migrate agent and statistical information from your existing Avaya Contact Center Select Release 6.x solution to Avaya Contact Center Select Release 7.0 on a Windows Server 2012 R2 server.

You can apply the most recent Avaya Contact Center Select patches to ensure that you have the most recent version of the application software, to resolve software issues.

You can apply patches to an Avaya Contact Center Select Business Continuity solution. Both Avaya Contact Center Select servers must be updated to the same patch level. Updating an Avaya Contact Center Select Business Continuity solution requires careful up-front planning.

To install an Avaya Contact Center Select Feature Pack or Service Pack, or to migrate an Avaya Contact Center Select server, you must schedule a maintenance cycle and restart the contact center. For more information, read the Feature Pack or Service Pack Readme file.

Migrating from Avaya Contact Center Select to Avaya Aura® Contact Center is not supported.

Migrating from Avaya NES Contact Center to Avaya Contact Center Select is supported.

Migrating from an Avaya Aura® Contact Center AML-based solution to Avaya Contact Center Select is supported.

The following table summarizes the supported migrations to Avaya Contact Center Select Release 7.0.

Existing	New
Avaya Contact Center Select Release 7.0 on Microsoft Windows Server 2012 Release 2	Avaya Contact Center Select Release 7.0 Feature Pack 3 on Microsoft Windows Server 2012 Release 2
Avaya Contact Center Select Release 6.4.2 on Microsoft Windows Server 2008 R2	
Avaya Aura® Contact Center AML-based solutions	

Reporting Source of Call Disconnect

Avaya Contact Center Select (ACCS) records which party on a contact center call is the first to disconnect from the call. In a typical contact center call, the person who disconnects or hangs up first is the source of call disconnect (SOCD). ACCS supports SOCD monitoring and reporting for inbound contact center contacts. In some countries the agent must not hang-up on a contact center caller. For example, the Brazilian Presidential Decree 6.523 requires that an agent must not disconnect the call while talking to a caller who rang the contact center. Therefore, ACCS records the source of call disconnect (SOCD).

The SOCD information appears in the *Associated Data* field in the Call by Call and Contact Summary reports. The SOCD feature provides the following information about routed contact center contacts:

- Called Party: identifies that the agent disconnected the call
- Calling Party: identifies that the caller disconnected the call
- Transfer: identifies that an agent transferred the call and completed the transfer
- Conference Party: identifies that the caller or an agent dropped from a call that the initial agent conferenced

- Conference Tear Down: identifies that either the caller or the last agent dropped a call that an agent conferenced
- System: identifies that a system generated event released the call
- If a customer abandons the call, the ‘Disconnect Source’ is UNKNOWN but a ‘Final Disposition’ of abandoned is populated.

The following are some limitations of SOCD reporting:

- For direct (non contact center) calls to or from logged-in agents, SOCD is displayed as Unknown for all these call types.
- SOCD is recorded only for logged in ACCS agents. SOCD is not recorded if the ACCS agent is not logged in.
- If the agent that originally received the call starts a conference with another agent, and then drops from the conference, all subsequent SOCD information messages are Conference Tear Down. In this case, reports cannot show accurately which party dropped the call.

Automatically forward IP Office voicemail to multimedia agents

In an Avaya Contact Center Select (ACCS) solution licensed and configured to support multimedia agents, you can configure IP Office and Voicemail Pro to automatically forward voicemail messages to ACCS agents.

ACCS provides of sample *Customer Service* menu with a few basic options. This sample menu allows a caller to leave a voicemail message by selecting the voicemail option from the *Customer Service* menu. The caller is then routed to a pre-configured IP Office number from where they can leave a voicemail message. This pre-configured voicemail number is the *Callback Mailbox Number* option on the ACCS Ignition Wizard. Agents can use their phone and the IP Office voicemail system to listen to the caller’s voicemail message.

The IP Office administrator can configure the IP Office callback mailbox number and Voicemail Pro to automatically forward the voicemail message, as an email message with a .WAV file attachment, to an email address monitored by ACCS. ACCS can then treat the email contact and present it to an available multimedia agent. The agent can use their computer headphones to listen to the caller’s voicemail message in the .WAV file. ACCS agents cannot listen to .WAV file attachments using their IP Office phones.

For more information about forwarding voicemail messages to an email address, refer to your IP Office and Voicemail Pro documentation.

Limitations

The following are some of the limitations of Avaya Contact Center Select (ACCS) solutions:

- ACCS registers with IP Office as a SIP User. ACCS must refresh this active registration repeatedly every 180 seconds to prevent the registration expiring. If ACCS fails to refresh the registration, IP Office begins to terminate all active ACCS calls.
  - In the event of an ACCS service or network outage of less than 180 seconds, SIP registration with IP Office might expire and active ACCS calls might begin to terminate.
  - In the event of an ACCS service or network outage of greater than 180 seconds, SIP registration with IP Office expires and IP Office begins to terminate all active ACCS calls.
- If an ACCS agent is directly part of an IP Office conference call and the agent invokes hold on this call, music-on-hold is not streamed by IP Office even if the number of parties on this conference drops to two. Agents can identify whether they are part of this scenario by checking their phone set display for the ‘Conference’ keyword.
- Agent Desktop always uses 3–line appearance with reserve last call appearance, regardless of the IP Office settings on the agent’s phone. When an agent logs on using Agent Desktop, the Agent Desktop phone configuration overrides the IP Office phone configuration.
- For CDN to CDN conference, join, barge-in, or emergency call scenarios, if an IP Office softphone agent is a party on this multi-party conference call and invokes hold, music-on-hold might be played into the active multi-party audio stream for a short period of approximately 500 milliseconds before being terminated.
- If a customer dials an agent and this first agent then initiates a consultation with a second agent, the second agent’s phone displays the customer’s phone number while the consultation call is ringing. After the second agent answers the consultation call, their phone then displays the phone number of the first agent. This is how IP Office processes consultations.
- Call Intrude: The IP Office Call Intrude feature permits an agent to join or barge-in on another agent’s call. ACCS implements Call Intrude as a Join conference. The intruded agent’s call is briefly placed on-hold to allow the conference to complete. The intruded party might notice the Held state change and consult call leg appear briefly as the operation completes. Hold music might be played briefly to the Intruded party call.
- Manual transfer from softphone: A transfer completed manually on the IP Office softphone appears to Agent Desktop as a Join transfer where a Join is carried out on the main and consult calls with the transferring party then dropped from the call.
- IP Office supports third-party integrations using the IP Office TAPI interface. These third-party integrations can potentially interfere with the operation of Avaya Contact Center Select. You must configure, implement, and monitor third-party integrations to avoid interfering with Avaya Contact Center Select. Third-party applications implementing the IP Office TAPID interface are not supported for controlling Agent devices.

- Not all features invoked on the physical phoneset are reflected in Agent Desktop. The following scenarios are some examples of this:
  - Paging: Agents receiving an incoming Page call cannot answer this call using Agent Desktop. A Page call can be answered only on the user's phone. A Page call which is alerting on a user's phone is displayed in Agent Desktop as a connected call. Agent Desktop displays this call as connected if the user answers the Page. Agent Desktop drops this Page call if another user answers the Page.
  - Hold Reminder: If a call remains in the Held state longer than the IP Office system wide Hold Timeout configuration setting, then a Hold Reminder notification is displayed on the user's phone. A Hold Reminder notification can be an audio or visual notification. Agent Desktop does not support Hold Reminder notifications; in Agent Desktop the call remains in the Held state. Agents can use Agent Desktop to unhold the held call.
- When an ACCS agent logs on to an IP Office softphone, there is a short delay before the agent can use Agent Desktop software to control that softphone. This short delay can be up to 12 seconds long. Agents using an IP Office softphone are unable to answer incoming calls in Agent Desktop immediately after connecting the softphone to IP Office. However agents can answer these calls on their softphone. This limitation applies only to calls routed to the user in the immediate period after logging on to their softphone. If an agent attempts to answer a call in Agent Desktop during the short timeframe where answer is unavailable an error message is displayed in Agent Desktop. After the answer feature is available any subsequent attempts to answer a call in Agent Desktop are successful. But there is a limitation in that there is no notification in Agent Desktop that the Answer feature is now available.
- When an agent makes an outbound call using Agent Desktop, the Agent Desktop Hold button is immediately available. However, until the remote party answers the call and is connected, any attempt to Hold the call in Agent Desktop results in an error message being displayed.
- Avaya Contact Center Select does not support agent operation from the telephone only. This is commonly referred to as Telephone Mode only support. All Avaya Contact Center Select agents must use Agent Desktop for agent functionality.

The following are call flows that can experience limitations:

- Agent initiated calls (originate or transfer) to a Voicemail Pro call flow which invokes 'assisted transfer' telephony action to a Route Point CDN, are rejected by ACCS.
  - A workaround for this limitation is to use "Transfer" (blind transfer) on Voicemail Pro.
- Agent conferencing a call to a Voicemail Pro call flow which invokes any transfer telephony action ('assisted transfer' or 'transfer') to a Route Point CDN, can experience redirection limitations such as looping, redirected call being rejected by ACCS, incorrect CLID for the redirected call.
- Agent initiated calls to a remote expert where the remote expert forwards the call to a Route Point CDN, might be rejected by ACCS. The call might fail and can be retried.
- An agent conferencing a call (CC call or personal call) on ringing to a user which subsequently redirects the call to a Route Point CDN, causes ACCS to reject this redirected call. The agent remains on the call with the original caller and can reattempt the conference if desired.

- An agent transferring a call (CC call or personal call) on ringing to a user which subsequently redirects the call to a Route Point CDN, can intermittently cause the CLID of the redirected call to be intermittently incorrect. The agent that routed this redirected call might notice an incorrect CLID.

ACCS does not support single-step transfer of Contact Center (CDN) calls to another ACCS agent. The agent receiving the transferred call can answer the call on their phone, but the call is not presented in Agent Desktop and the agent appears as idle in reporting.

- ACCS agents using Avaya Communicator.

  When working on a call in Avaya Communicator, selecting the ‘Transfer’ option from the drop-down menu associated with the call results in a single-step transfer. This is not supported by ACCS. The workaround is to use Agent Desktop to transfer CDN calls. Alternatively, instead of selecting the ‘Transfer’ option from the drop-down menu in Avaya Communicator, make an unrelated outbound call to the CDN. Then, in Avaya Communicator, drag the two calls together and select ‘Transfer’ from the resulting menu.

- ACCS agents using 1140E/1230 SIP desk phones.

  When transferring a call manually using 1140E/1230 SIP desk phones, the user is prompted Yes/No to consult with the destination party. Selecting ‘No’ results in a single-step transfer. This is not supported by ACCS. The workaround is to use Agent Desktop to transfer CDN calls. Alternatively, when using 1140E/1230 SIP desk phones to transfer calls, select ‘Yes’ to consult with the destination party.

ACCS agents must not configure Forward on No Answer (FONA) to the DN of another ACCS agent. A Contact Center (CDN) call transferred on ringing to an ACCS agent with FONA configured to another ACCS agent is not supported by ACCS. When FONA is applied and the call is forwarded, the ACCS agent receiving the forwarded call can answer the call on their endpoint but the call is not presented in Agent Desktop and the agent appears to be idle in reporting.

For ACCS agents using SIP endpoints (1140E/1230 desk phones, Avaya Communicator for Windows, or IP Office Softphone), a consult transfer/conference call initiated from the SIP endpoint cannot be completed using Agent Desktop. Avaya recommends that agents use Agent Desktop for both the initiation and completion of transfers and conferences.

ACCS agents using IP Office Softphones can experience some limitations when performing Hold/Unhold in Agent Desktop after being transferred to another party. The limitation occurs only when an ACCS agent using IP Office Softphone is transferred to an IP Office user who is also using an IP Office Softphone or Avaya 1140E/1230 desk phones. In Agent Desktop, the Hold/Unhold request does not work, the call state does not change on the IP Office Softphone, and Agent Desktop does not display an error message. In a limited number of cases, due to a limitation of the IP Office Softphone, the call can drop after a period of time. This limitation does not apply to customer calls or when either leg of the transfer operation is a Contact Center (CDN/Route Point) call. To avoid this limitation, Avaya recommends that ACCS agents using IP Office Softphone perform Hold/Unhold operations using the IP Office Softphone.

Note:

Ensure the Avaya Contact Center Select *Redirection* feature is enabled. To enable redirection, log on to Contact Center Manager Administration and navigate to **Configuration** > **Global Settings** > **Redirection Settings** > **Media Shuffling on Transfer**.

Chapter 4: Avaya Contact Center Select DVD

The Avaya Contact Center Select DVD software provides a context-sensitive, collaborative, voice and multimedia customer experience solution that allows small to midsize enterprises to anticipate, accelerate, and enhance customer interactions. Avaya Contact Center Select uses the Avaya IP Office telephone system to provide a real-time telephony platform. Avaya IP Office is a flexible and scalable phone system designed specifically for small and midsize enterprises. IP Office supports a wide range of phones and devices for use in contact centers.

The Avaya Contact Center Select DVD deployment option supports Platform Vendor Independence (PVI). PVI gives the customer the flexibility to purchase a server that meets the Avaya Contact Center Select server requirements and conforms to the customer's corporate standards. To use the Avaya Contact Center Select DVD deployment option, the customer must provide the following:

- Server hardware that meets the Avaya Contact Center Select Platform Vendor Independence (PVI) specification.
- Microsoft Windows 2012 Release 2 Standard or Datacenter Edition operating system and license.

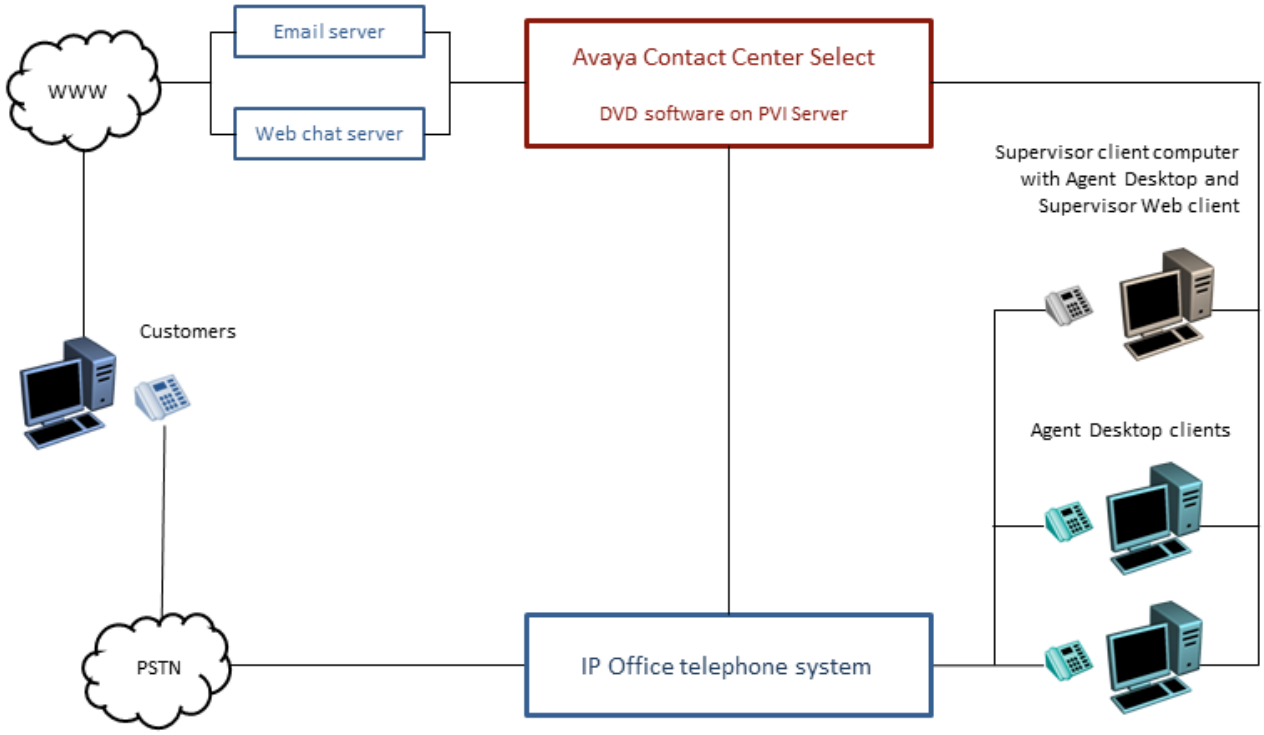


Figure 8: Topology of a typical Avaya Contact Center Select solution

Avaya Contact Center Select is preloaded with sample users, skillsets, and contact center parameters. You can use this sample data to rapidly commission the solution and make the first routed call and email contact. Avaya Contact Center Select delivers quick and simplified contact center deployment. After the basic telephony features are working, you can then configure multimedia contacts, multiplicity, custom prompts, other enhanced features and functions to improve your customer's experience.

To deploy Avaya Contact Center Select software using the DVD software, perform the following:

- Obtain a server that meets the Avaya Contact Center Select PVI requirements.
- Configure the server and format the hard disk partitions to the required specifications.
- Install the Microsoft Windows 2012 Release 2 Standard or Datacenter edition operating system.
- License and activate the Microsoft Windows 2012 R2 operating system.
- Obtain an Avaya Contact Center Select DVD and license.
- Use the Avaya Contact Center Select DVD to install the software components and applications.
- Use the Avaya Contact Center Select Configuration Ignition Wizard to rapidly deploy a functional contact center solution.

The Avaya Contact Center Select DVD is supported only on the Microsoft Windows 2012 Release 2 Standard or Datacenter edition operating system.

The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.

Note:

The Avaya Contact Center Select with Avaya Aura® Media Server DVD deployment option does not support VMware.

Platform Vendor Independence server specification

The Avaya Contact Center Select DVD deployment option supports Platform Vendor Independence (PVI). PVI gives the customer the flexibility to purchase a server that meets the Avaya Contact Center Select server requirements and conforms to the customer's corporate standards. To use the Avaya Contact Center Select DVD deployment option, the customer must provide server hardware that meets the Avaya Contact Center Select PVI specification.

The Avaya Contact Center Select DVD deployment option supports the following PVI server specifications:

- Entry-level server specification on page 65
- Mid-range server specification on page 66
- High end server specification on page 68

The high-end server specifications support the same maximum agent capacity and call rate figures. The mid-range server specification supports a reduced agent capacity and call rate.

For information about achieving the maximum performance from your server hardware, see Server performance and BIOS settings on page 70.

Entry-level server specification

The following table lists the minimum specifications for an entry-level single 4-core server.

Specification	Configuration	Comment
CPU	Single 4-core Intel Xeon E3-1275L v3 2.70 GHz	Select a CPU that meets or exceeds the benchmark rating for the Intel Xeon E3-1275L v3 2.70 GHz CPU. Relative benchmark comparisons only apply for CPUs with the same number of cores. You can make CPU comparisons by viewing the benchmarked High End CPU passmark rankings here: http://www.cpubenchmark.net • AMD processors are not supported.
CPU - Minimum Clock Speed	2400 MHz	CPU clock speed must meet or exceed the minimum clock speed of 2400 MHz.

Table continues…

Specification	Configuration	Comment
CPU - Required Technologies	Hyper-Threading	• 1 x additional logical core for each physical core. • Hyper-Threading must be enabled.
RAM	32 GB minimum	For maximum performance, Avaya recommends that all DIMM slots are populated.
Disk Type and Speed	SATA, SAS, minimum 10000 RPM	• Avaya recommends using 15000 RPM disks. • Solid State Drives (SSDs) are not supported.
Total Disk size	• 900 GB minimum • 1.2 TB recommended	• 900 GB disks required for 300 GB Multimedia partition. • 1.2 TB disks required for 600 GB Multimedia partition. Avaya recommends a 600 GB multimedia partition to support longer offline data retention. • For information about the hard disk partitions, see Contact Center hard disk partition sizes on page 69.
RAID	Hardware RAID 1, RAID 5, or RAID 10	• Battery backed hardware RAID controller with 512 MB cache minimum. • Requires duplicate drives with identical specifications.
DVD Drive	One dual-layer DVD drive	• 16X or faster recommended • DVD/Blu-Ray combo drives are supported.
Network Interface	Dual NIC 1 Gbit/s or faster	• NIC must support Receive Side Scaling (RSS) with a minimum of 4 queues and minimum Receive Buffer size of 500. • Only Ethernet is supported.

For information about achieving the maximum performance from your server hardware, see Server performance and BIOS settings on page 70.

Mid-range server specification

The following table lists the minimum specifications for a mid-range dual 6–core server.

Specification	Configuration	Comment
CPU	Dual 6–core Intel Xeon X5660 2.80 GHz	Select a CPU that exceeds the benchmark rating for the Dual 6–core Xeon Intel Xeon X5660 2.80 GHz. Relative benchmark comparisons only apply for CPUs with the same number of cores. You can make CPU comparisons by viewing the benchmarked High End CPU passmark rankings here: http://www.cpubenchmark.net • AMD processors are not supported.
CPU - Minimum Clock Speed	2400 MHz	CPU clock speed must meet or exceed the minimum clock speed of 2400 MHz.
CPU - Required Technologies	Hyper-Threading	• 1 x additional logical core for each physical core. • Hyper-Threading must be enabled.
RAM	32 GB minimum	For maximum performance, Avaya recommends that all DIMM slots are populated.
Disk Type and Speed	SAS, minimum 10000 RPM	• Avaya recommends using 15000 RPM disks. • Solid State Drives (SSDs) are not supported.
Total Disk size	• 900 GB minimum • 1.2 TB recommended	• 900 GB disks required for 300 GB Multimedia partition. • 1.2 TB disks required for 600 GB Multimedia partition. Avaya recommends a 600 GB multimedia partition to support longer offline data retention. • For information about the hard disk partitions, see Contact Center hard disk partition sizes on page 69.
RAID	Hardware RAID 1, RAID 5, or RAID 10	• Battery backed hardware RAID controller with 512 MB cache minimum. • Requires duplicate drives with identical specifications.
DVD Drive	One dual-layer DVD drive	• 16X or faster recommended • DVD and Blu-Ray combo drives are supported.

Table continues…

Specification	Configuration	Comment
Network Interface	Dual NIC 1 Gbit/s or faster	• NIC must support Receive Side Scaling (RSS) with a minimum of 4 queues and minimum Receive Buffer size of 500. • Only Ethernet is supported.

For information about achieving the maximum performance from your server hardware, see Server performance and BIOS settings on page 70.

High-end server specification

The following table lists the minimum specifications for a high-end server with dual 8–core CPU.

Specification	Configuration	Comment
CPU	Dual 8–core Intel Xeon E5-2670 2.60GHz	Select a CPU that equals or exceeds the benchmark rating for the Dual 8–core Intel Xeon E5-2670 60GHz CPU. Relative benchmark comparisons only apply for CPUs with the same number of cores. You can make CPU comparisons by viewing the benchmarked High End CPU passmark rankings here: http://www.cpubenchmark.net **Note:** CPUs based on more than 12 cores are not supported • AMD processors are not supported.
CPU - Minimum Clock Speed	2400 MHz	CPU clock speed must meet or exceed the minimum clock speed of 2400 MHz.
CPU - Required Technologies	Hyper-Threading	• 1 x additional logical core for each physical core. • Hyper-Threading must be enabled.
RAM	32 GB minimum	For maximum performance, Avaya recommends that all DIMM slots are populated.
Disk Type and Speed	SAS, minimum 10000 RPM	• Avaya recommends using 15000 RPM disks. • Solid State Drives (SSDs) are not supported.

Table continues…

Specification	Configuration	Comment
Total Disk size	• 900 GB minimum • 1.2 TB recommended	• 900 GB disks required for 300 GB Multimedia partition. • 1.2 TB disks required for 600 GB Multimedia partition. Avaya recommends a 600 GB multimedia partition to support longer offline data retention. • For information about the hard disk partitions, see Contact Center hard disk partition sizes on page 69.
RAID	Hardware RAID 1, RAID 5, or RAID 10	• Battery backed hardware RAID controller with 512 MB cache minimum. • Requires duplicate drives with identical specifications.
DVD Drive	One dual-layer DVD drive	• 16X or faster recommended. • DVD and Blu-ray combo drives are supported.
Network Interface	Dual NIC 1 Gbit/s or faster	• NIC must support Receive Side Scaling (RSS) with a minimum of 4 queues and minimum Receive Buffer size of 500. • Quad NICs are required for virtualized environments where this server is a VMware ESXi host. • Only Ethernet is supported.

For information about achieving the maximum performance from your server hardware, see Server performance and BIOS settings on page 70.

Contact Center hard disk partition sizes

Select your hard disk size and configure the required partitions. For each partition, specify a volume size in MBs that when formatted results in a disk partition that is equal to or greater than the required minimum partition size.

For improved multimedia offline data retention, Avaya recommends using 1.2 TB hard disks with a 600 GB partition for multimedia storage.

Table 1: Contact Center hard disk minimum partition sizes

Hard disk drive partition description	Drive letter	900 GB hard disk Minimum size partition	1.2 TB hard disk Minimum size partition
Operating System drive Excluding the 350 MB Windows boot loader *System Reserved* partition.	C:	80 GB NTFS partition	80 GB NTFS partition
Application drive	D:	120 GB NTFS partition	120 GB NTFS partition
DVD drive For continuity and consistency, Avaya recommends using Drive letter E: for the DVD drive. However, Contact Center supports any DVD Drive letter, other than the Drive letters listed here for the hard disk partitions.	E:	—	—
Voice Contact Server database drive	F:	200 GB NTFS partition	200 GB NTFS partition
Multimedia Contact Server database drive	G:	300 GB NTFS partition	600 GB NTFS partition
Database journal drive	H:	100 GB NTFS partition	100 GB NTFS partition
	Total	801 GB of NTFS partitions on a formatted 900 GB hard disk.	1101 GB of NTFS partitions on a formatted 1.2 TB hard disk.

Contact Center requires Hardware RAID-1 with duplicate hard disk drives with identical specifications. Therefore as a minimum, the Contact Center server must have two 900 GB hard disks or two 1.2 TB hard disks with identical specifications.

Server performance and firmware settings

The Basic Input Output System (BIOS) of a server configures the hardware components and boots the operating system from a storage device. The server operating system (OS) then uses the BIOS to control the server hardware. You must configure the server BIOS settings to ensure optimum performance from the underlying server hardware. For most BIOS settings, you must choose between optimizing a server for power savings or for server performance. For real-time applications such as Avaya Contact Center Select, you must always choose the server BIOS settings that ensure the optimum performance from the underlying server hardware.

Server manufacturers provide their own motherboards, BIOS, hardware, and firmware. Determining the BIOS configuration for your server’s hardware can be challenging. There are several BIOS settings that can significantly impact the system performance. When optimizing for

system performance, you must select the BIOS settings that enhance the system performance over those that contribute to power savings. Other BIOS settings and recommendations are not as straight forward. Start by consulting the manufacturer's technical data for your server. Avaya recommends that you then test your solution in order to make the best BIOS configuration decisions.

Configure the server hardware, firmware, and Operating System settings to select system performance over power savings.

Server firmware

Firmware is a computer program that is stored on the server motherboard or on an add-on hardware controller. The firmware stored on the server motherboard is called the Basic Input Output System (BIOS). The BIOS is responsible for the behavior of the system when it is first switched on and for passing control of the server to the operating system. Firmware is also stored in hardware components such as Redundant Array of Independent Disks (RAID) controllers.

Routinely consult the manufacturer's technical data for your servers and, where appropriate, apply the most recent BIOS and firmware updates. The steps required to update firmware or a system BIOS vary depending on the hardware vendor and the component to be updated. Typically, the manufacturer supplies a firmware updating utility. Keeping your server BIOS and firmware at a supported level can improve reliability, serviceability, and help ensure optimum performance.

Unified Extensible Firmware Interface

The Unified Extensible Firmware Interface (UEFI) specification defines the interface between the operating system and the server firmware. Similar to the BIOS, UEFI is installed by the server manufacturer and it is the first program to run when the server is turned on. UEFI firmware provides some technical advantages over the traditional BIOS system.

Contact Center software, when deployed on physical servers, supports UEFI.

Contact Center software, when deployed on VMware virtual machines, does not support UEFI.

Contact Center does not support the UEFI Secure Boot feature.

Select the firmware boot option, BIOS or UEFI, on the server before installing the Windows Server 2012 R2 Operating System and the Contact Center software. Refer to your hardware vendor's documentation on how to change and implement the required firmware boot option. Changing the firmware boot option after the Operating System has been installed renders the server unbootable and this is not supported.

Power and performance management

For real-time applications such as Avaya Contact Center Select, you must always select the hardware, BIOS, firmware, and Operating System settings that enhance the system performance over those that contribute to power savings.

Intel Xeon CPUs offer two main power management options: C-states and Intel Turbo Boost.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to full power on.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power.

These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described below. Other server makes and models can have other terminology but equivalent BIOS settings.

The following are the recommended BIOS settings for the Dell PowerEdge servers:

- Set the Power Management Mode to Maximum Performance.
- Set the CPU Power and Performance Management Mode to Maximum Performance.
- Processor Settings: set Turbo Mode to enabled
- Processor Settings: set C States to disabled

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to Static High Mode.
- Disable Processor C-State Support
- Disable Processor C1E Support
- Disable QPI Power Management
- Enable Intel Turbo Boost

Configure the server hardware, firmware, and Operating System settings to select system performance over power savings.

Disk caching and RAID

Hard disk drives use cache memory to improve read and write access to the disk drives. In write-back mode caching, the disk or RAID controller writes data from the server to cache memory and acknowledges write completion to the server. The server is free to perform other tasks while the disk controller transfers the data from the write cache to the disk drives. This approach significantly increases write performance.

Avaya Contact Center Select supports hardware RAID-1, RAID-5, and RAID-10. RAID technology provides disk data redundancy as well as error detection and correction. For maximum security and mission-critical solutions, Avaya recommends that all Contact Center servers contain a RAID

controller. Hardware RAID-1, RAID-5, and RAID-10 are the only levels and types of RAID supported.

Read the hardware documentation for your server to determine how to configure disk caching. Typically, disk caching can be configured as a BIOS setting, a RAID setting, a RAID controller setting, or as an Operating System setting. Some RAID controllers expose the ability to manipulate the Caching Policy through the OS and therefore the OS level setting can override the BIOS level setting. Refer to your hardware documentation for more information about configuring disk caching. Avaya Contact Center Select does not support Operating System level disk caching, software disk caching, or software RAID. Avaya Contact Center Select requires battery backed hardware RAID caching to avoid data loss and possible database corruption on power outage.

Non-Uniform Memory Architecture and memory

Non-uniform memory access (NUMA) is a computer memory design used in multiprocessing, where the memory access time depends on the memory location relative to the processor. Using NUMA, a processor can access its own local memory faster than non-local memory (memory local to another processor or memory shared between processors). For Avaya Contact Center Select, the server must support and implement NUMA.

In the server BIOS settings, configure the memory operating mode for performance optimization and disable Node Interleaving. For example, for a Dell server configure “Memory Operating Mode” as “Optimizer Mode”, and configure “Node Interleaving” as “Disabled”. Refer to your hardware documentation for more information about NUMA and memory performance.

Hyper-Threading

Hyper-Threading is Intel’s proprietary technology for increasing parallel computational power (processor multi-tasking) by allowing the operating system (OS) to see and address each physical processor core as if it were two virtual processors. It also enables the OS and applications to share work between those virtual processors whenever possible, thereby making full use of the available resources.

Enable Hyper-Threading on the Avaya Contact Center Select server.

Unused hardware devices

On the server, disconnect or disable unused and unnecessary physical hardware devices such as: COM ports, LPT ports, USB controllers, Network interfaces, and Storage controllers. You must retain some USB devices for the mouse and keyboard. Disabling unnecessary hardware devices improves server performance and security. Consult the manufacturer’s technical data for your servers for information about disabling unused hardware devices in the BIOS.

Summary

For real-time applications such as Avaya Contact Center Select, choose server BIOS settings that optimize for performance in preference to power savings. Start by consulting the manufacturer's technical data for your server. Avaya recommends that you then test your solution in order to make the best BIOS configuration decisions. Avaya recommends that you enable CPU Hyper-Threading. By enabling BIOS options such as CPU Prefetchers and CPU Hyper-Threading, the system performance can be improved effectively. When tuning system BIOS settings for performance, you must consider the various processor and memory options. Experiment with other options to find the optimum setting for your specific hardware and Contact Center solution.

Configure the server hardware, BIOS, firmware, and Operating System settings to select system performance over power savings.

Avaya Contact Center Select DVD software specification

The Avaya Contact Center Select DVD contains the following software components:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)
- Contact Center Multimedia (CCMM)
- Avaya Aura® Media Server Hyper-V instance on the Windows Server 2012 server
- Avaya Contact Center Select Firewall policy
- Default Avaya Contact Center Select configuration data
- Configuration Ignition Wizard

The Avaya Contact Center Select DVD is supported only on the Microsoft Windows 2012 Release 2 Standard or Datacenter edition operating system.

Server naming requirements

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

- Use only characters a to z, A to Z, and 0 to 9 can be used in a host name.

- You can use a hyphen (-), but not to start or end the host name.
- Host names must be 6 to 15 characters in length.
- Host names must not start with a number.
- Do not use the underscore character (_) and period character (.).
- Do not use spaces in the host name.

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

If network connectivity on your network requires the use of Fully Qualified Domain Names (FQDN), then the FQDN of each computer must be resolvable between all servers associated with Contact Center.

Microsoft security hotfixes

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

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

Operating system updates

Operating system updates includes service updates and service packs.

Service updates

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

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

Whenever possible, Avaya incorporates the most recent operating system security recommendations and service updates in an integrated solutions testing strategy during each test

cycle. However, due to the urgent nature of security service updates when vulnerabilities are discovered follow Microsoft guidelines as they are issued, including any Microsoft installation procedures and security service update rollback processes.

Finally, you must perform a full system backup before you update the system to ensure that a rollback is possible, if required. If a Contact Center application does not function properly after you apply a Microsoft security service update, you must remove the service update and revert to the previous version of the application (from the backup you made before applying the service update). For added security, always determine whether Avaya verified the Microsoft service update for compatibility with Contact Center Manager.

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

Service packs

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

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

Important:

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

Java Runtime Environment updates

Contact Center supports only specific versions of Java Runtime Environment (JRE). During installation, Contact Center disables JRE automatic updates on the contact center servers.

Important:

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

Dynamic Host Configuration Protocol support

Contact Center applications (CCMS, CCMA, CCT, CCMM, LM, and Avaya Aura® Media Server) do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Agent Desktop client computers support both DHCP and static IP addresses.

Third-party software requirements

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

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

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

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

Generic guidelines for utility-class software applications

The following are generic guidelines for utility-class software:

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

Guidelines for the use of antivirus software

This section describes the Avaya Contact Center Select antivirus software requirements.

Avaya Contact Center Select supports the following antivirus products:

- Symantec Antivirus
- McAfee

For more information about Avaya Contact Center Select anti-virus considerations and supported versions, see *Avaya Contact Center Select Security Reference Guide* available from the Avaya Support website at http://support.avaya.com.

You can deploy antivirus products from other vendors subject to the following guidelines:

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

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

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

- `F:\Avaya\Contact Center\Databases\`
- `<additional database drive>:\Avaya\Contact Center\Databases\`
- TSM_OAM files located in the following folders:
  - 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
- `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\Contact Center\Common Components\CMF`
- `D:\Avaya\Contact Center\Manager Administration\Apps\` (including sub-directories)
- The folder where you store Service Packs and patches

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

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the email server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Avaya Contact Center Select 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.
- Ensure the antivirus software is configured to permit outbound email messages. For example, configure the McAfee antivirus software *Access Protection* option not to block *Prevent mass mailing worms from sending mail*. Alternatively, add the Contact Center Multimedia “EmailManager.exe” process to the McAfee *Processes to exclude* list.

  Exclude the Contact Center Multimedia database partition from being scanned.
- If firewalls on individual computers are enabled on the Agent Desktop computer, the Report Listener might be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.
- You must not enable the Microsoft Updater to Auto-Run. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

Warning:

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

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

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

Exclude the Caché Journal file folder; `G:\Avaya\`

For Avaya Aura® Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

- `D:\Avaya\MAS\Multimedia_Applications\MAS\platdata`
- `D:\Avaya\MAS\Multimedia_Applications\MAS\common\log`

Avaya Contact Center Select DVD licensing

The Avaya Contact Center Select DVD deployment option requires a Nodal Enterprise license delivered as a WebLM XML file. This license file is used to control access to licensed features such as multimedia contacts and multiplicity.

Contact Center License Manager provides central control and administration of licensing for Avaya Contact Center Select. Each Contact Center License Manager includes a local instance of WebLM. When the Contact Center License Manager service starts, it extracts WebLM license keys from the local WebLM instance. Contact Center License Manager then converts the WebLM license keys into local PLIC license keys and distributes the keys the Avaya Contact Center Select applications as required.

- Obtain the WebLM Host ID for your Avaya Contact Center Select server.
- Use the WebLM Host ID to obtain a nodal WebLM license file from the Avaya Product Licensing and Delivery System (PLDS).
- You load the license file onto the Avaya Contact Center Select server as you run the configuration utility when you are deploying the Avaya Contact Center Select server. You can also load the license file after the configuration process. When Contact Center License Manager loads the license, if the unique number in the license does not match the WebLM Host ID, then License Manager shuts down and Avaya Contact Center Select cannot process contacts. If the unique number in the license matches the WebLM Host ID, then License Manager provides license keys, and Avaya Contact Center Select processes customer contacts.

Chapter 5: Avaya Contact Center Select software appliance

For increased productivity, efficiency, and flexibility, Avaya Contact Center Select supports VMware virtualization.

You can use a single Open Virtual Appliance (OVA) package to distribute a virtual appliance. For example, an Avaya Aura® Media Server OVA package includes all of the Open Virtualization Format (OVF) information required to create an Avaya Aura® Media Server virtual appliance on a VMware host. A virtual appliance contains a preinstalled, preconfigured operating system and an application stack optimized to provide a specific set of services.

Avaya Contact Center Select offers a software appliance package that consists of the following components:

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

The Avaya Aura® Media Server and Avaya WebLM OVAs are prepackaged and ready for deployment. For the Avaya Contact Center Select virtual machine, you must build a suitably specified virtual machine and then install product software from the Avaya Contact Center Select DVD or ISO image.

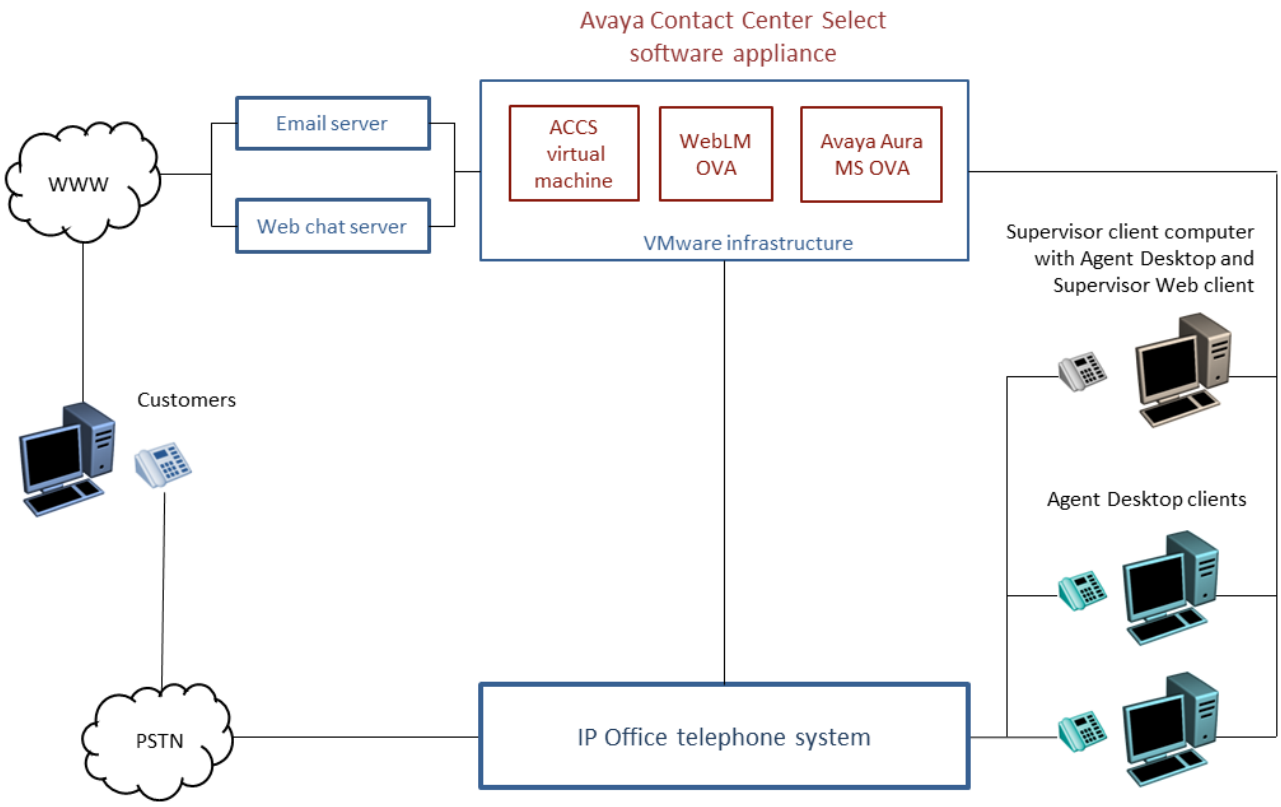


Figure 9: Typical virtualized contact center solution using Avaya Contact Center Select, Avaya Aura® Media Server, and Avaya WebLM deployed on a single VMware host server

You can use VMware vSphere or vCenter and these components to create virtual machines in your virtualized environment. The OVA packages are created as VMware hardware version 8 archives.

The Avaya Contact Center Select software appliance is supported only with the following virtualization environments:

- ESXi 5.5
- ESXi 6.0
- ESXi 6.5

Note:

VMFS 5.54 or later is required for all supported versions of ESXi.

Avaya Contact Center Select supports the Avaya WebLM virtual machine co-resident on the same VMware host server or deployed on a separate VMware host server.

Avaya Contact Center Select supports the Avaya Aura® Media Server virtual machine co-resident on the same VMware host server or deployed on a separate VMware host server.

For more information about the Avaya Contact Center Select software appliance components, see the following:

- Avaya Contact Center Select virtual machine on page 83
- Avaya Aura Media Server OVA on page 90
- Avaya WebLM OVA on page 91

Avaya Contact Center Select virtual machine

Create the Avaya Contact Center Select virtual machine to provide context-sensitive and skill-based routing for customer voice and multimedia contacts.

The Avaya Contact Center Select virtual machine (guest) contains the following contact center application software.

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)
- Default Avaya Contact Center Select configuration data
- Firewall policy

To create the Avaya Contact Center Select virtual machine, perform the following:

1. Create a VMware virtual machine with the hardware characteristics:
2. Install the Windows Server 2012 Release 2 Standard or Datacenter edition English operating system on the virtual machine.
3. License and activate the Microsoft Windows 2012 R2 operating system.
4. Configure the server and format the hard disk partitions to the required specifications.
5. Install VMware Tools on the server.
6. Obtain an Avaya Contact Center Select DVD or ISO image.
7. Obtain an Avaya Contact Center Select license file.
8. Use the Avaya Contact Center Select DVD or ISO image to install the software components and applications.
9. Use the Avaya Contact Center Select Configuration Ignition Wizard to rapidly deploy a functional contact center solution.

10. Continue to monitor the VMware real-time resources.

Each Avaya Contact Center Select virtual machine requires a Linux-based Avaya Aura® Media Server. Each Avaya Contact Center Select virtual machine also requires an additional, separate, Avaya WebLM licensing manager server.

Contact Center virtual machine hard disks and partitions

Create individual virtual hard disks for each of the required partitions for your Contact Center virtual machine. When creating a virtual hard disk for the Operating System partition, create a hard disk size 1GB greater that the required partition size to accommodate the creation of any additional Windows partitions which might be created automatically as part of the Windows Server 2012 R2 install.

For example, for an Operating System partition size requirement of 80GB, create an 81GB virtual hard drive. For each additional Contact Center required partition, create a virtual hard drive greater than or equal to the partition size requirement. The virtual hard disk must be of sufficient size such that when the associated partition is created and formatted it has a size matching the required partition size for the install.

For improved multimedia offline data retention, Avaya recommends using a 600 GB partition for multimedia storage. The multimedia 600 GB partition requires SAN Storage.

Table 2: Contact Center Virtual Machine hard disk minimum partition sizes

Hard disk drive partition description	Drive letter	Minimum partition sizes	Recommended partition sizes, 300 GB multimedia partition	Recommended partition sizes, 600 GB multimedia partition
Operating System drive	C:	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition
Application drive	D:	100 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition
DVD drive	E:	—	—	—
Voice Contact Server database drive	F:	180 GB NTFS partition	200 GB NTFS partition	200 GB NTFS partition
Multimedia Contact Server database drive	G:	200 GB NTFS partition	300 GB NTFS partition	600 GB NTFS partition
Database journal drive	H:	80 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition
	Total	641 GB of Thick Provisioned disk space in a VMware datastore.	801 GB of Thick Provisioned disk space in a VMware datastore.	1101 GB of Thick Provisioned disk space in a SAN datastore.

If using 900 GB Raid–1 disks, use the above Minimum Partition size option.

Contact Center requires Hardware RAID-1 with duplicate hard disk drives with identical specifications. Therefore, the VMware host server must implement Hardware RAID-1 or better.

Server naming requirements

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

- Use only characters a to z, A to Z, and 0 to 9 can be used in a host name.
- You can use a hyphen (-), but not to start or end the host name.
- Host names must be 6 to 15 characters in length.
- Host names must not start with a number.
- Do not use the underscore character (_) and period character (.).
- Do not use spaces in the host name.

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

If network connectivity on your network requires the use of Fully Qualified Domain Names (FQDN), then the FQDN of each computer must be resolvable between all servers associated with Contact Center.

Microsoft security hotfixes

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

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

Operating system updates

Operating system updates includes service updates and service packs.

Service updates

Given the number of operating system security service updates and the complexity inherent in any network, create a systematic and accountable process for identifying and applying service

updates. To help create such a process, you can follow a series of best practices guidelines, as documented in the National Institute of Standards and Technology (NIST) Special Bulletin 800-40, Procedures for Handling Security Patches.

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

Whenever possible, Avaya incorporates the most recent operating system security recommendations and service updates in an integrated solutions testing strategy during each test cycle. However, due to the urgent nature of security service updates when vulnerabilities are discovered follow Microsoft guidelines as they are issued, including any Microsoft installation procedures and security service update rollback processes.

Finally, you must perform a full system backup before you update the system to ensure that a rollback is possible, if required. If a Contact Center application does not function properly after you apply a Microsoft security service update, you must remove the service update and revert to the previous version of the application (from the backup you made before applying the service update). For added security, always determine whether Avaya verified the Microsoft service update for compatibility with Contact Center Manager.

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

Service packs

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

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

Important:

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

Java Runtime Environment updates

Contact Center supports only specific versions of Java Runtime Environment (JRE). During installation, Contact Center disables JRE automatic updates on the contact center servers.

Important:

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

Dynamic Host Configuration Protocol support

Contact Center applications (CCMS, CCMA, CCT, CCMM, LM, and Avaya Aura® Media Server) do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Agent Desktop client computers support both DHCP and static IP addresses.

Third-party software requirements

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

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

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

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

Generic guidelines for utility-class software applications

The following are generic guidelines for utility-class software:

- During run-time, the utility must not degrade the contact center application beyond an average percentage of CPU use (see each specific application section in this document for the recommended maximum CPU usage level). Furthermore, the utility must not lower the minimum amount of free hard disk space required by contact center application and the Windows Operating system.
- The utility must not cause improper software shutdowns or out-of-sequence shutdowns.
- The utility must not administer the contact center application.
- If the utility has a database, it must not affect the contact center application database.
- Disk compression utilities must not be used.
- Memory tweaking utilities used to reclaim memory that is unused by Microsoft must not be used.

- The installation or uninstallation of the third-party software must not impact or conflict with the contact center application (for example, it must not cause DLL conflicts). If such conflicts are discovered, a server rebuild might be necessary.
- The implementation personnel must perform tests to ensure these conditions and recommendations are met before you place the Contact Center application into production. Support personnel can ask for the results of the testing during fault diagnosis. As part of fault diagnosis, the distributor or end user might be asked to remove third-party software.
- HyperTerminal must not be installed on the server as it interferes with the operation of Contact Center.

Guidelines for the use of antivirus software

This section describes the Avaya Contact Center Select antivirus software requirements.

Avaya Contact Center Select supports the following antivirus products:

- Symantec Antivirus
- McAfee

For more information about Avaya Contact Center Select anti-virus considerations and supported versions, see *Avaya Contact Center Select Security Reference Guide* available from the Avaya Support website at http://support.avaya.com.

You can deploy antivirus products from other vendors subject to the following guidelines:

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

- Product Support does not provide support on the configuration of antivirus software, but offer guidance where possible. Direct questions or problems on antivirus software to the appropriate vendor.
- If performance or functionality issues are raised to Avaya support personnel as part of the fault diagnosis, you might be asked to remove third-party utility software or antivirus software.

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

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

- `F:\Avaya\Contact Center\Databases\`
- `<additional database drive>:\Avaya\Contact Center\Databases\`
- TSM_OAM files located in the following folders:
  - 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
- `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\Contact Center\Common Components\CMF`
- `D:\Avaya\Contact Center\Manager Administration\Apps\` (including sub-directories)
- The folder where you store Service Packs and patches

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

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the email server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Avaya Contact Center Select 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.
- Ensure the antivirus software is configured to permit outbound email messages. For example, configure the McAfee antivirus software *Access Protection* option not to block *Prevent mass mailing worms from sending mail*. Alternatively, add the Contact Center Multimedia “EmailManager.exe” process to the McAfee *Processes to exclude* list.

Exclude the Contact Center Multimedia database partition from being scanned.

- If firewalls on individual computers are enabled on the Agent Desktop computer, the Report Listener might be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.
- You must not enable the Microsoft Updater to Auto-Run. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

Warning:

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

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

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

Exclude the Caché Journal file folder; `G:\Avaya\`

For Avaya Aura® Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

- `D:\Avaya\MAS\Multimedia_Applications\MAS\platdata`
- `D:\Avaya\MAS\Multimedia_Applications\MAS\common\log`

Avaya Aura® Media Server OVA

Avaya Aura® Media Server is a software based media processing platform. Deploy the Avaya Aura® Media Server OVA to provide the conference services required by Avaya Contact Center Select.

The Avaya Aura® Media Server OVA creates and configures a virtual machine containing Avaya Aura® Media Server software. The resulting virtual machine contains a Linux operating system, hard disk drive, third-party components, system configuration, firewall settings, and Avaya Aura® Media Server application software.

You can deploy the Avaya Aura® Media Server OVA on the same VMware host server as the Avaya Contact Center Select virtual machine and the Avaya WebLM OVA. Alternatively, you can deploy the Avaya Aura® Media Server OVA standalone on a separate VMware host server.

The Avaya Aura® Media Server OVA contains information about the virtual machine specification, operating system, and application software. This OVA contains the following components:

- Red Hat Enterprise Linux 6.x - 64bit

- Avaya Aura® Media Server Release 7.8 software
- IP tables firewall file application
- VMware Tools. Do not update the VMware Tools software on this virtual machine unless instructed to do so by Avaya.

The Avaya Aura® Media Server OVA package has the following default hardware configuration:

vCPU	Minimum CPU speed	Virtual memory required	Number of NICs	Virtual disk storage required	
4	2400 MHz	4.5 GB (4608 MB)	1 VMXNET3	Size	50 GB
				Deploy the Avaya Aura® Media Server OVA using Thick Provision Lazy Zeroed. Avaya Aura® Media Server does not support thin provisioning.	

Note:

Avaya Contact Center Select does not support Avaya Aura® Media Server using these default deployment settings. After you deploy the Avaya Aura® Media Server OVA, re-configure the virtual machine to have 4 or 8 CPUs and at least 8 GB RAM.

In a virtualized Avaya Contact Center Select environment, you can use VMware to load the Avaya Aura® Media Server OVA package into a virtual machine in your contact center solution. The virtualized Avaya Contact Center Select server can then use the virtualized Avaya Aura® Media Server as a voice media processor.

Deploy the Avaya Aura® Media Server OVA using Disk Format - Thick Provision Lazy Zeroed. Avaya Aura® Media Server does not support thin provisioning.

Avaya WebLM OVA

Deploy the Avaya WebLM Release 7.1 OVA to provide solution licensing. You can deploy the Avaya WebLM OVA on the same VMware host server as the Avaya Contact Center Select virtual machine and the Avaya Aura® Media Server OVA. Alternatively, you can also deploy the Avaya WebLM OVA standalone on a separate VMware host server.

Each Avaya Contact Center Select supports one WebLM license manager server. Each WebLM license manager server supports one Avaya Contact Center Select. For increased efficiency and flexibility, the WebLM licensing manager supports the VMware Virtual Appliance and Open Virtualization Archive (OVA) deployment mechanisms. In a virtualized Avaya Contact Center Select environment, you can use VMware to load the WebLM OVA package onto a separate virtual machine in your contact center solution. The virtualized Avaya Contact Center Select server can then use the virtualized WebLM server as the license manager.

The WebLM OVA contains a hardened Linux operating system.

The Avaya WebLM OVA requires the following:

vCPU	Minimum CPU speed	Virtual memory reservation	Number of NICs	Virtual disk storage reservation
1	—	2 GB	1 shared	35 GB

Note:

Do not change any of these Avaya WebLM OVA VMware virtual machine settings.

The WebLM OVA uses the following network mapping:

WebLM Server VM Interface	Application
Eth0	License management

The WebLM server for VMware is packaged as a vAppliance ready for deployment using either VMware vSphere Client or VMware vCenter.

Deploy the WebLM OVA using Disk Format - Thick Provision Lazy Zeroed. WebLM does not support thin provisioning in production environments.

VMware host server specification and profiling

This section specifies the VMware resources required to support the Avaya Contact Center Select software appliance for a number of solution sizes. The Avaya Contact Center Select (ACCS) software appliance consists of the following components:

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

The Avaya Contact Center Select, Avaya Aura® Media Server, and Avaya WebLM virtual machines are supported on a single VMware host or on separate VMware hosts.

VMware host server minimum CPU specification

Configure each VMware virtual machine with the CPU resources to support an ACCS software appliance component. For each virtual machine and required agent count, configure a specified number of vCPU cores and CPU Reservations in MHz. Each vCPU core must have a corresponding underlying physical CPU core on the VMware host. The performance of each physical CPU core, and corresponding vCPU core, is determined by the VMware server processor and hardware.

ACCS VMware profiling uses a Dual 8-core Intel Xeon E5-2670 2.60GHz CPU as a reference CPU. This reference processor has 16 physical CPU cores. Each of these 16 cores has an individual benchmark value that is one sixteenth of the overall benchmark score of the reference processor. You use this individual core benchmark value to compare the cores from different processors and to select suitable VMware host hardware for ACCS virtualization.

The individual core benchmark value for the processor in your VMware host server must be equal to or greater than 90% of the individual core benchmark value for the ACCS reference processor.

Follow these steps to ensure your proposed VMware host CPUs meet the ACCS minimum requirements.

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the reference CPU: Dual 8-core Intel Xeon E5-2670 2.60GHz.

  Reference individual core benchmark value = (Reference CPU benchmark from website / Number of cores in reference CPU)
- Using the https://cpubenchmark.net website, determine the individual core benchmark value for your VMware host server CPU.

  Individual core benchmark value = (Your host server CPU benchmark from website / Number of cores in host server CPU)
- To support ACCS virtualization, the individual core benchmark value of your VMware host must be equal to or greater than 90% of the reference individual core benchmark value.

To support an Avaya Contact Center Select software appliance component, your VMware host must have a sufficient number of CPU cores each with at least the minimum individual core benchmark value.

VMware host server minimum resources

Use the following tables to determine the minimum VMware resources required to support a range of agent counts and system contact rates.

Table 3: Avaya Contact Center Select virtual machine VMware resource requirements

Maximum number of supported Agents	**250**	**400**
Maximum System Contact Rate (system contacts per hour)	**5000**	**8000**
Email Contact Rate (Emails per hour)	750	750
WebChat Contact Rate (WebChats per hour)	375	375
Number of CPUs (Minimum CPU clock speed 2400 MHz)	4	6
CPU Reservation (MHz)	9560	14340
Minimum RAM (GB)	16	16
Minimum RAM Reservation (MB)	16384	16384
Minimum Disk Size (GB) - Thick Lazy Provisioning	641	641
Virtual Network Interface Cards (1 GB) VMXNET3	1	1

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

Note 2: Multimedia contact rates are applicable only if multimedia is part of the solution. Email contacts per hour (Eph). Standard Web chats per hour (WCph). Standard Web chat maximum capacity is based off an average chat duration of 5 minutes. The maximum number of simultaneous Web Chat sessions is 50.

Table 4: Avaya Aura® Media Server virtual machine VMware resource requirements

Maximum number of supported agents	**200**	**400**
Maximum supported sessions	**500**	**1000**
Number of CPUs (Minimum CPU clock speed 2400 MHz)	4	8
CPU Reservation (MHz)	9560	19120
Minimum RAM (GB)	8	8
Minimum RAM Reservation (MB)	8192	8192
Minimum Disk Size (GB) - Thick Lazy Provisioning	50	50
Virtual Network Interface Cards (1 GB) VMXNET3	1	1

Avaya Aura® Media Server is supported only on virtual machines with 4 or 8 CPUs.

Table 5: Avaya WebLM virtual machine VMware resource requirements

Maximum supported license requests	**5000**
Number of CPUs (Minimum CPU clock speed 2300 MHz)	1
CPU Reservation (MHz)	2290
Minimum RAM (GB)	2
Minimum RAM Reservation (MB)	2048
Minimum Disk Size (GB)	35
Virtual Network Interface Cards (1 GB) VMXNET3	1

VMware host server resource monitoring and management

When the Avaya Contact Center Select software appliance is virtualized and commissioned, continue to monitor and manage its real-time VMware resources.

- The VMware host server must not be overcommitted. The total number of vCPUs assigned across all virtual machines must be less than the host's physical core count.
- Virtual CPU (vCPU) resource requirements refer to physical cores only and not logical cores associated with Hyper-Threading.
- Ensure VMware Tools is installed on all virtual machines. This is required for VMXNET3 support and VMware performance monitoring and management.
- 16 GB of RAM is the minimum RAM footprint for reduced agent count deployments. Depending on your solution requirements, your ACCS virtual machine might need 20 GB RAM.
- If the total average CPU usage spikes above 50% for sustained periods, add additional CPU resources to the Contact Center virtual machine.
- If ACCS software appliance virtual machine monitoring indicates resource starvation, add additional resources as necessary.
- Depending on your solution's call complexity, you might need to add additional VMware resources as necessary.

- Depending on your solution's administration and reporting requirements, you might need to add additional VMware resources as necessary. Avaya recommends running large or complex reports during off-peak hours.
- The minimum CPU Reservation (MHz) figure is based on the minimum supported clock speed. To fully reserve each CPU, reserve the number of CPUs multiplied by the virtualization host's core clock speed.
- The supported agent counts and associated contact processing is modelled using simple contact processing with moderate reporting and administration.

Job Aid

The Avaya Contact Center Select High-end PVI server specification (see High-end server specification on page 68), configured as a VMware host, can support the Avaya Contact Center Select software appliance up to the maximum agent count and system contact rate.

VMware profiling examples

This section provides a few worked examples of profiling ACCS solutions for virtualization using VMware.

Example 1

An ACCS solution is to support 230 agents at a call rate of 4600 voice contacts per hour.

Using the tables in the **VMware host server minimum resources** section, calculate the minimum number of CPUs. The following table specifies the minimum number of VMware CPUs for this example solution.

Virtual Machine	CPUs
ACCS virtual machine	4
AAMS virtual machine	8
WebLM virtual machine	1
ACCS software appliance total:	**13**
ESXi Hypervisor	1
ESXi host minimum:	**14**

The minimum number of CPU cores needed is 14 in total. This means that the VMware host must have at least a Dual 8-core (16 physical cores) CPU. Each of these CPU cores must have an individual core benchmark value equal to or greater than 90% of the individual core benchmark value for the ACCS reference processor.

The next step is to determine if a proposed server CPU is suitable.

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the ACCS reference processor: Dual 8-core Intel Xeon E5-2670 2.60GHz.

  Reference individual core benchmark value = (Reference processor benchmark from website / Number of cores in reference CPU)

  For example:

Using the reference Dual 8-core Intel Xeon E5-2670 2.60GHz CPU

The reference Dual 8-core CPU has a benchmark score of, for example, 18653.

Reference individual core benchmark value = (18653 / 16)

Reference individual core benchmark value = 1165

90% of Reference individual core benchmark value = 1050

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the proposed VMware host server processor.

  Individual core benchmark value = (The host server processor benchmark from website / Number of cores in host server processor)

  For example:

  Using a proposed Dual 8-core Intel Xeon E5-2640 v3 2.60GHz.

  The Dual 8-core CPU has a benchmark score of, for example, 20885.

  Individual core benchmark value = (20885 / 16)

  Individual core benchmark value = 1305

  1305 > 1050, so the proposed Dual 8-core Intel Xeon E5-2640 v3 2.60GHz is suitable.

The following table lists the total minimum resources required for this example solution.

Virtual Machine	CPUs	Minimum RAM	Minimum Disk Size
ACCS virtual machine	4	16 GB	641 GB
AAMS virtual machine	8	8 GB	50 GB
WebLM virtual machine	1	2 GB	35 GB
Minimum ACCS Software Appliance resources:	13	26 GB	726 GB

Example 2

An ACCS solution is to support 50 agents at a call rate of 1000 voice contacts per hour.

Using the tables in the **VMware host server minimum resources** section, calculate the minimum number of CPUs. The following table specifies the minimum number of VMware CPUs for this example solution.

Virtual Machine	CPUs
ACCS virtual machine	4
AAMS virtual machine	4
WebLM virtual machine	1
ACCS software appliance total:	**9**
ESXi Hypervisor	1
ESXi host minimum:	**10**

The minimum number of CPU cores needed is 10 in total. This means that the VMware host must have at least a Dual 6-core (12 physical cores) CPU.

Each of these CPU cores must have an individual core benchmark value equal to or greater than 90% of the individual core benchmark value for the ACCS reference processor.

The next step is to determine if a proposed server CPU is suitable.

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the ACCS reference processor: Dual 8-core Intel Xeon E5-2670 2.60GHz.

  Reference individual core benchmark value = (Reference processor benchmark from website / Number of cores in reference CPU)

  For example:

  Using the reference Dual 8-core Intel Xeon E5-2670 2.60GHz CPU

  The reference Dual 8-core CPU has a benchmark score of, for example, 18653.

  Reference individual core benchmark value = (18653 / 16)

  Reference individual core benchmark value = 1165

  90% of Reference individual core benchmark value = 1050

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the proposed VMware host server processor.

  Individual core benchmark value = (The host server processor benchmark from website / Number of cores in host server processor)

  For example:

  Using a proposed Dual 6-core Intel Xeon X5690 3.47GHz

  The Dual 6-core CPU has a benchmark score of, for example, 9239.

  Individual core benchmark value = (14363 / 12)

  Individual core benchmark value = 1197

  1197> 1050, so the proposed Dual 6-core CPU is suitable.

The following table lists the total minimum resources required for this example solution.

Virtual Machine	CPUs	Minimum RAM	Minimum Disk Size
ACCS virtual machine	4	16 GB	641 GB
AAMS virtual machine	4	8 GB	50 GB
WebLM virtual machine	1	2 GB	35 GB
Minimum ACCS Software Appliance resources:	9	26 GB	726 GB

Virtualization considerations

Using virtualization in a contact center enterprise solution requires careful up-front planning, engineering, and implementation. While the technical and business advantages are clear, virtualization imposes extra considerations when designing the contact center solution

architecture. Environmental isolation allows multiple operating systems to run on the same VMware host machine. While virtualization offers these forms of isolation, virtualization environments do not provide performance isolation. The behavior of one virtual machine can adversely affect the performance of another virtual machine on the same host. Most modern virtualization environments provide mechanisms that you can use to detect and reduce performance interference. You must carefully engineer your virtualized contact center solution to avoid performance interference.

If you plan to install non-Contact Center software applications on the other guests of a host server with Contact Center installed, you must carefully analyze the impact of these applications on the contact center solution and provide extra performance isolation to safeguard Contact Center functionality.

Important:

Deploy Contact Center on an enterprise-grade virtual environment with the most recent hardware that supports hardware-assisted virtualization. Avaya recommends that you apply virtualization planning, engineering, and deployment with full organizational support for virtualization rather than organically growing a virtualization infrastructure.

VMware features

Avaya Contact Center Select is a collection of real-time applications running on the MS Windows Server 2012 R2 operating system. Avaya Contact Center Select provides real-time call control, multimedia handling, and statistical reporting.

Avaya Aura® Media Server is a real-time media processing application running on the Red Hat Enterprise Linux (RHEL) operating system. Avaya Aura® Media Server provides the real-time conferencing and media processing capabilities for Avaya Contact Center Select.

Some VMware features require CPU, Disk I/O, or networking resources to function. Running these VMware features can cause resource constraints and impact the real-time performance of the Avaya Contact Center Select and Avaya Aura® Media Server Virtual Machines (VMs). These features are therefore not supported while Avaya Contact Center Select or Avaya Aura® Media Server are active.

Some VMware features are not supported by Avaya Contact Center Select or Avaya Aura® Media Server. Some other VMware features are supported only while the Avaya Contact Center Select or Avaya Aura® Media Server Virtual Machines are stopped for maintenance.

The following table shows the Avaya Contact Center Select and Avaya Aura® Media Server level of support for VMware features.

VMware Feature	Supported on active Avaya Contact Center Select VM	Supported during Avaya Contact Center Select VM maintenance window	Supported on active Avaya Aura® Media Server VM	Supported during Avaya Aura® Media Server VM maintenance window
Cloning	No	Yes	No	No
Distributed Power Management (DPM)	No	Yes	No	Yes
Distributed Resources Scheduler (DRS)	No	Yes	No	Yes
Distributed Switch	Yes	Yes	Yes	Yes
Fault Tolerance	No	No	No	No
High Availability (HA)	No	No	No	No
Snapshots	No	See Avaya Contact Center Select VMware snapshot considerations on page 104	No	See Avaya Aura Media Server VMware snapshot considerations on page 105
Storage DRS	No	Yes	No	Yes
Storage Thin Provisioning	No	N/A	No	N/A
Storage vMotion	No	Yes	No	Yes
Suspend & Resume	No	N/A	No	N/A
vMotion	No	Yes	No	No

VMware vSphere Host considerations

When planning virtual machines (guests) on your host system, the total resources needed by the virtual machines running on the host server must not exceed the total capacity of the host. It is good practice to under-commit CPU and memory resources on the host. If the host CPU capacity is overloaded, Contact Center does not function correctly.

Important:

Avaya Contact Center Select is not supported on an over-committed host where the total virtual resources from all virtual machines hosted exceeds the physical resources of the host.

Hardware-Assisted Virtualization

Most recent enterprise-level processors from Intel support virtualization. There are two generations of virtualization support: the first generation introduced CPU virtualization; the second generation included CPU virtualization and added memory management unit (MMU) virtualization. For the best performance, make sure your system uses processors with at least second-generation hardware-assist features.

Virtual Machine File System (VMFS)

VMware virtual machines and snapshots are stored in a Virtual Machine File System (VMFS) datastore. To support Avaya Contact Center Select on a virtual machine, the VMware datastore containing Contact Center must be VMFS 5.54 or later. If you upgrade an existing VMware host server, ensure the associated datastore is upgraded to VMFS 5.54 or later.

Hardware-Assisted CPU Virtualization (Intel VT-x)

The first generation of hardware virtualization assistance includes VT-x from Intel. These technologies automatically trap sensitive interrupts, eliminating the overhead required to do so in software. This allows the use of a hardware virtualization (HV) virtual machine monitor (VMM).

Hardware-Assisted MMU Virtualization (Intel EPT)

More recent enterprise-level processors also include a feature that addresses the overheads due to memory management unit (MMU) virtualization by providing hardware support to virtualize the MMU. VMware vSphere supports this feature in Intel processors, where it is called Extended Page Tables (EPT).

Storage Area Network (SAN)

A Storage Area Network (SAN) is a dedicated storage network that provides access to consolidated block level storage. SANs are used to make storage devices such as disk arrays, accessible to servers so that the devices appear as locally attached to the operating system.

When Avaya Contact Center Select is installed on virtual machines it supports a SAN. You must monitor the Contact Center demand on the SAN storage device. Adhere to your vendor-specific SAN configuration recommendations to ensure the SAN storage device meets the demands of Contact Center.

Disk drive provisioning

Provision sufficient hard disk drive space on the host server to support all the guest virtual machines, an ISO library, and provision additional space for snapshot image storage.

Server performance and firmware settings

The Basic Input Output System (BIOS) of a server configures the hardware components and boots the operating system from a storage device. The server operating system (OS) then uses the BIOS to control the server hardware. You must configure the server BIOS settings to ensure optimum performance from the underlying server hardware. For most BIOS settings, you must choose between optimizing a server for power savings or for server performance. For real-time applications such as Avaya Contact Center Select, you must always choose the server BIOS settings that ensure the optimum performance from the underlying server hardware.

Server manufacturers provide their own motherboards, BIOS, hardware, and firmware. Determining the BIOS configuration for your server’s hardware can be challenging. There are several BIOS settings that can significantly impact the system performance. When optimizing for system performance, you must select the BIOS settings that enhance the system performance over those that contribute to power savings. Other BIOS settings and recommendations are not as

straight forward. Start by consulting the manufacturer's technical data for your server. Avaya recommends that you then test your solution in order to make the best BIOS configuration decisions.

Configure the server hardware, firmware, and Operating System settings to select system performance over power savings.

Server firmware

Firmware is a computer program that is stored on the server motherboard or on an add-on hardware controller. The firmware stored on the server motherboard is called the Basic Input Output System (BIOS). The BIOS is responsible for the behavior of the system when it is first switched on and for passing control of the server to the operating system. Firmware is also stored in hardware components such as Redundant Array of Independent Disks (RAID) controllers.

Routinely consult the manufacturer's technical data for your servers and, where appropriate, apply the most recent BIOS and firmware updates. The steps required to update firmware or a system BIOS vary depending on the hardware vendor and the component to be updated. Typically, the manufacturer supplies a firmware updating utility. Keeping your server BIOS and firmware at a supported level can improve reliability, serviceability, and help ensure optimum performance.

Power and performance management

For real-time applications such as Avaya Contact Center Select, you must always select the hardware, BIOS, firmware, and Operating System settings that enhance the system performance over those that contribute to power savings.

Intel Xeon CPUs offer two main power management options: C-states and Intel Turbo Boost.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to full power on.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power.

These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described below. Other server makes and models can have other terminology but equivalent BIOS settings.

The following are the recommended BIOS settings for the Dell PowerEdge servers:

- Set the Power Management Mode to Maximum Performance.
- Set the CPU Power and Performance Management Mode to Maximum Performance.
- Processor Settings: set Turbo Mode to enabled
- Processor Settings: set C States to disabled

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to Static High Mode.
- Disable Processor C-State Support
- Disable Processor C1E Support

- Disable QPI Power Management
- Enable Intel Turbo Boost

Configure the server hardware, firmware, and Operating System settings to select system performance over power savings.

Disk caching and RAID

Hard disk drives use cache memory to improve read and write access to the disk drives. In write-back mode caching, the disk or RAID controller writes data from the server to cache memory and acknowledges write completion to the server. The server is free to perform other tasks while the disk controller transfers the data from the write cache to the disk drives. This approach significantly increases write performance.

Avaya Contact Center Select supports hardware RAID-1, RAID-5, and RAID-10. RAID technology provides disk data redundancy as well as error detection and correction. For maximum security and mission-critical solutions, Avaya recommends that all Contact Center servers contain a RAID controller. Hardware RAID-1, RAID-5, and RAID-10 are the only levels and types of RAID supported.

Read the hardware documentation for your server to determine how to configure disk caching. Typically, disk caching can be configured as a BIOS setting, a RAID setting, a RAID controller setting, or as an Operating System setting. Some RAID controllers expose the ability to manipulate the Caching Policy through the OS and therefore the OS level setting can override the BIOS level setting. Refer to your hardware documentation for more information about configuring disk caching. Avaya Contact Center Select does not support Operating System level disk caching, software disk caching, or software RAID. Avaya Contact Center Select requires battery backed hardware RAID caching to avoid data loss and possible database corruption on power outage.

Non-Uniform Memory Architecture and memory

Non-uniform memory access (NUMA) is a computer memory design used in multiprocessing, where the memory access time depends on the memory location relative to the processor. Using NUMA, a processor can access its own local memory faster than non-local memory (memory local to another processor or memory shared between processors). For Avaya Contact Center Select, the server must support and implement NUMA.

In the server BIOS settings, configure the memory operating mode for performance optimization and disable Node Interleaving. For example, for a Dell server configure “Memory Operating Mode” as “Optimizer Mode”, and configure “Node Interleaving” as “Disabled”. Refer to your hardware documentation for more information about NUMA and memory performance.

Performance management and VMware

For VMware host servers, to allow the VMware kernel to control CPU power saving while maximizing server performance when required, it is possible to set power management in the BIOS to “OS Control Mode”. The VMware hypervisor can then provide balanced performance and power management. This BIOS setting and VMware feature combination does not meet the real-time performance requirements of Avaya Contact Center Select. Avaya Contact Center Select does not support the BIOS “OS Control Mode” settings or its equivalents.

Virtualization technology

When virtualization technology is enabled, the BIOS enables processor virtualization features and provides virtualization support to the operating system through the DMAR table. In general, only virtualized environments such as VMware take advantage of these features.

For VMware host servers, enable all available Virtualization Technology options in the hardware BIOS. For Intel based hosts: Enable Intel virtualization (VT-x) and if available enable Extended Page Tables (EPT). The available virtualization settings vary by hardware provider and BIOS version. Read your hardware provider's documents covering virtualization support to determine which settings to configure.

Hyper-Threading

Hyper-Threading is Intel’s proprietary technology for increasing parallel computational power (processor multi-tasking) by allowing the operating system (OS) to see and address each physical processor core as if it were two virtual processors. It also enables the OS and applications to share work between those virtual processors whenever possible, thereby making full use of the available resources.

Enable Hyper-Threading on the Avaya Contact Center Select server.

Unused hardware devices

On the server, disconnect or disable unused and unnecessary physical hardware devices such as: COM ports, LPT ports, USB controllers, Network interfaces, and Storage controllers. You must retain some USB devices for the mouse and keyboard. Disabling unnecessary hardware devices improves server performance and security. Consult the manufacturer’s technical data for your servers for information about disabling unused hardware devices in the BIOS.

Summary

For real-time applications such as Avaya Contact Center Select, choose server BIOS settings that optimize for performance in preference to power savings. Start by consulting the manufacturer’s technical data for your server. Avaya recommends that you then test your solution in order to make the best BIOS configuration decisions. Avaya recommends that you enable CPU Hyper-Threading. By enabling BIOS options such as CPU Prefetchers and CPU Hyper-Threading, the system performance can be improved effectively. When tuning system BIOS settings for performance, you must consider the various processor and memory options. Experiment with other options to find the optimum setting for your specific hardware and Contact Center solution.

Configure the server hardware, BIOS, firmware, and Operating System settings to select system performance over power savings.

VMware networking best practices

There are many different ways of configuring networking in a VMware environment. Review the VMware networking best practices documentation before deploying Avaya applications on an

ESXi host. This section is not a substitute for the VMware documentation. For improved performance and best practice, Contact Center uses Network Adapter type VMXNET 3.

The following are some suggested networking best practices:

- Separate network services to achieve greater security and performance. Create a vSphere *Standard Switch* with dedicated NICs for each service. Separate VMware Management, iSCSI (SAN traffic), and VM networks to separate physical NICs. If separate switches are not possible, consider port groups with different VLAN IDs.
- All physical NICs that are connected to the same vSphere *Standard Switch* must be connected to the same physical network.
- Configure all VMkernal vNICs to the same MTU (IP Maximum Transmission Unit).
- Configure Contact Center to use Network Adapter type VMXNET 3.

For more information about VMware networking best practices, refer to the VMware documentation.

Avaya Contact Center Select VMware snapshot considerations

VMware snapshots save the current state of the virtual machine, so you can return to it at any time. Snapshots are useful when you need to revert a virtual machine repeatedly to the same state, but you don't want to create multiple virtual machines.

The following considerations apply when using snapshots with Avaya Contact Center Select on VMware:

- Snapshots must be taken during an Avaya Contact Center Select maintenance window. Do not take a snapshot of a Contact Center virtual machine while Contact Center is running. Snapshots have a negative impact on the performance of a virtual machine over time. You must Delete All snapshots at the end of the maintenance window and *Consolidate* snapshots if required, before putting the Contact Center virtual machine back into production. For more information about consolidating snapshots, refer to VMware documentation. Before taking the snapshot, shutdown all Contact Center services and stop the Caché database instance using the Caché Cube.
- Create a snapshot for the Contact Center virtual machines all at the same time. Likewise, when you restore a snapshot, restore all snapshots to ensure the data is consistent across the Contact Center suite.
- When restoring snapshots, carefully consider the possible impact from out-of-date antivirus definitions, missed Microsoft Windows OS and security updates, and lapsed domain accounts on the contact center. Isolate the restored virtual machine until these issues are resolved.
- By default, a Windows Server 2012 R2 machine account password is changed every 30 days. This is an important consideration when reverting to a snapshot of a virtual machine that has been in use for more than 30 days, as it can cause the machine to lose its connection to the Windows domain. If this issue occurs, rejoin the Windows Server 2012 R2 virtual machine to the domain.

VMware snapshots are not a replacement for Avaya Contact Center Select database backup (and restore) procedures and practices. You must continue to perform regular and frequent Contact Center backups. For more information about maintenance, see *Deploying Avaya Contact Center Select Software Appliance*.

Avaya Aura® Media Server VMware snapshot considerations

VMware snapshots save the current state of the virtual machine, so you can return to it at any time. Snapshots are useful when you need to revert a virtual machine repeatedly to the same state, but you don't want to create multiple virtual machines.

The following considerations apply when using snapshots with Avaya Aura® Media Server on VMware:

- Snapshots must be taken during an Avaya Aura® Media Server maintenance window. Do not take a snapshot of an Avaya Aura® Media Server virtual machine while the contact center is running. Snapshots have a negative impact on the performance of a virtual machine over time. You must Delete All snapshots at the end of the maintenance window and *Consolidate* snapshots if required, before putting the Avaya Aura® Media Server virtual machine back into production. For more information about consolidating snapshots, refer to VMware documentation.
- When restoring snapshots, carefully consider the possible impact from out-of-date antivirus definitions, missed Linux operating system updates and security updates. Isolate the restored virtual machine until these issues are resolved.

VMware snapshots are not a replacement for Avaya Aura® Media Server database backup (and restore) procedures and practices. For more information about maintenance, see *Deploying Avaya Contact Center Select Software Appliance*.

Guidance for storage requirements

Input/Outputs per Second (IOPS) is a measure of the maximum number of reads and writes to *non-contiguous* storage locations performed per second. IOPS measurements are associated with smaller files and more continuous changes, and comprise the workloads most typical in real-time enterprise applications such as Avaya Contact Center Select.

In a virtualized environment, any given storage array must be designed to have an IOPS capacity exceeding the sum of the IOPS required for all resident applications.

For a fully loaded Avaya Contact Center Select instance, the IOPS is:

- Average: 105
- Maximum: 1488

These IOPS figures include Avaya Contact Center Select and the underlying operating system loads.

Performance monitoring and management

You must continuously monitor and measure the performance of the Contact Center host server. You can use VMware vSphere vCenter to measure the critical host performance metrics in real-time. VMware vCenter aggregates and archives performance data so that data can be visualized and reported on.

Configure VMware vCenter statistics collection to collect 5 minute and 30 minute Interval Duration data for the host at Statistics Level 3. Retain the 5 minute Interval Duration data for 3 days and retain the 30 minute Interval Duration for 1 week.

Generate performance reports using vCenter Report Performance and archive these reports to provide a baseline performance reference. Generate and store 1-day and 1-week reports. Store the associated vCenter Report Summary with the performance reports. You must analyze performance reports after changes to the host to assess the impact of the change on the host.

Monitor, acknowledge, and resolve VMware vCenter alarms. In particular, you must immediately investigate and resolve host CPU usage and host memory usage alarms.

In addition, the command-line tools “esxtop” and “resxtop” are available to provide a fine-grained look at real-time metrics. There are a number of critical CPU-related counters to watch out for:

- If the load average listed on the first line of the CPU Panel is equal to or greater than the number of physical processors in the system, this indicates that the system is overloaded.
- The usage percentage of physical CPUs on the PCPU line can indicate an overloaded condition. In general, 80 percent usage is a reasonable ceiling in production environments. Use 90 percent as an alert to the VMware administrator that the CPUs are approaching an overloaded condition, which must be addressed.
- %RDY - The percentage of time a schedulable entity was ready to run but is not scheduled to a core. If %RDY is greater than 10 percent, then this can indicate resource contention.
- %CSTP - The percentage of time a schedulable entity is stopped from running to allow other vCPUs in the virtual machine to catch up. If %CSTP is greater than 5 percent, this usually means the virtual machine workload is not using VCPUs in a balanced fashion. High %CSTP can be an indicator of a system running on an unconsolidated snapshot.

For more information about using esxtop or resextop, see the *VMware Resource Management Guide*.

Memory Reservations

Use VMware Reservations to specify the minimum amount of memory for a Contact Center virtual machine. VMware Reservations maintain sufficient host memory to fulfill all reservation guarantees. ESX does not power-on a virtual machine if doing so reduces the amount of available memory to less than the amount reserved. Using reservations can reduce the total number of virtual machines that can be hosted on a VMware host server. After all resource reservations have been met, ESX allocates the remaining resources based on the number of shares and the resource limits configured for your virtual machine.

Troubleshooting VMware

Virtualization platform performance issues can result with Contact Center performance problems. The virtualization platform includes the host and the running virtual machines on the host. The Contact Center performance problems can include (but are not limited to) high CPU usage, link instability, defaulted or abandoned calls.

You must logically and systematically investigate any Contact Center performance issues to rule out virtualization performance problems. All deviations from the published specifications must be investigated and resolved before the Contact Center software investigation is initiated. For more information, refer to the VMware vSphere documentation.

To support troubleshooting VMware resourcing issues, collect information about the following VMware Key Performance Indicators (KPIs).

VMware vSphere Host KPIs:

- Physical CPU
  - PCPU - Physical CPU usage.
  - CPU load average - Average CPU load average of host.
- Physical Memory
  - SWAP/MB - Memory swap usage statistics.

VMware vSphere Virtual Machine (VM) KPIs:

- vCPU
  - CPU RDY - Time VM was ready to run, but was not provided CPU resource.
  - CPU WAIT - Percentage of time spent in the blocked or busy wait state.
  - AMIN - Reservation allocated.
  - ASHRS - CPU shares allocated.
  - CPU CSTP - Amount of time a Symmetric Multi-Processing (SMP) VM was ready to run, but was delayed due to co-vCPU scheduling contention.
- Disk I/O
  - GAVG - Average guest operating system read latency per read operation.
  - DAVG/rd - Average device read latency per read operation.
  - DAVG/wr - Average device write latency per write operation.
  - RESETS/s - Number of commands reset per second.
  - ABRTS/s - Number of disk commands abandoned per second.
- Network
  - %DRPTX - Percentage of packets dropped when transmitting.

- %DRPRX - Percentage of packets dropped when receiving.

- Memory
  - MCTLSZ - Amount of physical memory reclaimed memory balloon statistics.

Software Appliance Licensing

Contact Center License Manager supports only the Virtualized Environment deployment of Avaya WebLM server.

When Contact Center License Manager starts, it extracts WebLM license keys from the remote WebLM server. Contact Center License Manager then converts the WebLM license keys into local PLIC license keys and distributes the keys to the Avaya Contact Center Select applications as required. Contact Center License Manager distributes PLIC license keys to Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, Contact Center Multimedia, and Avaya Aura® Media Server as required.

When Contact Center License Manager requests licenses from a remote Avaya WebLM server, it reserves all the Contact Center licenses available on that server. Contact Center therefore supports only the PLDS standard license file (SLF) type. Avaya Contact Center Select does not support the WebLM Enterprise model. Contact Center supports WebLM in nodal contact centers. WebLM does not support Contact Center corporate licensing.

Contact Center License Manager distributes nodal license keys to all configured Avaya Aura® Media Servers in the solution. Configure Avaya Aura® Media Server as a Media Server in Contact Center Manager Administration. Contact Center License Manager, when restarted, pushes license keys to that Avaya Aura® Media Server. Do not configure WebLM licensing on Avaya Aura® Media Server servers.

How to obtain a license

Avaya Contact Center Select uses a remote WebLM server to provide nodal licensing control.

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

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

Chapter 6: Avaya Contact Center Select hardware appliance

This section describes the Avaya Contact Center Select hardware appliance. The Avaya Contact Center Select hardware appliance is a physical rack mount server with the application software already loaded and partially preconfigured.

To deploy the Avaya Contact Center Select hardware appliance, you must activate the Windows operating system using the provided MS Windows product key, configure the server network setting, and then use a simple configuration wizard to rapidly commission the solution. At install time, the Avaya Contact Center Select hardware appliance server automatically launches a simple configuration wizard that you use to rapidly deploy a functional contact center solution. The Avaya Contact Center Select hardware appliance server is preloaded with sample users, skillsets, and contact center parameters. You can use this sample data to rapidly commission the solution and make the first routed call and email contact. The Avaya Contact Center Select hardware appliance server delivers quick and simplified contact center deployment. After the basic telephony and email features are working, you can then configure multimedia contacts, multiplicity, custom prompts, and other enhanced features and functions to improve your customer's experience.

You must activate the Microsoft Windows operating system on the Avaya Contact Center Select hardware appliance using the provided Microsoft Windows product key. The provided Microsoft Windows product key is displayed on a sticker attached to the top of the Avaya Contact Center Select hardware appliance server.

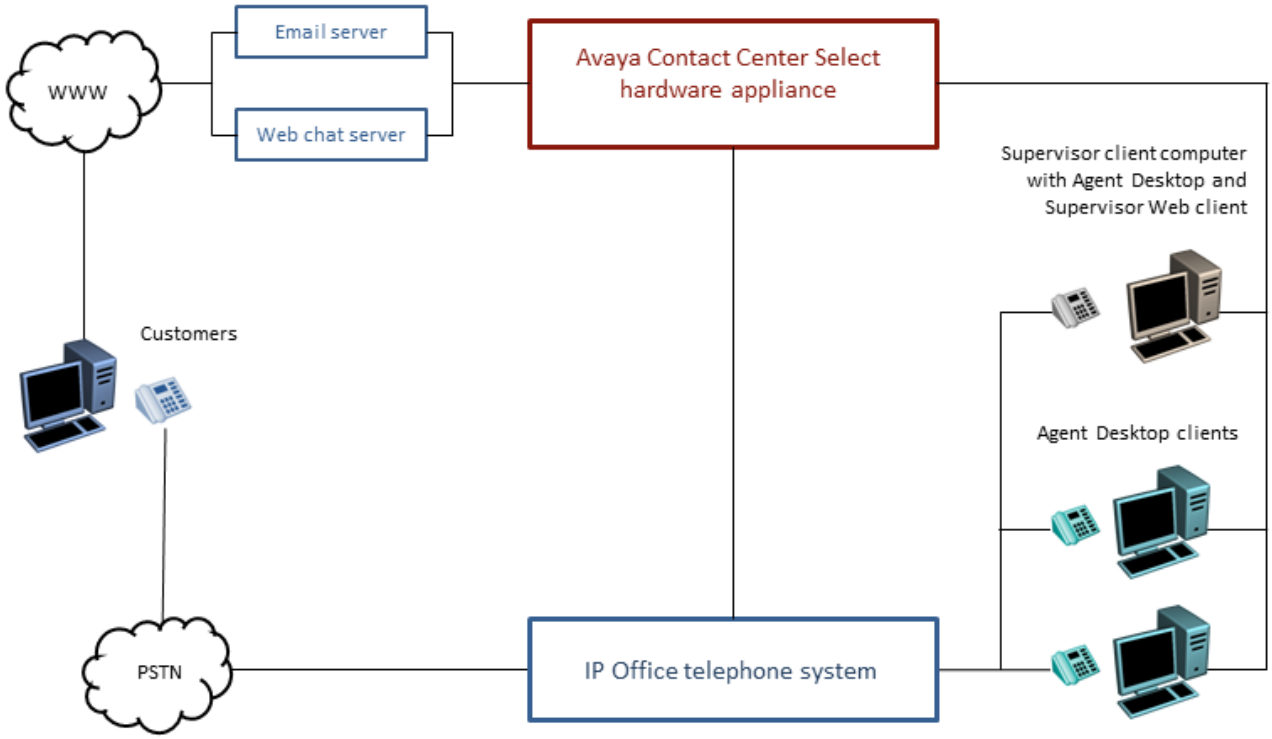


Figure 10: Topology of a typical Avaya Contact Center Select hardware appliance solution

- Hardware Appliance server specifications on page 110
- Avaya Contact Center Select hardware appliance software specifications on page 112
- Hardware Appliance Licensing on page 118

Hardware Appliance server specification

The Contact Center Hardware Appliance is a rack mount server preconfigured to support Contact Center.

Contact Center is a collection of real-time applications running on the Microsoft Windows Server 2012 R2 operating system. Contact Center provides real-time call control, multimedia handling, and real-time statistical reporting.

Important:

The Contact Center Hardware Appliance server supplied by Avaya is optimized to provide the real-time computational, networking, and logging resources required by Contact Center. You must not modify the Hardware Appliance server, unless instructed to do so by Avaya:

- Do not add additional internal hardware devices to this server.

- Do not change or upgrade the server BIOS version or settings.
- Do not change the server hardware settings.
- Do not update the server firmware.
- Do not change or upgrade the device drivers.
- Do not modify the hard disk partitions.
- Do not change the *Windows Update* application settings on the server.
- Do not upgrade the Java Runtime Environment (JRE) supplied on the Hardware Appliance.

Due to the real-time processing that Contact Center applications perform, you must not install any other application class software on the server. You can install only the supported antivirus and remote support utility class software on this server.

Install only the Microsoft Windows Server 2012 R2 Operating System patches and hotfixes supported by Contact Center. For more information about the supported Operating System patches, see the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Compatibility List* on http://support.avaya.com.

The following table lists the server specifications for the Contact Center Hardware Appliance server.

Specification	Quantity	Configuration	Comment
Form factor	1	Rack mount, 1U chassis	PowerEdge R630 rack mount server.
CPU	2	2.6 GHz E5-2640v3	—
RAM	12	4GB DDR4 RDIMM	—
Hard Disk	2	1.2 TB 10K Drives 2.5" SAS	—
RAID Controller	1	RAID1 PERC 730 1GB	—
Optical Drive	1	16X DVD +/-RW Drive SATA	—
Network Interface	2	Dual Port PCIe NIC 1GbE	Only Ethernet supported.
Power supply	2	750 Watt AC	—
Power cables	2	Power cables	Localized to region.
Additional interfaces		• 2 front USB ports • 2 back USB ports • Front video connector	—
Additional hardware	1	Rack mount kit	—
Weight	—	47.5 lbs approximately 21.5 kilograms approximately	—

Avaya Contact Center Select hardware appliance software specifications

Avaya Contact Center Select is offered as a hardware appliance server. The Avaya Contact Center Select hardware appliance server contains the following software:

- Microsoft Windows 2012 R2 Standard Edition operating system. The operating system is not activated until the end customer applies the Microsoft Windows license attached to the server.
- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)
- Contact Center Multimedia (CCMM)
- Avaya Aura® Media Server with Quick Fix Engineering (QFE) patches
- Default Avaya Contact Center Select configuration data
- Service Packs
- Firewall policy
- Configuration wizard

The Windows 2012 R2 operating system on the shipped hardware appliance server is not activated. The Contact Center hardware appliance provides a Microsoft Windows Server 2012 R2 product license key. The Microsoft Windows Server 2012 R2 product license key is printed on a label attached to the top of the Contact Center Hardware Appliance server. You must activate the Microsoft Windows operating system within 30 days of the initial power-up. Otherwise the Avaya Contact Center Select hardware appliance server stops working.

The following table shows the operating system on the Avaya Contact Center Select hardware appliance server.

Operating System	International Versions Supported	Minimum Service Pack Supported
Windows Server 2012 Release 2 Standard Edition	English	

Server naming requirements

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

- Use only characters a to z, A to Z, and 0 to 9 can be used in a host name.
- You can use a hyphen (-), but not to start or end the host name.
- Host names must be 6 to 15 characters in length.
- Host names must not start with a number.
- Do not use the underscore character (_) and period character (.).
- Do not use spaces in the host name.

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

If network connectivity on your network requires the use of Fully Qualified Domain Names (FQDN), then the FQDN of each computer must be resolvable between all servers associated with Contact Center.

Microsoft security hotfixes

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

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

Operating system updates

Operating system updates includes service updates and service packs.

Service updates

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

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

Whenever possible, Avaya incorporates the most recent operating system security recommendations and service updates in an integrated solutions testing strategy during each test cycle. However, due to the urgent nature of security service updates when vulnerabilities are discovered follow Microsoft guidelines as they are issued, including any Microsoft installation procedures and security service update rollback processes.

Finally, you must perform a full system backup before you update the system to ensure that a rollback is possible, if required. If a Contact Center application does not function properly after you apply a Microsoft security service update, you must remove the service update and revert to the previous version of the application (from the backup you made before applying the service update). For added security, always determine whether Avaya verified the Microsoft service update for compatibility with Contact Center Manager.

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

Service packs

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

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

Important:

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

Java Runtime Environment updates

Contact Center supports only specific versions of Java Runtime Environment (JRE). During installation, Contact Center disables JRE automatic updates on the contact center servers.

Important:

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

Dynamic Host Configuration Protocol support

Contact Center applications (CCMS, CCMA, CCT, CCMM, LM, and Avaya Aura® Media Server) do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Agent Desktop client computers support both DHCP and static IP addresses.

Third-party software requirements

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

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

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

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

Generic guidelines for utility-class software applications

The following are generic guidelines for utility-class software:

- During run-time, the utility must not degrade the contact center application beyond an average percentage of CPU use (see each specific application section in this document for the recommended maximum CPU usage level). Furthermore, the utility must not lower the minimum amount of free hard disk space required by contact center application and the Windows Operating system.
- The utility must not cause improper software shutdowns or out-of-sequence shutdowns.
- The utility must not administer the contact center application.
- If the utility has a database, it must not affect the contact center application database.
- Disk compression utilities must not be used.
- Memory tweaking utilities used to reclaim memory that is unused by Microsoft must not be used.
- The installation or uninstallation of the third-party software must not impact or conflict with the contact center application (for example, it must not cause DLL conflicts). If such conflicts are discovered, a server rebuild might be necessary.
- The implementation personnel must perform tests to ensure these conditions and recommendations are met before you place the Contact Center application into production.

Support personnel can ask for the results of the testing during fault diagnosis. As part of fault diagnosis, the distributor or end user might be asked to remove third-party software.

- HyperTerminal must not be installed on the server as it interferes with the operation of Contact Center.

Guidelines for the use of antivirus software

This section describes the Avaya Contact Center Select antivirus software requirements.

Avaya Contact Center Select supports the following antivirus products:

- Symantec Antivirus
- McAfee

For more information about Avaya Contact Center Select anti-virus considerations and supported versions, see *Avaya Contact Center Select Security Reference Guide* available from the Avaya Support website at http://support.avaya.com.

You can deploy antivirus products from other vendors subject to the following guidelines:

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

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

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

- `F:\Avaya\Contact Center\Databases\`
- `<additional database drive>:\Avaya\Contact Center\Databases\`
- TSM_OAM files located in the following folders:
  - 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
- `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\Contact Center\Common Components\CMF`
- `D:\Avaya\Contact Center\Manager Administration\Apps\` (including sub-directories)
- The folder where you store Service Packs and patches

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

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the email server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Avaya Contact Center Select 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.
- Ensure the antivirus software is configured to permit outbound email messages. For example, configure the McAfee antivirus software *Access Protection* option not to block *Prevent mass mailing worms from sending mail*. Alternatively, add the Contact Center Multimedia “EmailManager.exe” process to the McAfee *Processes to exclude* list.

  Exclude the Contact Center Multimedia database partition from being scanned.
- If firewalls on individual computers are enabled on the Agent Desktop computer, the Report Listener might be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.

- You must not enable the Microsoft Updater to Auto-Run. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

Warning:

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

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

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

Exclude the Caché Journal file folder; `G:\Avaya\`

For Avaya Aura® Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

- `D:\Avaya\MAS\Multimedia_Applications\MAS\platdata`
- `D:\Avaya\MAS\Multimedia_Applications\MAS\common\log`

Hardware Appliance Licensing

The Avaya Contact Center Select Hardware Appliance deployment option uses a Nodal Enterprise license delivered as a WebLM XML file. This license file is used to control access to licensed features such as multimedia contacts and multiplicity.

Contact Center License Manager provides central control and administration of licensing for Avaya Contact Center Select. Each Contact Center License Manager includes a local instance of WebLM. When the Contact Center License Manager service starts, it extracts WebLM license keys from the local WebLM instance. Contact Center License Manager then converts the WebLM license keys into local PLIC license keys and distributes the keys the Avaya Contact Center Select applications as required.

- Obtain the WebLM Host ID for your Avaya Contact Center Select server.
- Use the WebLM Host ID to obtain a nodal WebLM license file from the Avaya Product Licensing and Delivery System (PLDS).
- You load the license file onto the Avaya Contact Center Select server as you run the configuration utility when you are deploying the Avaya Contact Center Select server. You can also load the license file after the configuration process. When Contact Center License Manager loads the license, if the unique number in the license does not match theWebLM Host ID, then License Manager shuts down and Avaya Contact Center Select cannot process contacts. If the unique number in the license matches the WebLM Host ID, then License

Manager provides license keys, and Avaya Contact Center Select processes customer contacts.

Chapter 7: Solution capacity limits and supported features

This section specifies the maximum capacity limits of Avaya Contact Center Select. This section also specifies the telephony features and devices supported by Avaya Contact Center Select.

Avaya Contact Center Select maximum capacity limits

The maximum capacity for your solution is determined by your Avaya Contact Center Select deployment and the IP Office voice and call recording platform and Release.

You can install the Avaya Contact Center Select DVD on any server that meets the Platform Vendor Independence (PVI) server specifications. The Avaya Contact Center Select DVD supports three levels of PVI server specification; Entry-level, Mid-range, and a High-end PVI server specification. The maximum capacity figures for the Avaya Contact Center Select DVD depend on which PVI server specification is used. The High-end specification supports Avaya Contact Center Select to its maximum rated capacity.

The Avaya Contact Center Select software appliance is a set of virtualized servers; an Avaya Contact Center Select virtual machine, an Avaya Aura® Media Server OVA, and a WebLM OVA. You can deploy the Avaya Contact Center Select software appliance on a VMware ESXi host server that provides the required resources.

The Avaya Contact Center Select hardware appliance is a physical rack mount server with the application software already loaded and partially preconfigured. The supplied rack mount server supports Avaya Contact Center Select to its maximum rated capacity.

The following table specifies the maximum capacity values supported by the Avaya Contact Center Select deployment types for each supported IP Office configuration.

Server type	Maximum Capacity	IP Office (IPO) configuration					
		IPO SE 10.1 or 11.0 R630, R620, DL360	**IPO SE - DL120**	**IPO 500V2 SIP trunks no CR**	**IPO 500V2 SIP trunks with CR**	**IPO 500V2 TDM trunks no CR**	**IPO 500V2 TDM trunks with CR**
Entry-Level Server	Maximum logged-in agents See Note 3	60	60	60	30	40	30
	Maximum CCMA supervisors	10	10	10	10	10	10
	Maximum System Contact Rate See Note 1	1200	1200	1200	600	800	600
	Maximum multimedia rate (WCph / Eph) See Note 2	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300
Mid-Range Server	Maximum logged-in agents See Note 3	150	125	60	30	40	30
	Maximum CCMA supervisors	30	30	30	30	30	30
	Maximum System Contact Rate See Note 1	3000	2500	1200	600	800	600
	Maximum multimedia rate (WCph / Eph) See Note 2	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600
High-End Server and Software Appliance	Maximum logged-in agents See Note 3	400 See Note 4	125	60	30	40	30
	Maximum CCMA supervisors	80	50	50	30	40	30
	Maximum System Contact Rate See Note 1	8000	2500	1200	600	800	600
	Maximum multimedia rate (WCph / Eph) See Note 2	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200
Hardware Appliance	Maximum logged-in agents See Note 3	400	125	60	30	40	30

Table continues…

Server type	Maximum Capacity	IP Office (IPO) configuration					
		IPO SE 10.1 or 11.0 **R630, R620, DL360**	**IPO SE - DL120**	**IPO 500V2 SIP trunks no CR**	**IPO 500V2 SIP trunks with CR**	**IPO 500V2 TDM trunks no CR**	**IPO 500V2 TDM trunks with CR**
	Maximum CCMA supervisors	80	50	50	30	40	30
	Maximum System Contact Rate See Note 1	8000	2500	1200	600	800	600
	Maximum multimedia rate (WCph / Eph) See Note 2	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200

- **Note 1:** The System Contact Rate is the total maximum combined contact rate across all supported contact types.
  - For System Contact Rate calculations, Web chat contacts have a weighting equivalent to 2 email messages. One Web chat is equivalent to two email messages.
  - For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + Email + (Web chat * 2))
  - *Route to CDN* and *Transfer/Conference to CDN* each count as two calls.
  - Complex call flows with transfer and conference scenarios de-rate the supported number of concurrent contacts.
- **Note 2:** Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Web chats per hour (WCph). Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes.
- **Note 3**: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on a high-end server Avaya Contact Center Select supports 350 Agent Desktops and 50 Agent Browser applications.
- **Note 4**: The incoming lines on IP Office (IP Office Line or IP Office SIP Line) that target inbound calls at Avaya Contact Center Select must have Direct Media enabled to support more than 250 simultaneously logged-in agents.

  With 400 Agents concurrently active on simple calls (no conference or transfer calls), the maximum number of calls in queue is 200. This figure is based on the maximum number of available sessions on Avaya Aura® Media Server.
- IP Office Call Recording (CR) is supported with IP Office 500V2. Avaya Contact Center Select supports Call Recording up to the maximum number of supported logged-in agents. Above this maximum limit, no one can leave a voicemail or record any other calls.

Server type	ACCS specification	IP Office platform						
		IPO SE R620/R630	IPO SE DL360	IPO SE DL120	IPO 500V2 SIP Trunks No CR	IPO 500V2 SIP Trunks With CR	IPO 500V2 TDM Trunks No CR	IPO 500V2 TDM Trunks With CR
Entry-level Server	Logged-in agents	60	60	60	60	30	40	30
	CCMA Supervisors	10	10	10	10	10	10	10
	System Contact Rate	1200	1200	1200	1200	600	800	600
	MM Rate (WCph/Eph)	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300
Mid-range Server	Logged-in agents	150	150	125	60	30	40	30
	CCMA Supervisors	30	30	30	30	30	30	30
	System Contact Rate	3000	3000	2500	1200	600	800	600
	MM Rate (WCph/Eph)	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600
High-end Server	Logged-in agents	400	400	125	60	30	40	30
	CCMA Supervisors	80	80	50	50	30	40	30
	System Contact Rate	8000	8000	2500	1200	600	800	600
	MM Rate (WCph/Eph)	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200
Hardware Appliance	Logged-in agents	400	400	125	60	30	40	30
	CCMA Supervisors	80	80	50	50	30	40	30
	System Contact Rate	8000	8000	2500	1200	600	800	600
	MM Rate (WCph/Eph)	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200

Figure 11: The maximum capacity values supported by the ACCS deployment types for each supported IP Office (IPO) configuration

Avaya Contact Center Select maximum configuration limits

The following table specifies the maximum overall configuration values supported by Avaya Contact Center Select.

Parameter	Maximum value
Maximum configured agents	1500
Maximum agents skillsets	3000
Maximum skillsets per agent	20
Maximum agents per skillset	400
Maximum supervisors per skillset	80
Maximum supervisors per system	600

Avaya Contact Center Select supported features

The following table specifies the main features supported by Avaya Contact Center Select:

Feature	Supported	Provider
Voice Skills Based Routing	Yes	Avaya Contact Center Select
FIFO Queuing	Yes	Avaya Contact Center Select
Longest Idle Agent queuing	Yes	Avaya Contact Center Select
ANI Number Available	Yes	Avaya Contact Center Select
ANI Number Routing	Yes	Avaya Contact Center Select
DNIS Number Available	Yes	
DDI Number Routing	Yes	Avaya Contact Center Select
Night Service	Yes	Avaya Contact Center Select
Threshold overflow for skills	Yes	Avaya Contact Center Select
Visual External Alarm for exceeded threshold	Yes	Avaya Contact Center Select
Voice Contact Classification	Yes	Avaya Contact Center Select and Agent Desktop
Multi-parameter Screen Pop per contact type per skillset	Yes	Avaya Contact Center Select
Music On Hold	Yes	IP Office
Multi Source Music on Hold	No	
On–Hold Announcements	No	
Skill Announcements	Yes	Avaya Contact Center Select
Agent Ext In/DN Key	Yes	Avaya Contact Center Select and IP Office with three line appearance
Coverage to Voicemail Pro	Yes	Direct calls to an agent station receive the configured coverage treatment. Calls routed from Avaya Contact Center Select to Agents do not receive coverage treatment.
Play Prompt and Collect Digits	Yes	Avaya Contact Center Select
Wallboards with API	Yes	Dev Connect and Avaya Contact Center Select
Activity /Work Codes	Yes	Avaya Contact Center Select
Aux/Not Ready Reason Codes	Yes	Avaya Contact Center Select
After Call Work Codes	Yes	Avaya Contact Center Select
Real Time Display Indication ACW/Act/AUX/NotRdy Codes	Yes	Avaya Contact Center Select
Three Line Operation (3 call appearance lines)	Yes	Avaya Contact Center Select and IP Office

Table continues…

Feature	Supported	Provider
Browser Based Agent Desktop	Yes	Avaya Contact Center Select and Agent Desktop Agent Desktop client is deployed using either the click-once deployment or an MSI file.
Browser Based Supervisor Desktop	Yes	Avaya Contact Center Select and Agent Desktop Supervisor Administration client use Internet Explorer based CCMA. Supervisor Agent client is deployed using either the click-once deployment or an MSI file.
Toll Free Queuing	Yes	Avaya Contact Center Select
Telephone Only Mode operation	No	
TLS transport type	Yes	Between IP Office and Avaya Contact Center Select
Report Creation Wizard	Yes	Avaya Contact Center Select
Media Server Zoning	No	
Contact Center Network Based Routing	No	
Mission Critical High Availability	No	Avaya Contact Center Select Business Continuity is supported.
Remote/Off-Site agent support	Yes	IP Office
IPv6 networking	No	
Database customization – import new Customer defined fields	No	

The following table specifies the multimedia features supported by Avaya Contact Center Select:

Feature	Sub feature	Supported	Provider
Multimedia Skills Based Routing		Yes	
Multimedia Management & Reporting		Yes	Avaya Contact Center Select
Multiplicity		Yes	Avaya Contact Center Select
Email Contact Handling		Yes	Avaya Contact Center Select

Table continues…

Feature	Sub feature	Supported	Provider
	Email Auto Response	Yes	Avaya Contact Center Select
	Email Auto Acknowledge	Yes	Avaya Contact Center Select
	Customer Contact History	Yes	Avaya Contact Center Select
	Email Real Time Reporting	Yes	Avaya Contact Center Select
	Screen Pop based on Email	Yes	Avaya Contact Center Select
	Fax Contact Types	Yes	Avaya Contact Center Select
	Scanned Documents	Yes	Avaya Contact Center Select
	SMS Contact Inbound	Yes	Avaya Contact Center Select
Web Communications		Yes	Avaya Contact Center Select
	Web Chat	Yes	Avaya Contact Center Select
	Web Call-back	Yes	Avaya Contact Center Select
	Co-browsing	No	
Outbound	Preview/Progressive	Yes	Avaya Contact Center Select
Self Service Integration			
	Self Service Data and CTI to external IVR	No	
	On board Avaya Aura® Media Server IVR - play prompt and collect digits	Yes	
Workforce Optimization			
	Bulk Voice Recording	No	Avaya Contact Center Select
	Selective Recording	No	Using IP Office button
	Agent Initiated	No	Using IP Office button
	Quality Monitoring	No	
Workforce Management/ Forecasting		No	

Table continues…

Feature	Sub feature	Supported	Provider
External Threshold Alerter/Alarms		No	
Multi-Site Reporting		Yes	For distributed agents in an SCN network.
Supervisor /Agent Instant Messaging		No	
OPEN QUEUE Contact Types		Yes	
SOA Enabled		No	
IM (Routed) Contact Types		No	
Predictive Outbound		No	
Agent Desktop Softphone – H.323 or SIP		No	
Agent Greeting		No	

The following table specifies the reporting features supported by Avaya Contact Center Select:

Feature	Sub feature	Supported	Provider
Unified Multi Channel Real-time and Historical Reporting		Yes	Avaya Contact Center Select
Predefined Real-time and Historical Reports		Yes	Avaya Contact Center Select
Customer Customizable Reports		Yes	Avaya Contact Center Select
Customer Definable Reports		Yes	Using third-party tools interfacing using Avaya Contact Center Select ODBC
Report Creation Wizard (RCW)		Yes	Avaya Contact Center Select
Historical Reports			
	Scheduled	Yes	Avaya Contact Center Select
	Interval	Yes	Avaya Contact Center Select
	Daily	Yes	Avaya Contact Center Select

Table continues…

Feature	Sub feature	Supported	Provider
	Weekly	Yes	Avaya Contact Center Select
	Monthly	Yes	Avaya Contact Center Select
	Quarterly	No	
	Skillset	Yes	Avaya Contact Center Select
	Trunk	No	
	Agents	Yes	Avaya Contact Center Select
	Abandoned Contacts	Yes	Avaya Contact Center Select
	Overflow Contacts	Yes	Avaya Contact Center Select
	Threshold Exceeded	Yes	Avaya Contact Center Select
	Contact Classification	Yes	Avaya Contact Center Select
	Source Of Disconnect	Yes	Avaya Contact Center Select
	Agent Station Key	No	
	Email Report Notifications	Yes	Avaya Contact Center Select
	System Status Reports	Yes	Avaya Contact Center Select

The following table specifies Avaya Contact Center Select product interoperability:

Product name	Supported
Avaya Aura® Workforce Optimization (WFO)	No. Use IP Office call recording.
Avaya Workforce Optimization Select (AWFOS)	Yes, Release 5.2, 5.2.1, and 5.3.
Proactive Outreach Manager (POM)	No
Avaya Aura® Experience Portal	Yes, Release 7.1, 7.2, and 7.2.1.
Avaya IQ Reporting	No
Avaya Control Manager Agent and Supervisor Administration	No
Avaya Proactive Contact	No
Avaya one-X® Agent	No

Table continues…

Product name	Supported
Social Media Manager	Yes (using the email contact type). Release 6.2.13 or later.
Avaya Aura® Presence Services	No
Avaya Communicator for Windows	Yes, softphone support.
Microsoft Lync (Release 2010 and 2013) and Microsoft Skype for Business 2015	Peer-to-peer IMs are supported. Routed IMs are not supported.

The following table specifies the Open Interfaces supported by Avaya Contact Center Select:

Open Interface name	Supported
Real-time Statistics Multicast (RSM)	Yes
Real-Time Display (RTD)	Yes
Database Integration Wizard (DIW) and Host Data Exchange (HDX)	Yes
Contact Center Multimedia (CCMM) Advanced Email Services	Yes
Contact Center Manager Administration (CCMA) Open Interfaces	Only for IP Office user data synchronization with Avaya Contact Center Select
Contact Center Multimedia Open Interfaces	Only for standard Web Chat communications (not supported for Agent Desktop).
Contact Center Multimedia Outbound Open Interfaces	Yes
Communication Control Toolkit (CCT) Open Interfaces	No
Open Queue	Yes
Open Networking	No
Meridian Link Services (MLS)	No
Communication Control Toolkit .NET SDK	Yes
Contact Control Service SDK	Yes
Contact Center Manager Server (CCMS) Open Interfaces	No
Avaya Contact Recording APIs	No
Salesforce Server Side support	Yes

Supported Telephony Features

The following tables list the IP Office telephony features available to a non-agent IP Office user and specify which features are supported on an Avaya Contact Center Select agent station.

Basic Call Handling:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Tones	Yes	Yes	No	No	Agent Desktop does not play specific tones dependent on geography.
Caller ID	Yes	Yes	Yes	Yes	
Call Screening	Yes	No	No	No	
Hold	Yes	Yes	Yes	Yes	
Toggle Calls	Yes	Yes	No	No	Toggle calls is not applicable to Avaya Contact Center Select agents with 3-line appearance.
Hold Call Waiting	Yes	Yes	No	No	Same as Auto-hold-allowed.
Hold Music (Music on Hold)	Yes	Yes	Yes	Yes	Provided by IP Office.
Park	Yes	No	No	No	
Automatic Callback	Yes	No	No	No	
Direct Inward Dialing (DID/ DDI)	Yes	Yes	Yes	Yes	
Transfer	Yes	Yes	Yes	Yes	
Distinctive and Personalized Ringing	Yes	No	No	No	
Personalized Ringing	Yes	Yes	No	No	
Message Waiting Indication (MWI)	Yes	No	No	No	Supported on some physical stations. Not supported by Agent Desktop. Contact Center (CC) calls are prevented from going to voicemail so cannot result in MWI light on telephone. However, an agent handling a CC call sees the MWI light on their telephone if a personal

Table continues…

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
					call results in a new voicemail message while handling the CC call.
Visual Voice	Yes	No	No	No	Supported on some IP Office stations only and not by Agent Desktop. Contact Center (CC) calls are prevented from going to voicemail so cannot result in messages that can be processed using Visual Voice on telephone. However, an agent servicing a CC call can use Visual Voice on their telephone while servicing the CC call.

Advanced Call Handling:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Absence Text	Yes	Yes	No	No	
Call Tagging	Yes	Yes	No	No	The Call Tagging feature is equivalent to the Avaya Contact Center Select Call Attached Data feature.
Reclaim Call	Yes	No	No	No	
Hunt Group Enable/Disable	Yes	Yes	No	No	Ability of a user to enable and disable their membership of hunt groups.
Call Waiting	Yes	N/A	Yes	N/A	If an Avaya Contact Center Select agent is active on a call, then another CC call is not routed to that agent. If an Avaya Contact Center Select agent is active on

Table continues…

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
					personal call, a CC call is not routed to the agent.
Do Not Disturb (DND)	No	No	No	No	Avaya Contact Center Select agents use NotReady (with reason code).
Dial Plan	N/A	N/A	N/A	N/A	Refers to the dial plan configuration on the IP Office. Configure a dial plan to route calls to extensions and agents.
Paging	Yes	Yes	No	No	Telephone must have a loudspeaker.
Intrude	Yes	Yes	No	No	Avaya Contact Center Select Supervisors can use Observe or Barge-in features.
Inclusion	Yes	Yes	No	No	
Private Call	Yes	Yes	No	No	
Hot Desking	Yes	Yes	N/A	N/A	This feature allows a number of users' non-exclusive use of the same extension. Once logged in, any calls to that user are routed to the physical extension they are logged in at.
Remote Hot Desking	Yes	Yes	N/A	N/A	This feature is the same as 'Hot Desking' but refers specifically to a user configured on a particular node logging in to an extension configured on another node in the Small Community Network (SCN).
Relay On/Off/ Pulse	N/A	N/A	N/A	N/A	
Pickup	Yes	No	No	No	
Call Recording	Yes	Yes	No	No	
Telecommuter Mode	No	No	No	No	
Twinning and Mobility	No	No	No	No	

Key and Lamp Operation:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Appearance Buttons	N/A	N/A	N/A	N/A	
Line Appearance	N/A	N/A	N/A	N/A	Three lines maximum. A Line Appearance is a representation of a trunk line on the IP Office system where the indicator tracks the activity on the Line. Only external calls can be answered or made on Line Appearances.
Call Appearance Buttons	Yes	Yes	No*	No*	Individual calls are represented individually on Agent Desktop, but there is no concept of selecting a particular call appearance button which corresponds to the telephone.
Alerting/Ring Tone for Covered Calls	Yes	No	No	No	IP Office blocks Avaya Contact Center Select calls from covering.
Bridged Appearance Buttons	No	No	No	No	
External Call Lamp Indication	Yes	No	No	No	
Call Coverage	Yes	No	Yes	No	IP Office blocks Avaya Contact Center Select calls from covering.
Call Coverage Buttons	Yes	N/A	No	N/A	

Outbound Call Handling:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Account Codes	Yes	Yes	No	No	
Authorization Codes	Yes	Yes	No	No	
Dial Emergency	Yes	N/A	No	No	The Dial Emergency feature is equivalent to the ACCS Emergency Call feature.
Call Barring	N/A	N/A	N/A	N/A	Avaya Contact Center Select independent

Alternate Route Selection (ARS):

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Maximum Call Length	Yes	Yes	Yes	Yes	Avaya Contact Center Select independent
Transferable Dial Out Privilege	Yes	N/A	No	N/A	Avaya Contact Center Select independent
Idle Line Preference	Yes	N/A	No	N/A	Avaya Contact Center Select independent
Alternate Route Selection	N/A	N/A	N/A	N/A	Configure IP Office to select appropriate trunk to route calls on.

Forwarding:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Coverage to Operator	Yes	No	No	No	
Forward on Busy	Yes	No	No	No	

Table continues…

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Forward on No Answer	Yes	No	No	No	
Forward Unconditional	Yes	No	No	No	
Unconditional Forward to Voicemail	Yes	No	No	No	
Forward Hunt Group	Yes	No	No	No	
Follow Me	Yes	No	No	No	

Avaya telephone features:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Programmable Buttons	Yes	Yes	No	No	
Busy Lamp Field (BLF) Indicators	Yes	Yes	No	No	Avaya Contact Center Select independent
Call History	Yes	Yes	No	No	
Language	Yes	Yes	No	No	Agent Desktop language is determined by the OS settings on the Agent Desktop client computer, not from the language configured for the IP Office extension.
Centralized Personal Directory	Yes	Yes	No	No	
Centralized System Directory	Yes	Yes	No	No	
Self-Administration	No	No	No	No	Avaya Contact Center Select agents are not allowed to modify telephone properties.

Table continues…

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
On Hook Dialing	Yes	Yes	Yes	Yes	

Inbound Call Handling. Applies only in Failover Mode to IP Office Hunt Groups:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Incoming Call Routing	Yes	Yes	Yes	Yes	IP Office system configuration decides where incoming calls are routed. Once call routing is configured, calls to agents are displayed on the telephone and in Agent Desktop.
Hunt Groups	Yes	N/A	Yes	N/A	
Multi-site Networking/ Small Community Networking (SCN) Distributed Hunt	Yes	N/A	Yes	N/A	
Night Service	Yes	N/A	Yes	N/A	
Time Profiles	Yes	No	Yes	No	
Queuing	Yes	N/A	Yes	N/A	Configure system to limit the number of calls that can be waiting to be serviced in a hunt group. For example, when all parties in the group are busy.
Announcements	Yes	N/A	Yes	N/A	Configure system to play announcements to calls waiting to be services in a hunt group.

Contact Center features:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Acquire Call (Call Steal)	Yes	No	No	No	Acquire Call can behave like 'Reclaim Call' or 'Call Pickup' depending on how it is invoked and the state of the two users involved.
Monitor Calls	Yes	No	No	No	A user can monitor other party's calls by listening in.
Queue Threshold Alert	N/A	N/A	N/A	N/A	Queue Threshold Alert applies only in Failover Mode to IP Office Hunt Groups.
Login	N/A	N/A	N/A	N/A	Login applies only in Failover Mode to IP Office Hunt Groups.

System Short Codes:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
User Short Codes	Yes	Yes	No	No	
System Short Codes	Yes	Yes	No	No	
Post-Dialing Short Codes	Yes	Yes	No	No	
Incoming Number Short Codes	Yes	Yes	No	No	

Miscellaneous Features:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Conference Calls	Yes	Yes	Yes	Yes	

Table continues…

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Coaching/Silent Intrusion/ Whisper Page	Yes	Yes	No	No	
Dial On Pickup	No	No	No	No	This IP Office feature is also known as Hotline. The feature automatically dials a specified extension when the telephone is taken off hook. Do not configure this feature for Avaya Contact Center Select agents.
Off Hook Operation	N/A	N/A	N/A	N/A	Analog station feature not supported by Avaya Contact Center Select.
E911 Emergency Call	Yes	N/A	Yes	N/A	

Supported Telephony Devices

This section specifies the telephony connection types and devices supported in an Avaya Contact Center Select solution. The Avaya Contact Center Select solution supports all of the IP Office platform trunks types. There is no direct integration between the Avaya Contact Center Select and IP Office trunking interfaces. The Avaya Contact Center Select contact center functionality is independent of these IP Office trunks.

The following table lists the stations and telephone types supported by Avaya Contact Center Select.

Agent Phone	Phone Model	Avaya Contact Center Select Supported	Notes
Analogue – All Models		No	
Digital	9500 Series	Yes	
	1400 Series	Yes	
	5400 Series 2400 Series	Yes	The 5400 series is not supported with IP Office 10.x or later.

Table continues…

Agent Phone	Phone Model	Avaya Contact Center Select Supported	Notes
IP: H.323	96x1	Yes	
	96x0	Yes	
	J129 IP deskphone J139 IP deskphone J169 IP deskphone J179 IP deskphone	Yes	Supported only with IP Office 11.0 or later.
	1600 Series	Yes	
	5600 Series 4610/4620x	Yes	Not supported with IP Office 10.x or later.
IP: SIP	IP Phone 1140E Model NTYS05 IP Phone 1230 Model NTYS20 IP Phone 1120e IP Phone 1220 J129 IP deskphone J139 IP deskphone J169 IP deskphone J179 IP deskphone	Yes	Supported when running IP Office SIP firmware. The 1120e and 1220 IP phones are supported only with IP Office 10.x or later. The J-series IP deskphones are supported only with IP Office 11.0 or later.
DECT – All Models		No	
Wi-Fi Wireless – All Models		No	
Avaya Communicator for Windows		Yes	Softphone support with IP Office.
IP Office Softphone		Yes	Supported as co-resident softphone on agent workstation with Agent Desktop. Not supported as integrated softphone.

The following table shows the Avaya Contact Center Select agent experience for various phone types.

Phone Type	Skillset on Agent Desktop		Skillset on the phone		PSTN Number	Recording Indication
	Ringing	Connected	Ringing	Connected		
96x0 (9640)	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

Phone Type	Skillset on Agent Desktop		Skillset on the phone		PSTN Number	Recording Indication
	Ringing	Connected	Ringing	Connected		
96x1 (9641)	Yes	Yes	Yes	Yes	Yes	Yes
J129	Yes	Yes	Yes	Yes	Yes	Yes
J139	Yes	Yes	Yes	Yes	Yes	Yes
J169	Yes	Yes	Yes	Yes	Yes	Yes
J179	Yes	Yes	Yes	Yes	Yes	Yes
56xx (5610)	Yes	Yes	Yes	No	Yes	Yes
46xx (4610)	Yes	Yes	Yes	No	Yes	Yes
16xx (1616)	Yes	Yes	Yes	Yes	Yes	Yes
Softphone	Yes	Yes	Yes	Yes	Yes	No
95xx (9504)	Yes	Yes	Yes	Yes	Yes	No
54xx (5410)	Yes	Yes	Yes	No	Yes	Yes
24xx (2420)	Yes	Yes	Yes	No	Yes	Yes
14xx (1408)	Yes	Yes	Yes	Yes	Yes	Yes

Remote access support

Avaya Contact Center Select supports remote access using the following:

- Microsoft Windows Remote Desktop
- IP Office Support Services (IPOSS)

Both of these support remote troubleshooting and technical support.

Communication Control Toolkit supported functionality

This section compares the features supported by Avaya Contact Center Select using Avaya IP Office with the features supported by Avaya Aura® Contact Center using Avaya Aura® Communication Manager or Avaya Communication Server 1000 (CS 1000).

Communication Control Toolkit and Agent Desktop implement and use these features. Agent Desktop is a client of Communication Control Toolkit so they support the same features.

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

Table 6: Basic Communication Control Toolkit and Avaya Agent Desktop functions

Event	SIP-enabled Avaya Aura® Contact Center with Avaya Aura®	AML-based Avaya Aura® Contact Center using CS 1000	Avaya Contact Center Select using IP Office
Make Call	Yes	Yes	Yes
Hold Current Call	Yes	Yes The CS 1000 Swap Hold switch feature is not supported.	Yes
Unhold Call	Yes (Retrieve Call)	Yes (Retrieve Call)	Yes
Drop Current Call (Release)	Yes	Yes	Yes
Blind Transfer Call	No	Yes	No
Initiate Supervised Transfer	Yes	Yes	Yes
Complete Transfer	Yes	Yes	Yes
Initiate Conference Call	Yes	Yes (up to six parties)	Yes
Complete Conference Call	Yes	Yes	Yes
Call Forward	No	Yes	No
Cancel Call Forward	No	Yes	No
Join Conference	Yes, Avaya Aura® only	No	Yes
Deflect Calls	No	No	No
Get Status	Yes	Yes	Yes
Get Call Capabilities	Yes	Yes	Yes
Get Data	Yes	Yes	Yes
Delete Data	Yes	Yes	Yes
Append Data	Yes	Yes	Yes
Make Set Busy (Do Not Disturb)	No	Yes (on Agent Terminals only)	No
Get/Set UUI	Yes	No (UUI attached as call data)	Yes
Send DTMF (for example, credit card number to IVR)	Yes	Yes	Yes
Mute/Unmute	No	No	No
Consult	Yes	Yes (but must designate as transfer or conference)	Yes
Park/Unpark	No	No	No
Message Waiting Indicator	No	No	No

Table continues…

Event	SIP-enabled Avaya Aura® Contact Center with Avaya Aura®	AML-based Avaya Aura® Contact Center using CS 1000	Avaya Contact Center Select using IP Office
HER (Host Enhanced Routing)	No	Yes	No
Answer	Yes	Yes	Yes

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

The following table lists the Contact Center specific functions supported by Agent Desktop and Communication Control Toolkit.

Table 7: Contact Center-specific functions

Event	SIP-enabled Avaya Aura® Contact Center with Avaya Aura®	AML-based Avaya Aura® Contact Center using CS 1000	Avaya Contact Center Select using IP Office
Agent Login	Yes	Yes	Yes
Agent Logout	Yes	Yes	Yes
Set Ready	Yes	Yes	Yes
Set Not Ready	Yes	Yes	Yes
ACD Set Activity Code	Yes	Yes	Yes
ACD Set Not Ready/Reason Code	Yes	Yes	Yes
ACD Set After Call Work Item Code	Yes	Yes	Yes
Work Ready Key support	No	No	No
Agent Whisper	No	No	No
Observe call	Yes	No	Yes
Set Call treatment	No	Yes	No
Barge In	Yes	No	Yes
Call Supervisor	Yes	Yes	Yes
Emergency Key	Yes	Yes	Yes
Redirect to another skillset	No, must transfer to a CDN (Route Point)	No	No, must transfer to a CDN (Route Point)
Return a call to the queue skillset that it came from	No	No	No
Redirect to another skillset	No	No	No
Return a call to the queue skillset that it came from	No	No	No

The following table lists the events delivered by Communication Control Toolkit.

Table 8: Communication Control Toolkit events

Event	SIP-enabled Avaya Aura® Contact Center with Avaya Aura®	AML-based Avaya Aura® Contact Center using CS 1000	Avaya Contact Center Select using IP Office
Ringing Event	Yes	Yes	Yes
Dialtone Event	No	No	No
Busy Event	No	No	No
Offering Event	Yes	Yes	Yes
Ringback Event	Yes	Yes	Yes
Inbound Connected Event	Yes	Yes	Yes
Outbound Connected Event	Yes	Partial	Yes
Connected Event	Yes	Yes	Yes
Disconnected Event	Yes	Yes	Yes
Held Event	Yes	Yes	Yes
Unheld Event	Yes	Yes	Yes
OnHold Pending Conference Event	Yes	Yes	Yes
Onhold Pending Transfer Event	Yes	Yes	Yes
Transferred Event	Yes	Yes	Yes
Conference Event	Yes	Yes	Yes
Initiated Transfer Event	Yes	Yes	Yes
Initiated Conference Event	Yes	Yes	Yes
Session Disconnect Event (includes shutdown)	Yes	Yes	Yes
Device Forward Event	No	No	No
Status Change Event	Yes	Yes	Yes
Notice Message Waiting Event	No	No	No
Notice No Message Waiting Event	No	No	No
Agent Logged out Event	Yes	Yes	Yes
Agent Logged in Event	Yes	Yes	Yes
Agent Ready Event	Yes	Yes	Yes
Agent Not Ready Event	Yes	Yes	Yes
Agent Busy Event	No	No	No

Table continues…

Event	SIP-enabled Avaya Aura® Contact Center with Avaya Aura®	AML-based Avaya Aura® Contact Center using CS 1000	Avaya Contact Center Select using IP Office
Agent Work Ready Event	No	No	No
Activity Code Entered	Yes	Yes	Yes
WalkAway Activated	No	No	No
WalkAway Return	No	No	No
Emergency Invoked	No	No	No
Call Supervisor Invoked	No	No	No

Chapter 8: Avaya Aura® Experience Portal Integration

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

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

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

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

- Front-end Avaya Aura® Experience Portal
- Back-end Avaya Aura® Experience Portal using SIP header information
- Back-end Avaya Aura® Experience Portal using Context Creation

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

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

- SIP header information. SIP includes a number of message headers in each SIP message. These headers contain information that enables the receiver to understand and use the message properly. In a contact center solution, SIP headers can be used to transfer small amounts of call-related information between SIP-enabled applications. Avaya Contact Center Select supports the User-to-User Information (UUI) SIP header and the Avaya custom P-Intrinsics SIP private header.
- SIP INFO message body using Context Creation: If your call-related context information does not fit in a SIP User-to-User Information (UUI) header or in the larger P-Intrinsics header, you can use the sample Context Creation application to pass more context information from Avaya Aura® Experience Portal to Avaya Contact Center Select. This sample Context Creation application can return multiple values from Avaya Aura® Experience Portal, rather than the single value returned by the sample Play and Collect application. The Context Creation sample

application can return call-related context information in a SIP INFO message body. A SIP INFO message body holds and transfers much more information than a SIP header.

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

- SIP header information
- SIP INFO message using Context Creation

There are no additional licensing requirements for Avaya Contact Center Select and Avaya Aura® Experience Portal integration.

Data transfer methods

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

Transfer method	Maximum data supported by Contact Center
UUI SIP header using ASAI	96 bytes maximum.
P-Intrinsics SIP header	Depends on your solution. Note 1
SIP INFO message body using Context Creation	8K bytes total maximum: • Maximum of 10 ASCII key-value pairs. • And 1K characters of Call Attached Data (CAD) within the CC application.
Note 1 The following limitations apply to P-Intrinsics SIP header information: • The amount of P-Intrinsics information associated with a call depends on the other SIP headers in the call and on the call flow path. Typically, Contact Center supports up to 10 ASCII key-value pairs of P-Intrinsics.	

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

Avaya Aura® Experience Portal Orchestration Designer

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

Voice XML

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

Call Control XML

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

SIP-enabled Avaya Contact Center Select

Avaya Contact Center Select uses Session Initiation Protocol (SIP) architecture to provide maximum interoperability and flexibility. SIP-enabled Avaya Contact Center Select simplifies solution architecture and CTI deployments. Avaya Contact Center Select SIP-enabled architecture and Contact Intrinsic data make it easy to develop screen pop applications, reducing the time, effort, and cost required to launch new capabilities.

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

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

In a SIP-enabled contact center solution, the information stored in some SIP INFO messages can be used to transfer call-related information between SIP-enabled components. This call-related information enables the receiver to better understand and handle the call. If your call-related context information does not fit in a SIP User-to-User Information (UUI) header or in the larger P-

Intrinsics header, you can use the sample Context Creation application to pass more context information from Avaya Aura® Experience Portal to Avaya Contact Center Select. The Context Creation sample application can inject multiple pieces of context information (Intrinsics and Call Attached Data) into Avaya Contact Center Select, whereas the Play and Collect sample application can retrieve only a single piece of data, for example collected digits. The call-related context information is returned in a SIP INFO message body. A SIP INFO message body holds and transfers much more information than a SIP header.

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

P-Intrinsic SIP Header

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

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

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

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

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

Typical solution using P-Intrinsics

A front-end Avaya Aura® Experience Portal system uses XML speech applications and SIP header information to integrate with Avaya Contact Center Select. A self-service Voice XML speech application running on the Avaya Aura® Experience Portal – Application Server answers customer calls and gathers call-associated information based on customer’s answers and inputs.

Experience Portal then transfers the customer call, complete with this call-associated information stored in the P-Intrinsics SIP header, to Avaya Contact Center Select.

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

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

User-to-User Information

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

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

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

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

Universal Call Identifier

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

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

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

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

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

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

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

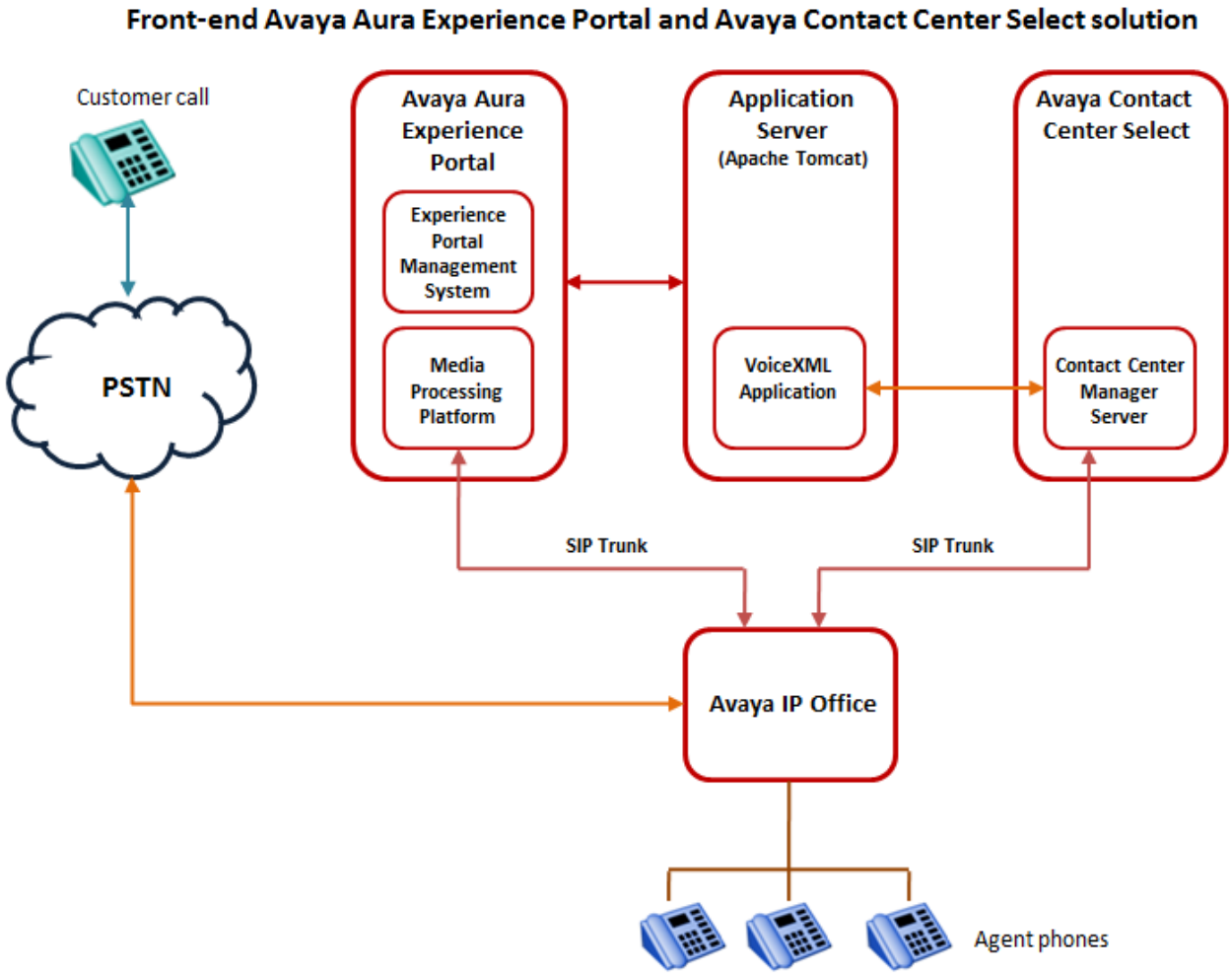


Figure 12: Example of front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

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

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

1. Incoming customer calls are routed to a Media Processing Platform (MPP) server in the Avaya Aura® Experience Portal system.
2. The MPP server checks the Dialed Number Identification Service (DNIS) for the incoming call and uses the configuration information downloaded from the Experience Portal Manager (EPM), server to match the number to a speech application on Avaya Aura® Experience Portal.

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

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

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

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

Avaya Aura® Experience Portal provides back-end Interactive Voice Response (IVR) services like text-to-speech, digit collection, music, and speech recognition. A combined Avaya Aura® Experience Portal system and Avaya Contact Center Select solution gives your customers exceptional service and improved efficiency. Back-end Interactive Voice Response (IVR) reduces contact center operating costs and improves Customer Satisfaction (CSAT).

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

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

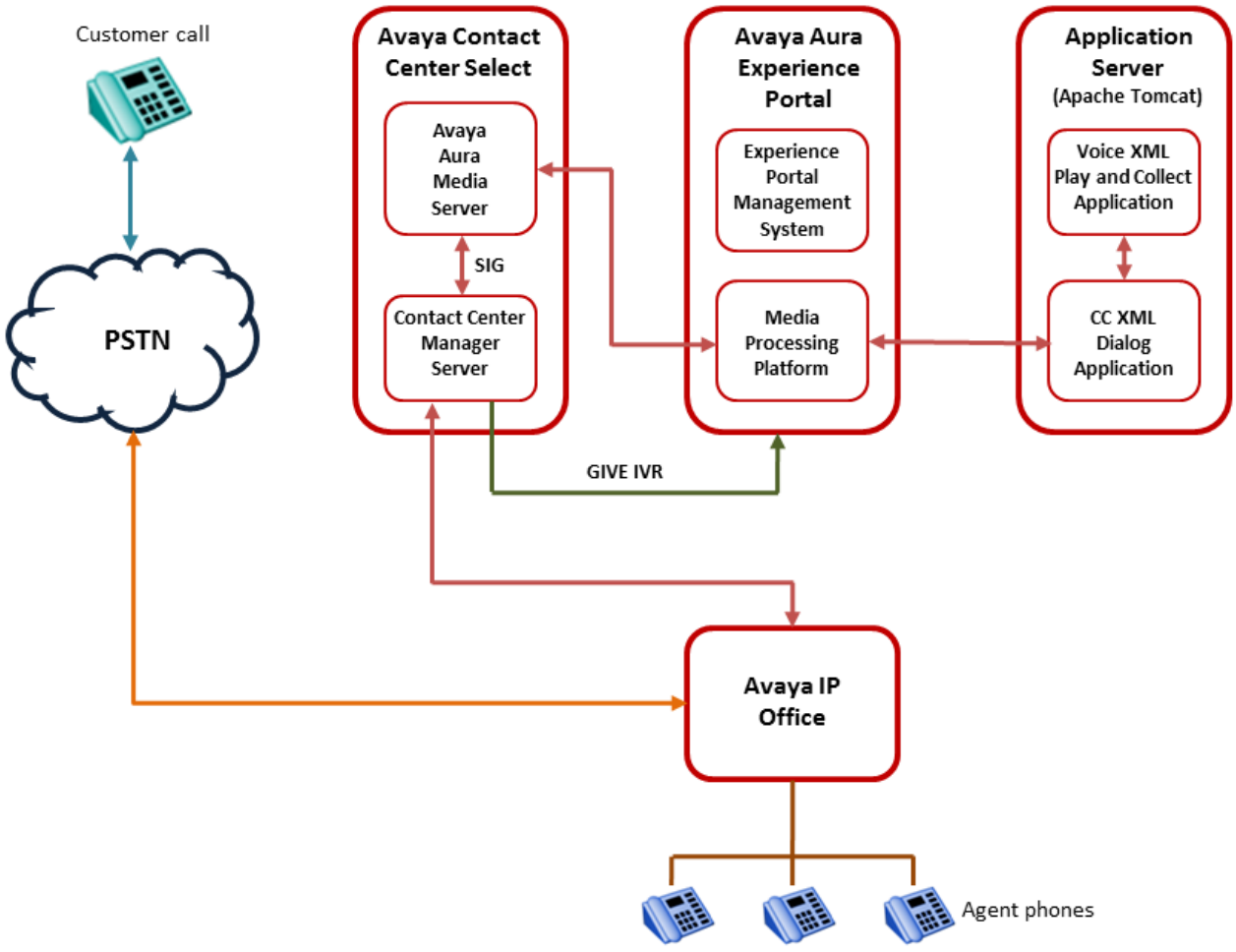


Figure 13: Example of back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

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

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

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

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

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

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

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

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

Experience Portal system and Avaya Contact Center Select solution gives your customers exceptional service and improved efficiency.

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

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

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

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

In a back-end integration where Avaya Aura® Experience Portal is using the Context Creation sample application, the Avaya Contact Center Select Orchestration Designer script sends a GIVR IVR (SIP INVITE) message into the Avaya Aura® Experience Portal system. The SIP INVITE message has “treatmenttype” set to “contextcreation”. Avaya Aura® Experience Portal passes the SIP call to a sample Dialog CC XML application. The Dialog CC XML and Context Creation VoiceXML applications process the call, and return hex-encoded call-related information. Because the “treatmenttype” was set to “contextcreation”, the Dialog application returns a SIP INFO message of type “application/x-aacc-info” to the Contact Center. The Contact Center SIP Gateway Manager (SGM) recognizes this SIP message type and converts the context information in the call into Contact Intrinsics. The Orchestration Designer script can then access and use the Contact Intrinsics for the call, and Contact Center can pass them on to Agent Desktop.

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

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

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

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

Example of the single intrinsic when Hex-encoded:

```
3c63633e3c693e435553544f4d45525f53455353494f4e5f49443d31323334353c2f693e3c2f63633e
```

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

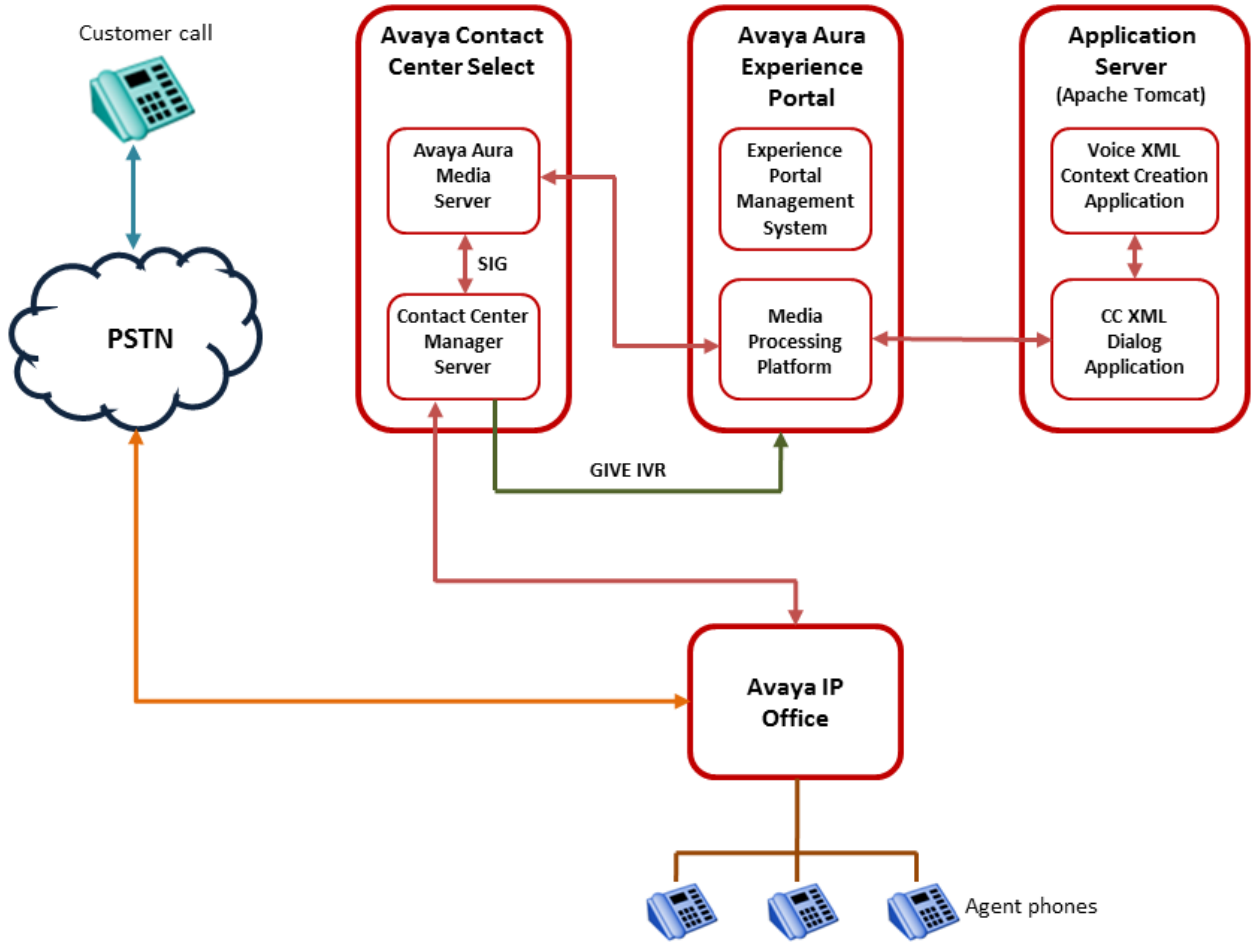


Figure 14: Example of back-end Avaya Aura® Experience Portal using the Context Creation sample application

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

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

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

   The sample Context Creation application uses the account number details from the configuration files for illustration purposes. In a real solution, you can extract the context data from anywhere; be it an external database, a Customer Relationship Management (CRM) system, or from context gathered within the Orchestration Designer application.
10. The Context Creation Voice XML application then passes the encoded hex data back to the CCXML dialog application.

11. The CCXML dialog application returns the encoded hex data to Avaya Contact Center Select in a SIP INFO message. Because “treatmenttype” was set to “contextcreation”, the dialog application sets the type of the SIP message body to ‘application/x-aacc-info’.
12. The CCXML dialog application then drops out (`BYE`).
13. The Avaya Contact Center Select SIP Gateway Manager (SGM) recognizes this SIP message type and creates context information for the call by converting the hex encoded data in the SIP INFO message body into Contact Intrinsics.
14. The Avaya Contact Center Select script logs the returned value.

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

Avaya DevConnect

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

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

For more information, and to download the complete Avaya Aura® Experience Portal front-end self-service and Avaya Contact Center Select using SIP header sample files, see Orchestration Designer Sample Applications on www.avaya.com/devconnect.

Chapter 9: Administration client computer requirements

This section provides the configuration requirements for the browser-based Avaya Contact Center Select administration client computers. Install this client computer to configure and administer Avaya Contact Center Select resources, to monitor performance, and to generate (real-time and historical) reports. You can also use this client computer to upload and download data using the Configuration Tool spreadsheets.

Administrator computer hardware requirements

The following table lists the minimum hardware requirements for the Administrator client computer.

Table 9: Client computer minimum hardware requirements

Hardware item	Minimum requirements	Additional information
CPU	1 Gigahertz (GHz) or faster CPU with support for PAE, NX, and SSE2	Physical Address Extension (PAE), NX processor bit (NX), and Streaming SIMD Extensions 2 (SSE2) are features of the processor. These CPU features are required to run Microsoft Windows 7.0 and Microsoft Windows 8.1. Dual- and quad-CPU systems are supported with or without Hyper-Threading enabled. AMD processors of the same or higher specification are also supported.
RAM	1 Gigabyte (GB) (32-bit) or 2 GB (64-bit)	Additional memory is required, if you run other memory intensive applications.
Hard disk space	16 GB (32-bit) or 20 GB (64-bit)	
Hard disk partitioning	No specific partitioning requirements	—
Hard disk speed	2.5 inch disk minimum speed: 10000 RPM	—

Table continues…

Hardware item	Minimum requirements	Additional information
	3.5 inch disk minimum speed: 7200 RPM	
Floppy drive	Not required	If a floppy drive is installed, it must be A.
DVD ROM	Not required	
Network interface	One network interface card	100 Mb/s Ethernet or higher is recommended.
Video card	Microsoft DirectX 9 graphics device with WDDM driver	1024 x 768 pixels minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—

Client operating system requirements

The following table lists the operating system requirements for client computers.

Table 10: Client operating system requirements

Operating system	International versions supported	Minimum service pack
Windows 7 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) Japanese (JA) Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	
Windows 8.1 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL)	

Table continues…

Operating system	International versions supported	Minimum service pack
	Japanese (JA) Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	
Windows 10 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) Japanese (JA) Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	

Administration Client Citrix support

Contact Center Manager Administration (CCMA) is supported in Citrix deployments. A Citrix server solution uses software to deliver on-demand Windows applications to physical desktops. This allows client users to access and use programs which are available on the Windows Server 2012 R2 operating system of the Citrix server. Contact Center Manager Administration supports the following versions of Citrix server:

- Citrix XenApp 6.5
- Citrix XenApp 7.x

Users access Contact Center Manager Administration through a Citrix client on their client computer, connecting through an Internet Explorer browser that runs on the Citrix server. The browser is available to users through a Citrix client on their client computer. In a client Citrix deployment of CCMA, you must install ActiveX controls on the Citrix server. For more information about installing ActiveX controls on the Citrix server, see *Avaya Contact Center Select Advanced Administration*.

For more information about Citrix application publishing, see your Citrix documentation. For more information on how to configure your Citrix server to allow users to access CCMA, see *Avaya Contact Center Select Advanced Administration*.

Avaya Contact Center Select supports only the Multicast option for Real-Time Displays (RTDs) in a Citrix environment. Avaya Contact Center Select does not support the Unicast option for Real-Time Displays (RTDs) in a Citrix environment.

Important:

No Avaya Contact Center Select client components, other than Agent Desktop and Contact Center Manager Administration, are supported in a Citrix deployment. The Orchestration Designer (OD), Outbound Campaign Management Tool (OCMT), and CCMM Administration utility client components are supported in a Citrix deployment.

Third-party software requirements

This section describes the third-party software requirements for the administration client computer.

The following components are required on the administration client PC:

- Microsoft Internet Explorer 10.0 (32-bit version only), and 11.0 (32-bit version only).

  Note:

  You must run Internet Explorer in compatibility mode for Contact Center Manager Administration and Communication Control Toolkit.

- Microsoft Excel 2007 or later (for Configuration Tool only)

Contact Center Manager Administration supports only the 32-bit version of Microsoft Internet Explorer.

Contact Center Manager Administration does not support Microsoft Edge.

Chapter 10: Agent Desktop computer requirements

This section provides the configuration requirements for the Agent Desktop client computers. Agent Desktop is a single-interface client application used by contact center agents to interact with customers. Agents download and install Agent Desktop client software from the Avaya Contact Center Select server. Avaya Contact Center Select agents use the Agent Desktop software in conjunction with an IP Office provisioned telephone.

Avaya Contact Center Select supports backwards compatibility with the previous Feature Pack or Service Pack version of Agent Desktop. This allows you to upgrade the Avaya Contact Center Select server without the requirement to upgrade Agent Desktop in a single maintenance window. For example, if you upgrade to Release 7.0 Feature Pack 3, you can use the Release 7.0 Feature Pack 2 version of Agent Desktop. New Agent Desktop features added in the latest Avaya Contact Center Select release are not available until you upgrade Agent Desktop to that release. Backwards compatibility is not supported for major or minor releases. For example, if you upgrade to Release 7.1, you cannot use the Release 7.0 version of Agent Desktop.

Note:

Agent Desktop does not support touch screen devices or tablets.

Note:

Agent Desktop does not support Network Address Translation (NAT).

Agent Desktop localized languages

Agent Desktop is supported in the following localized languages:

- English
- French
- German
- Italian
- Japanese
- Korean

- Latin Spanish
- Brazilian Portuguese
- Russian
- Simplified Chinese

A single Avaya Contact Center Select solution, with the localization language patches installed, supports all of the Agent Desktop localized languages. For example, a single English language Voice and Multimedia Contact Server supports the English, Chinese, French, and Russian language versions of Agent Desktop client software.

Avaya Contact Center Select supports Agent Desktop client operating systems that use a different language family to the Contact Center server.

Agent Desktop computer hardware requirements

The following table lists the minimum hardware requirements for a computer running Agent Desktop software.

Table 11: Agent Desktop computer minimum hardware requirements

Hardware item	Minimum requirements	Additional information
CPU	1 Gigahertz (GHz) or faster CPU with support for PAE, NX, and SSE2	Physical Address Extension (PAE), NX processor bit (NX), and Streaming SIMD Extensions 2 (SSE2) are features of the processor. These CPU features are required to run Microsoft Windows 7.0 and Microsoft Windows 8.1. Dual- and quad-CPU systems are supported with or without Hyper-Threading enabled.
RAM	1 Gigabyte (GB) (32-bit) or 2 GB (64-bit)	Additional memory is required, if you run other memory intensive applications at the same time as Agent Desktop.
Hard disk space	16 GB (32-bit) or 20 GB (64-bit)	
Hard disk partitioning	No specific partitioning requirements	—
Hard disk speed	2.5 inch disk minimum speed: 10000 RPM 3.5 inch disk minimum speed: 7200 RPM	—
Floppy drive	Not required	If a floppy drive is installed, it must be A.

Table continues…

Hardware item	Minimum requirements	Additional information
DVD ROM	Not required	
Network interface	One network interface card	100 Mb/s Ethernet or higher is recommended.
Video card	Microsoft DirectX 9 graphics device with WDDM driver	1024 x 768 pixels minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—

Agent Desktop does not support touch screen devices or tablets.

Client operating system requirements

The following table lists the operating system requirements for client computers.

Table 12: Client operating system requirements

Operating system	International versions supported	Minimum service pack
Windows 7 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) Japanese (JA) Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	
Windows 8.1 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) Japanese (JA)	

Table continues…

Operating system	International versions supported	Minimum service pack
	Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	
Windows 10 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) Japanese (JA) Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	

Third-party software requirements

This section describes the third-party software requirements for Agent Desktop client computers.

Agent Desktop supports only Microsoft Internet Explorer 10.0 (32-bit version only) and 11.0 (32-bit version only).

Agent Desktop supports only the 32-bit version of Microsoft Internet Explorer.

Agent Desktop does not support Microsoft Edge.

Agent Desktop client network infrastructure requirements

Agent Desktop is a client application which communicates with the Avaya Contact Center Select server. For optimal Agent Desktop operation, the underlying contact center network infrastructure must provide adequate latency and bandwidth between the agent computer and the Avaya Contact Center Select server.

This section provides a high-level overview of the data that is passed between Agent Desktop and the Avaya Contact Center Select server. It also sets out the recommended network values and likely impacts on agents if these values are not met. This section also describes the performance of Agent Desktop in varying Round Trip Time (RTT) and bandwidth environments.

Important:

Agent Desktop performance degrades as network Round Trip Time increases and network bandwidth decreases.

Network Latency

Network latency is a measure of the time delay experienced in a system, measured in Round Trip Time (RTT). RTT is the average Round Trip (packet) Time as measured using the ping command for a 1024-byte (1KB) data size.

For optimal performance, Avaya recommends a RTT of less than 80ms from the Agent Desktop client computer to the following Avaya Contact Center Select components:

- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Contact Center Manager Server (CCMS)

The RTT from the Agent Desktop client PC to the Avaya Contact Center Select server must be less than 120ms. For network environments with an RTT greater than 120ms, refer to the Citrix deployments of Agent Desktop in the next section.

RTT impacts on Voice traffic

This section describes how the underlying RTT and latency of the network affects the experience of handling voice traffic in Agent Desktop.

Agent Desktop used with a physical desk phone

The CCT component sends Computer Telephony Integration (CTI) signals to Agent Desktop, for example to prompt Agent Desktop to alert an incoming contact. These CTI signals are passed across the network as data. However, if the agent is using a physical desk phone, voice packets are transported across a network.

The following table details the time taken for the contact to alert on the Agent Desktop, compared to the time taken for the same contact to ring on the agent's phone, where the phone is subject to a constant RTT of 1ms.

RTT (ms)	Delay between desk phone ring and call alert on Agent Desktop	Delay between clicking Accept button on Agent Desktop and active voice path
1ms LAN	<0.5 Seconds	<0.5 Seconds
50ms	0.5 Seconds	1.0 Seconds
120ms	1.0 Seconds	2.5 Seconds

RTT impact on Multimedia Contacts

Contact Center Multimedia contacts are also affected by network latency. Agent Desktop downloads Customer contacts from the Avaya Contact Center Select server and displays their contents as soon as they are fully retrieved.

The table below shows how varying RTTs affect multimedia contact display times – in this case, email contacts – on Agent Desktop. The “Customer Details/Customer History Display” column indicates how much time passes between the email being opened on the Agent Desktop and the additional context information being loaded and displayed. These sample times are for ideal laboratory conditions.

RTT (ms)	Email Display	Customer Details/Customer History Display
1ms LAN	2 Seconds	0 Seconds
50ms	3 Seconds	Additional 3 Seconds
100ms	4 Seconds	Additional 4 Seconds
120ms	4 Seconds	Additional 5 Seconds

This data was generated using a 20KB email message, a customer history containing 30 contacts of 20KB each, in a network where bandwidth is not limiting the data transfer. Email messages of different sizes generate different results.

Bandwidth

The network bandwidth available to Agent Desktop client computers for communication with Avaya Contact Center Select servers is critical to Agent Desktop performance. If voice traffic is carried on the same network, this traffic is often prioritized above other network traffic – this bandwidth is therefore not available to Agent Desktop. In many cases agents use other third party applications over the same network. The bandwidth requirements of these third party applications must be considered as part of the overall bandwidth calculations (in addition to bandwidth allocated for voice soft phones and for Agent Desktop).

Several factors affect the recommended bandwidth for Agent Desktop. Depending on which Contact Center Multimedia (CCMM) features are in use on a given Customer deployment, not all factors apply. Indicative calculations to estimate the actual bandwidth usage are presented below for the various contact types and features. To calculate the required bandwidth, the relevant figures for the deployed features and supported contact types can be combined to derive an overall figure.

The network usage can be one of two types:

Constant traffic	These require dedicated, permanently available network use for the lifetime of the consumption. Examples of this type of traffic include; statistics display in Agent Desktop, update of live Web chat contacts. Many factors influence constant traffic levels, for example the number of agents with a large number of assigned skillsets, the number of active supervisors running RTDs in unicast mode, and large numbers of skillsets in use (large data packet) even for multicast.
Bursty traffic	The display of multimedia contacts and multimedia contact history is bursty traffic. A significant amount of data is downloaded to the Agent Desktop over a number of seconds. The frequency of these download is driven by agent activity.

Table continues…

	These require high usage of the available network for short times to download bursts of data. The time window that this data takes to download depends on the available network bandwidth at that time. Since this is not constant network consumption, a Kilo bits per second value is not reflective of the bandwidth required and a Kilo bit value has been provided instead.

Bandwidth impacts on Voice

If the agents are using a physical desk phone for voice or any other application which utilizes network bandwidth, this needs to be factored into the engineering of the network to meet the expected performance levels on Agent Desktop.

Retrieve Customer History on voice contacts

The Agent Desktop Customer History feature enables agents to retrieve voice callers' multimedia Customer history, from the Avaya Contact Center Select server, when a voice contact is accepted. Agent Desktop Customer History is an optional feature which is enabled in the CCMM Administration tool. These historical contacts can be of any multimedia contact type. Agent Desktop Customer History requires adequate bandwidth to function and it must be included in your network bandwidth planning calculations.

To calculate the impact of a voice callers' multimedia Customer history on bandwidth, consider voice contacts as an additional Multimedia contact type and add the number of voice contacts to your multimedia calculation for bandwidth calculations.

Multimedia Contact bandwidth requirements

This section details the bandwidth requirement of Agent Desktop Customer History for the following multimedia contact types:

- Email messages
- Fax messages
- Scanned Documents (SD)
- SMS text messages
- Outbound contacts
- Web Communications (WCs)

This section also details the bandwidth requirement for voice contact types if multimedia history display is enabled.

Some multimedia contact supports attachments and these attachments must also be included in network calculations:

- Email contacts are of variable size. The average email size is a reasonable estimate, and is used for Agent Desktop calculations.
- Fax messages are delivered as email attachments. Fax messages must be included in the attachment size and rate estimates.
- Outbound contacts from Avaya Contact Center Select solution do not have attachments.
- SMS test messages from customers. SMS test messages do not have attachments.

- Web chat messages do not have attachments.

The Agent Desktop Customer History feature enables agents to retrieve multimedia Customer history (containing up to 30 previous contacts), from the Avaya Contact Center Select server, when a multimedia contact is accepted. Agent Desktop Customer History requires adequate bandwidth to function and it must be included in your network bandwidth planning calculations. Retrieving Agent Desktop Customer history from the Avaya Contact Center Select server uses the bursty type of network data, and where the Customer history feature is enabled, it must be included in all network bandwidth calculations.

Example of calculating the bandwidth requirements of Agent Desktop Customer history downloads (based on ideal laboratory conditions):

N = Number of agents working on multimedia (MM) contacts. If the feature to display multimedia history with voice calls is activated, then N must include voice agents.

C = Maximum number of multimedia contacts per hour for the entire contact center solution. If the feature to display multimedia history with voice calls is activated, then C must include voice traffic per hour to all those agents.

avg_contact_size = average size of a contact in Kbits (not Kbytes). (Kbits = KBytes * 8). In many cases this is the average size of the incoming or outgoing email.

att_rate_in = percentage of incoming contact attachments. Contact attachments apply to email messages and fax messages.

att_rate_out = percentage of incoming email messages that are responded to with agent attached attachments in the reply.

avg_att_size = average size of an attachment in Kbits. Contact attachments apply to email messages and fax messages.

Note:

In-line attachments must also be included in the bandwidth calculations as regular attachments.

A key factor in calculating the minimum bandwidth for processing multimedia contacts is an assessment of the number of active agents that accept contacts in any one second period. The available bandwidth is shared across all of these agents in this time period.

The long term average number of agents active in any one second is calculated as follows:

$n_{average}$ = Roundup(C / 3600)

This equates to the average number of agents clicking the Accept button on the Agent Desktop at any one time. However, since the length of time it takes an agent to handle a contact is random, the number of agents clicking the Accept button is random. It is incorrect to engineer a bandwidth solution based solely on this average, as nearly 50% of the time more than $n_{average}$ agents are clicking the Accept button.

Therefore the number of active agent per second is calculated with a factor F as follows:

n_{active} = Roundup(F* C / 3600)

where F is an engineering factor between 3 and 10. A higher value for F must be used when N, the total number of agents processing multimedia contacts and multimedia history with voice

contact, is lower than 50. The choice of value F is your decision. F reflects the amount of extra bandwidth to build into your network to handle both the inherently random distribution of agent activity which results in natural peaks of use and any data spike events attributable to your particular Contact Center business models, such as initial shift start times, promotions and emergencies. A higher value reduces the level of bandwidth limitation caused by the overlapping of multiple agent download of multimedia contacts.

Once F is defined, the minimum bandwidth (in Kbits per second) can be estimated as follows:

$BWMM_{min}$ =

n_{active} * ((avg_contact_size * 64) + 2000) + avg_att_size * (att_rate_in% + att_rate_out%) / 100) Kbps

Important:

The minimum recommended bandwidth available for processing multimedia contacts $BWMM_{min}$ must be greater than 10 Mbits per second.

The time to download and display contacts on Agent Desktop is directly impacted by the bandwidth available between the Avaya Contact Center Select server and Agent Desktop at the time when the contact is accepted in Agent Desktop. The impact of bandwidth limitation is observed as a delayed display of contact and contact history in the Agent Desktop.

The following table demonstrates the impact of limiting bandwidth on multimedia contact display times on Agent Desktop. The data was generated using a 20KB email message, a Customer history of 30 contacts of 20KB size each, with a fixed RTT of 80ms.

Available bandwidth	Email display	Customer Details/Customer History Display
1Mbps	3 Seconds	Additional 6 Seconds
3Mbp	3 Seconds	Additional 3 Seconds
5Mbps	3 Seconds	Additional 2 Seconds

Retrieve Customer History on Voice contacts

This optional feature enables Agent Desktop to retrieve voice callers' multimedia Customer history (containing up to 30 previous contacts), from the Avaya Contact Center Select server, at the time a voice contact is accepted. These historical contacts can be of any multimedia contact type. If this feature is activated, the size of this history can be added to your network planning by considering voice as an additional multimedia contact type and adding the number of voice contacts to your multimedia calculation.

Web Communication (WC) network bandwidth calculation

Processing web communications, after they have been received by the agent requires a constant level of bandwidth.

Network usage type: Constant

c = Number of WC contacts per hour

avg_session_length = Average length in seconds of WC session

Data size: 50 Kbps per active WC contact

WC network bandwidth requirement (Kbps):

WC_{BW} = (c * 50Kbps * avg_session_length)/ 3600

Presence network bandwidth calculation

Presence updates require a constant level of bandwidth.

Network usage Type: Constant

N = Number of agents working on MM contacts

avg_pres = Average number of presence updates per user per hour

Data size: 7 Kb per Presence update

Presence network bandwidth requirement (in Kbps) = (N* 7Kb * avg_pres)/ 3600

CCMM Search network bandwidth calculation

Bandwidth must be provided for an agent carrying out multimedia searches.

Network usage Type: Bursty

N = Number of agents running searches

average_search = Average number of searches per hour

Data transmitted: 1280Kb per search

CCMM Search bandwidth requirement (in Kbps) = (1280Kb * average_search * N)/3600

CCMM Pull Mode network bandwidth calculation

Pull Mode allows agents to work outside the normal Avaya Contact Center Select routing mode. They personally select individual contacts from the Avaya Contact Center Select queues. Their view of the Avaya Contact Center Select queue is automatically updated using the same web services as the Avaya Contact Center Select CCMM search feature, and so uses the same bandwidth.

N = Number of agents working in Pull Mode

c = Number of contacts per hour per agent

Data transmitted: 1280Kb per search

CCMM Pull Mode search bandwidth requirement (in Kbps) = (1280Kb * c * N)/3600

Web Statistics network bandwidth calculation

Network usage Type: Bursty

N = Number of agents

avg_skills = Average number of skillsets per agent

Data transmitted: 3.2 Kb per skillset once a minute

Web Statistics bandwidth requirement: (3.2 Kb * avg_skills * N)/60

Agent Desktop downloads by agent

Agent Desktop is a smart client which is downloaded from the Avaya Contact Center Select server over the network onto each agent computer on initial install. On each software update (service pack or patch) the updated Agent Desktop is re-downloaded onto each agent computer. The download requirements of Agent Desktop must be considered when planning the bandwidth requirements to remote agents.

Summary of total bandwidth requirements

You must sum up all the applicable bandwidth demands listed above to arrive at a minimum bandwidth for the site. Calculate the cumulative bandwidth for all multimedia features.

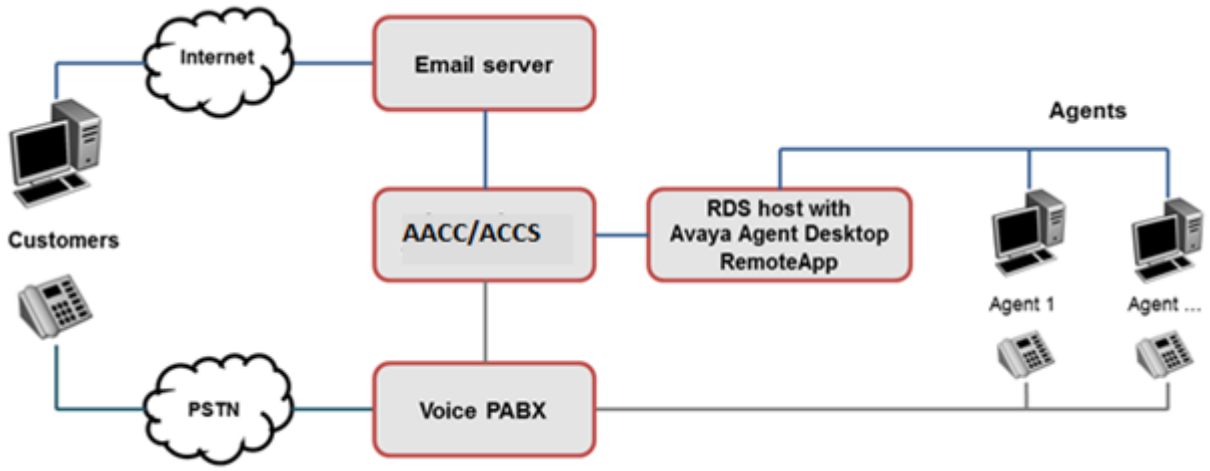
Remote Desktop Services support

Avaya Contact Center Select (ACCS) supports using Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop.

Remote Desktop Services, formerly known as Terminal Services, allows a server to host multiple simultaneous client sessions. In the Remote Desktop Services (RDS) environment, an application runs entirely on the Remote Desktop Session Host (RD Session Host) server. The RDC client performs no local processing of application software. The server transmits the graphical user interface to the client. The client transmits the user's input back to the server. With RDS, only software user interfaces are transferred to the client system. All input from the client system is transmitted to the server, where software execution takes place.

You must use the Agent Desktop MSI package for Remote Desktop Services deployments. How you deploy and use Agent Desktop RDS clients depends on your solution requirements and virtualization infrastructure. For more information about building a client infrastructure using RDS, refer to the Microsoft Remote Desktop Services product documentation.

The following diagram shows a typical Remote Desktop Services solution with Agent Desktop hosted on the RDS Session Host server.



Remote Desktop Services requires careful up-front planning and engineering. It requires some additional maintenance and full organizational support to deliver an enterprise grade contact center agent and customer experience.

RemoteApp:

RemoteApp allows you to make programs that are accessed remotely through Remote Desktop Services appear as if they are running on the end user's local computer. These programs are referred to as RemoteApp programs. Instead of being presented to the user in the desktop of the Remote Desktop Session Host (RD Session Host) server, the RemoteApp program is integrated with the client's desktop. The RemoteApp program runs in its own resizable window, can be dragged between multiple monitors, and has its own entry in the taskbar. If a user is running more than one RemoteApp program on the same RD Session Host server, the RemoteApp program shares the same Remote Desktop Services session.

Limitations:

The following limitations apply when you use Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop:

- Agent Desktop My Computer embedded softphone mode is not supported. Agents must use a desk phone, or use a supported softphone concurrently with Agent Desktop.
- Avaya recommends that the RDS server hosting Agent Desktop is located in the same Local Area Network (LAN) as the ACCS server. If the RDS server hosting Agent Desktop is not in the same LAN as the ACCS server, then the ACCS bandwidth, Round Trip Time, and networking requirements apply.
- ACCS supports the Multicast option only for Real-Time Displays (RTDs) in a RDS environment. Unicast is not supported in a RDS environment.
- You cannot use the ACCS server as the RDS host.
- Agents must define default template or attachment folders in Agent Desktop preferences to an AppData folder on the RDS host. Agents do not have access to shared or mapped drives. For more information on configuration settings for temporary folders on the RDS Host Server, refer to the Microsoft Remote Desktop Services product documentation.

For information about how to use Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop, see *Avaya Contact Center Select Advanced Administration*.

Client Citrix support

Agent Desktop is supported as a Citrix-published application. A Citrix server solution uses software to deliver on-demand Windows applications to physical desktops. This allows client users (agents in this case) to access and use programs which are available on the Windows Server 2012 R2 operating system of the Citrix server.

Agent Desktop supports the following versions of Citrix server:

- Citrix XenApp 6.5
- Citrix XenApp 7.x

On the Avaya Contact Center Select server the Agent Desktop folder is typically located in:

`D:\Avaya\Contact Center\Multimedia Server\Agent Desktop\client`

This folder contains the entire Agent Desktop application. Copy this folder on the Agent Desktop server to the Citrix server. Then configure your Citrix server to publish Agent Desktop as a published application, accessed from this Agent Desktop folder on the Citrix server. On the Citrix server select the users (agents) allowed to run the Agent Desktop published application. For more information about Citrix application publishing, see your Citrix documentation. For more information on how to configure your Citrix server to publish Agent Desktop as a published application, see *Avaya Contact Center Select Advanced Administration*.

The Citrix server publishing Agent Desktop must be located in the same Local Area Network (LAN) as the Avaya Contact Center Select server.

Avaya Contact Center Select supports only the Multicast option for Real-Time Displays (RTDs) in a Citrix environment. Avaya Contact Center Select does not support the Unicast option for Real-Time Displays (RTDs) in a Citrix environment.

Agent Desktop network ports

Agent Desktop uses the following network ports to communicate with Contact Center components.

Feature	Component	Port number
HTTP (Web services)	CCMM	80
HTTP (Web services)	CCMM	443 (if TLS is enabled for CCMM)
CCT	CCT	29373
Voice History	CCMS	57772
Web Statistics	CCMS	9086

Chapter 11: Contact Center Agent Browser application requirements

This section provides information on the configuration requirements for the Contact Center Agent Browser application.

Voice-only Contact Center agents can use the Agent Browser application to log on to Contact Center and perform basic tasks. The Agent Browser application does not provide call control, multimedia features, or supervisor functions. Agents must use a supported desktop phone for call control. The Agent Browser application supports the following tasks:

- logging on and off
- changing the agent status
- setting not ready reason codes
- setting activity codes
- setting after call work item codes
- calling your supervisor
- handling an emergency

The Contact Center Agent Browser application is supported only in SIP-enabled Contact Center solutions. All agents using Agent Browser require an associated Windows domain account, or a local Widows account, configured in CCMA, to log on to Agent Browser. If using a domain, the agent domain accounts must be in the same domain as the Contact Center server.

Agents access the Agent Browser application through a web browser, using the Contact Center server Fully Qualified Domain Name (FQDN). In Business Continuity solutions, agents must log on to the Agent Browser application using the FQDN of the Business Continuity pair.

In the event of a switchover to a Remote Geographic Node (RGN) server, agents must log on to the Agent Browser application using the FQDN of the RGN server.

The Agent Browser application does not support the Remote Agent feature.

You must access the Agent Browser application using HTTPS only. You must also install a valid TLS certificate, issued by a trusted Certificate Authority (CA), in Security Manager. To avoid certificate security warnings, install the root certificate of the CA on all client devices used to access the Agent Browser application. For more information, see Avaya Contact Center Select secure TLS communications on page 180.

If you use a mobile device to access the Agent Browser application, Avaya recommends using a medium size screen of 992 pixels or higher. Some mobile devices automatically lock after a defined

timeout period — the Agent Browser application has no control over the automatic locking of mobile devices.

Language support

The Contact Center Agent Browser application supports the following languages:

- English
- French (FR)
- German (DE)
- Italian (IT)
- LA Spanish (ES)
- Brazilian Portuguese (PT-BR)
- Russian (RU)
- Simplified Chinese (Zh-CN)
- Traditional Chinese (Zh-TW)
- Japanese (JA)
- Korean (KO)

You can set the application language on the Settings menu of the Agent Browser application.

Web browser requirements

The Agent Browser application is hosted on the Internet Information Services (IIS) that is running on the Contact Center server. Agents access the application through a web browser. The following table lists the supported browsers.

Browser	Versions supported	Operation system
Microsoft Internet Explorer	11.0	• Windows 7 • Windows 8.1 • Windows 10
Microsoft Edge	20.10240	• Windows 10
Google Chrome	43.0.23	• Windows 7 • Windows 8.1 • Windows 10 • Android 4.4.2 • Android 5.0.1 • iOS 8.3

Table continues…

Browser	Versions supported	Operation system
		• OS X Yosemite 10.10.3
Mozilla Firefox **Important:** The Agent Browser application does not support using the “Search for text when I start typing” feature in Firefox.	38.0.5	• Windows 7 • Windows 8.1 • Windows 10
Safari	8.0.5	• iOS 8.3 • OS X Yosemite 10.10.3

Chapter 12: Avaya Contact Center Select secure TLS communications

Avaya Contact Center Select (ACCS) includes a number of services that you can secure by using the HTTPS protocol. At the installation stage, you can use the Ignition Wizard to create a security store, generate a Certificate Signing Request (CSR) and import a Certificate Authority root certificate. Alternatively, you can skip security configuration at the installation stage and configure your security certificates later using Security Manager.

HTTPS security basics

HTTPS is a secure protocol for Web communications. HTTPS provides both authentication of the Web server, and encryption of communications between the server and the client in both directions. HTTPS uses connections encrypted by the Transport Layer Security (TLS) protocol.

When a client initiates a secure connection with a server, the server returns its public cryptographic key in a server certificate. To ensure the integrity of the server certificate, it must be signed by a third party, called a Certificate Authority (CA). The client must have a root certificate from the CA that provided the signed server certificate. If the client has a matching root certificate, it completes the connection and secure communication is established.

Encryption levels, TLS versions, and SSL

Avaya Contact Center Select (ACCS) supports both the SHA1 and SHA2 cryptographic hash functions, with key sizes of 1024, 2048, or 4096. However, the SHA1 hash function and the 1024 key size do not provide the current industry-recommended level of encryption. ACCS supports SHA1 and a 1024 key size only to provide backward compatibility.

Avaya recommends that you use only SHA2 either a 2048 or 4096 key size. The default values for new security stores are SHA2 with a 2048 key size.

Secure Sockets Layer (SSL) also is obsolete, having a number of known weaknesses. Contact Center now uses only Transport Layer Security (TLS) for secure communications. Note that TLS is an extension of the older SSL protocol, and the industry frequently accepts and uses the term ‘SSL’ to refer to TLS.

Contact Center implements Transport Layer Security (TLS) version 1.2 as the default minimum version negotiated for secure communications. This is to avoid security vulnerabilities that exist in TLS 1.0. For backward compatibility and inter-operation with third-party or custom applications connecting to Contact Center, Administrators can set lower versions of TLS on certain

communication channels. When a lower version of TLS is available, Contact Center still negotiates the highest level of TLS that the other application can support.

Server certificate

The server certificate, sometimes called a signed certificate, is the certificate that the server sends to a client that requests a secure service (HTTPS). The server certificate combines a public key used for encryption with an organization's details, and is signed by a certificate authority to allow clients to verify that it is valid. The client can use the server certificate to encrypt the data it sends to the server.

Certificate Authority

A Certificate Authority (CA) is a third-party organization that provides digital certificates that certify the owner of a public key for cryptography used in secure communications. If you use a single CA for all your security setup, it reduces you workload for security configuration, because you need to copy just a single root certificate to all clients. The root certificates for many well know CAs are frequently already embedded in common operating systems for clients and servers.

Root certificate

The root certificate proves the authenticity of the signed certificate. It contains a digital signature from a Certificate Authority (CA). To trust the server certificate sent to them by the server, clients must have a copy of the root certificate with the digital signature of the CA that signed the server certificate. Root certificates exported from different security stores work in the same way if they contain a digital signature from the same CA.

Server Certificate name

Each server certificate has a name, which normally derives from the server Fully Qualified Domain Name. If a server certificate name does not match the name of the website or web service to which the client connected, the client generates a warning. This impacts ACCS as follows:

- In Business Continuity (BC) systems, you need to commission your own certificates with Subject Alternative Names (SANs) to use the managed name of the campus HA pair. Therefore you must decide on the managed name before you set up your own certificates.

Subject Alternative Name

A Subject Alternative Name (SAN) is an extension to HTTPS that allows various values to be associated with a security certificate. These values are called "Subject Alternative Names", or SANs. There are several types of SAN values, but for ACCS only the DNS name type is relevant.

In ACCS you use SANs on security certificates to include the BC active, standby, and managed names in the server certificate, so that secure connections continue during a BC switchover and clients do not see warning messages.

When you create the ACCS security store in Security Manager, you can add SANs to the server certificate.

Avaya Contact Center Select security store

Avaya Contact Center Select (ACCS) includes a security store to enable secure communications over Transport Layer Security (TLS), both between ACCS applications and with external clients or

third party applications. Customers must create a security store using either the Ignition Wizard or Security Manager, with a server certificate and root certificate from a Certificate Authority (CA).

ACCS also uses the Internet Information Services (IIS) security store for some services. On an ACCS server, Security Manager controls both the IIS security store and the ACCS security store. These two stores always use the same server certificate, which you configure in Security Manager.

Avaya Aura® Media Server also has a security store. You configure this store through Avaya Aura® Media Server Element Manager.

Figure 15: Example of security stores on a single ACCS server with co-resident Avaya Aura® Media Server

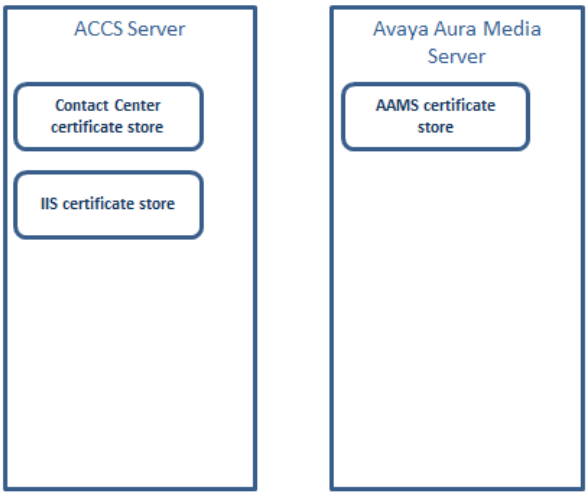


Figure 16: Example of security stores on an ACCS server with standalone Avaya Aura® Media Server

The following table lists the security stores on the ACCS servers:

Security store	Applications	Services that use this store	Managed by
ACCS security store	CCMS, CCT	TAPI-D CTI link	ACCS Security Manager
Windows 2012 IIS security store	CCMA, CCMM	CCMA CCMM Administration Agent Desktop Multimedia Services Orchestration Designer Outbound Campaign Management Tool CCT Web Administration	ACCS Security Manager

ACCS services that can use TLS security

The following table lists all the ACCS services that must be secure, or can be configured to be not secure.

ACCS Service	Always secure	Security optional
TAPI-D CTI connection	Y	
Agent Browser application	Y	
CCMA Administration		Y
CCMM Administration		Y
Agent Desktop		Y
Orchestration Designer		Y
Outbound Campaign Management Tool		Y
ACCS Web Services		Y
CCT Web Administration		Y

- These services all use the server certificate that you configure in Security Manager. If you change this certificate, the change impacts all the services.
- You must use a certificate for TAPI-D CTI services and Agent Browser application. You generate this certificate in ACCS Security Manager. The CTI connection between ACCS and IPO requires Mutual Transport Layer Security (MTLS).

  The IPO server has a server certificate and must have the ACCS root certificate. The ACCS server has a server certificate and must have the IPO root certificate.
- You must use a certificate for Web Services, unless you turn off Web Services security. You use the certificate in Security Manager.
- You must use a certificate for Avaya Aura® Media Server. On an ACCS with Avaya Aura Media Server, you can use the server certificate you created in Security Manager.

Contact Center automatically backs up a new security store when you create it. This allows you to recover from situations where the store is damaged or deleted between sending the Certificate Signing Request (CSR) to a Certificate Authority (CA), and receiving a signed certificate back from

the CA. The location for this automatic security store backup is `D:\Contact Center \autoBackUpCertStore`. Do not overwrite or delete this backup location.

Avaya Contact Center Select Security Manager

Avaya Contact Center Select (ACCS) includes a number of services that you can secure by using the HTTPS protocol.

ACCS Security Manager provides an interface for managing the security certificates in the ACCS security store and the IIS security store. ACCS supports the management of the IIS security store only through Security Manager: do not use IIS functions to manage the IIS security store on an ACCS server. Security Manager supports importing chained certificates, and places these certificates in the security store for distribution across the solution.

Server certificates

Each security store must have a server certificate signed by a CA, and a root certificate from the same CA. In ACCS, you can use the same server certificate in all the security stores on a single server. You can also generate different server certificates for each security store on a single server. You cannot use the same server certificate on two different servers.

Certificate Authority root certificates

When a client initiates a secure connection with a server, it must have a root certificate from the CA that provided the signed server certificate. If the client does not have a matching root certificate, it does not complete the connection. If the client has a root certificate from a given CA, it can trust any server certificate signed by that CA.

Avaya recommends that you use a single CA to sign all the certificates in your contact center. This simplifies the deployment process, because you need to distribute only a single root certificate to all the clients.

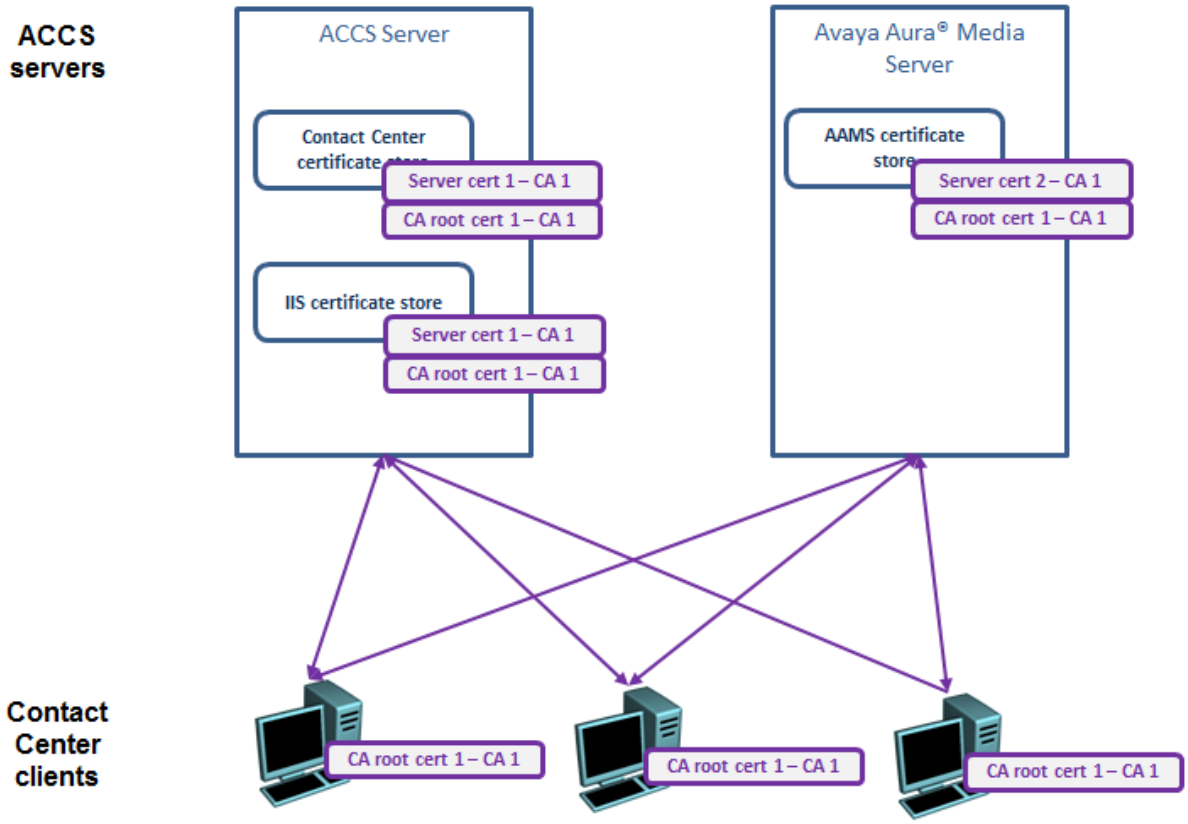


Figure 17: Example of how a single CA root certificate can work with different server certificates signed by the same CA

If you want to use different CAs to sign certificates for your different servers, you must copy the root certificate from each CA to all the clients in your contact center. For some ACCS Web services, ACCS servers can act as clients of other servers. Therefore you must ensure that the ACCS servers also have the required CA root certificates.

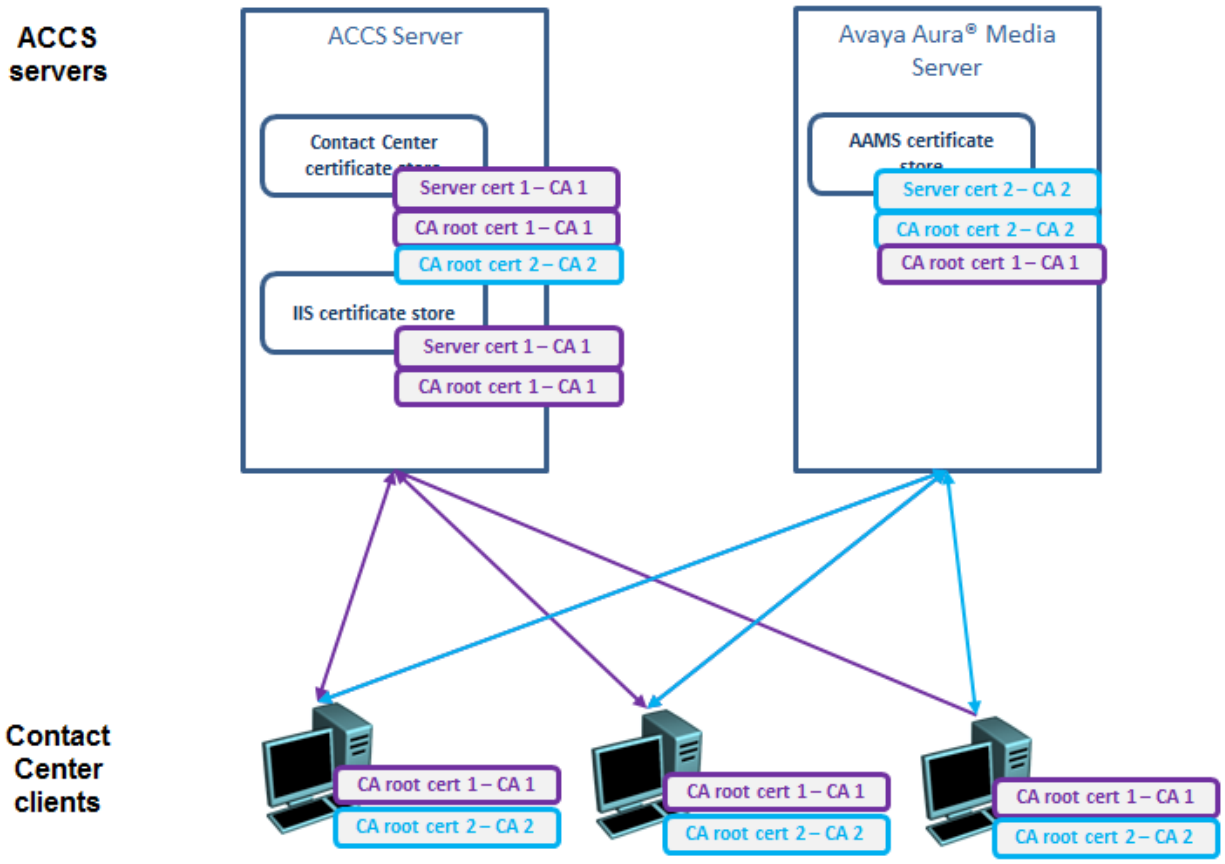


Figure 18: Example of how clients must have the CA root certificates from each CA that signed a server certificate, if the contact center uses server certificates signed by different CAs

You can distribute root certificates to client computers using a Group Policy on Microsoft Windows Server 2012.

TLS Security in a Business Continuity environment

If you implement Business Continuity (BC), Avaya Contact Center Select (ACCS) clients and servers must be able to communicate with the active contact center server, the standby contact center server, and the managed name of the BC server pair.

In a BC system, create a security store with Subject Alternative Names (SANs). The security store for a BC pair must have the common name of the ACCS server, and a SAN for:

- the ACCS server name
- the managed name of the BC pair

This ensures clients connecting to ACCS using the managed name do not get warnings that the server certificate name does not match the server name.

ACCS supports using the same certificate on both the active server and the standby server in the BC pair.

Avaya recommends that you plan your BC active, managed, and standby names in advance of creating a new security store. In this way you can create your certificates once using SANs during the initial commissioning, instead of re-creating certificates when you commission BC.

Migrating secured Contact Center systems

You cannot migrate a Contact Center security store from Release 6.x to Release 7.0. If you are migrating a secure Contact Center system from Release 6.x, you must create a new security store on the Release 7.0 Contact Center server.

Avaya Contact Center Select Security store notifications

Security certificates contain an expiration date and they are not valid after this date. If the security certificates used by Avaya Contact Center Select (ACCS) expire, the contact center loses call control and stops functioning.

Security Manager provides a security store inspection utility to help you monitor and maintain valid security certificates. You can use Security Manager to schedule a security store inspection task. Security Manager adds the scheduled task to the underlying Windows Task Scheduler. The scheduled task runs the security store inspection utility once a week. The inspection utility checks the status of the security certificates in the ACCS security store. If any of the security certificates are due to expire within a month, the inspection utility sends a notification email to the contact center administrator. The contact center administrator must then refresh the security certificates.

Security Manager provides the notification email; it cannot renew expired security certificates. For uninterrupted ACCS functionality, if you receive an email about upcoming certificate expiration dates, you must renew the security certificates before they expire. Security Manager uses the Microsoft Windows Task Scheduler to schedule the weekly security store inspection. You must ensure that there is a Microsoft Windows user account that has the necessary privileges from which Security Manager can schedule a task on Windows Task Scheduler. You can use the Windows administrator account that you used to install ACCS to add a task to Windows Task Scheduler.

Security Manager uses a specified Simple Mail Transport Protocol (SMTP) server to send the notification emails to the administrator’s email address. ACCS does not provide this SMTP server. You must provision this SMTP server and ensure that the ACCS server can communicate with it at all times. ACCS does not support Transport Layer Security (TLS) connectivity to this SMTP server.

Server Message Block signing

Contact Center installs and updates modify the Windows Server 2012 local group policy to enable Server Message Block (SMB) signing. SMB signing places a digital tag into each server message block, which helps prevent man-in-the-middle attacks on network file sharing.

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

Chapter 13: Avaya Contact Center Select port matrix

This section lists the ports used by Avaya Contact Center Select. The Avaya Contact Center Select server contains the following components:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)
- Contact Center Multimedia (CCMM)
- Avaya Aura® Media Server

These components use the following ports.

Contact Center Manager Server port requirements

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

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

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

Table 13: Contact Center Manager Server port usage

CCMS port number	Functionality
445	TCP port used Windows File and Printer Sharing for Microsoft Networks. Required when copying data between active and standby servers using Windows File Sharing.
1550	HDX CAPI
1972	Caché database, and Caché shadowing
4422	HDX NameService
12668–12670	TraceControl
10000	Hardcoded Toolkit Name Service
10001–10082	Networking
10038	NCP_CHANNEL—This channel is used to communicate between the NCP of one node to the NCP of another node. The NCP on one node sends sanity messages to the other node through this port.
10039	ASM_CHANNEL—Different modules like NCP and TFE send messages to ASM through this channel.
10040	NCP_ASM_CHANNEL—ASM uses this channel to send messages to NCP.
10060	ASM_Service—The ASM service runs on this port. The Service Control Manager can send messages such as START, STOP, and RESTART to the ASM service through this port.
10062	NCP_Service—The NCP service runs on this port. The Service Control Manager can send messages such as START, STOP, and RESTART to NCP on this port.
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
9080–9083	Web Services Open Interfaces
9086	CC Web Statistics
9100	XMPP Web Service Server Port
9120	XMPP Web Service Client Port
57012	System Management and Monitoring Component (SMMC) system tray.

Contact Center Manager Administration port requirements

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

Table 14: Contact Center Manager Administration port usage

CCMA port number	Functionality
TCP 80	For Internet Explorer communication.
TCP 443	For secure HTTP communication (only applicable if SSL is enabled for secure Internet Information Services (IIS) communication).
TCP Port 445	Windows File and Printer Sharing for Microsoft Networks. Required when copying data between active and standby servers using Windows File Sharing.
TCP Port 3389	For remote desktop connection.
TCP Port 25 (SMTP)	For the Historical Reporting component to send email notifications when reports are printed and saved.
TCP Port 8200	For the Emergency Help component on the client PC.
UDP ports 6020, 6030, 6040, 6050, 6060, 6070, 6080, 6090, 6100, 6110, 6120, 6130	For the CCMA server to receive IP multicasting data from CCMA Server (needed for Real-Time Reporting and Agent Desktop Displays).
UDP ports 7020, 7030, 7040, 7050, 7060, 7070, 7080, 7090, 7100, 7110, 7120, 7130, 7140, 7150	For the CCMA server to send IP multicasting data to client PCs (needed for Real-Time Reporting and Agent Desktop Displays).
UDP ports 7025, 7035, 7045, 7055, 7065, 7075, 7085, 7095, 7105, 7115, 7125, 7135, 7145 and 7155	For the CCMA server to send IP unicast data to client PCs. This is an optional method of sending the data required for Real-Time Reporting. If you do not use the multicast method, then you must configure the unicast option. You can also use a combination of the two methods.
TCP Port 10000	Used by the Nameservice process on the CCMA server (nbnmsrvc.exe). It permits communication between the CCMA server and the server in Contact Center Manager Server. **Important:** The default port for the third-party software. This conflicts with the default port used by the CCMA Toolkit NameService. To avoid issues with CCMA functionality when using Veritas Backup Exec, you must change the default port of Veritas Backup Exec to another port number that is not being used by the network.
Default UDP port 3998	License Manager destination port.
Default UDP ports 3999 - 4007	License Manager destination source port.

Communication Control Toolkit port requirements

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

Table 15: Communication Control Toolkit port usage

CCT port number	Functionality
1972	Caché database, and Caché shadowing solutions.
3998	License Manager (LM) destination port, which is the first of 10 consecutive ports required for license management.
3999 - 4007	LM client source ports.
5000	To connect to the server in CCMS.
8081	Default port of the Apache Tomcat Server which hosts the CCT Web Administration.
8085	For CCT services to access the CCT database.
8098	For the Contact Management Framework on the CCT server.
8099	For the Contact Management Framework on the CCT server.
8087	For CCT CMF component.
9000	For CCT WebAdmin component.
9010	For CCT CMF component.
11110	Used by the CCT Server service for the CMF Web Service - Callback port.
11111	Used by the CCT Server service for the CMF Web Service - Web server port.
29373	Listens for requests from CCT client applications.
29374	Data Access Layer Service listens for requests from CCT Remote Administration Console.

Contact Center Multimedia port requirements

The following table lists the configurable Multimedia ports.

Table 16: Contact Center Multimedia ports

Port	Host	Client	Network interface	Functionality
1972	Contact Center Multimedia	Contact Center Manager Administration Server	Contact Center Multimedia Caché database	Port opened on database for reporting. Caché database, and Caché shadowing.
445	Windows File and Printer Sharing for Microsoft Networks.	Windows File and Printer Sharing for Microsoft Networks.	Windows File and Printer Sharing for Microsoft Networks.	Windows File and Printer Sharing for Microsoft Networks. Required when

Table continues…

Port	Host	Client	Network interface	Functionality
				copying data between active and standby servers using Windows File Sharing.
110	Email server	Email Manager	Email server POP3	Receiving email
143	Email server	Email Manager	Email server IMAP	Receiving email
995	Email server	Email Manager	POP3 over SSL (optional)	Receiving secure email (optional)
993	Email server	Email Manager	IMAP over SSL (optional)	Receiving secure email (optional)
110	Email server	Email Manager	POP3 over TLS (optional)	Receiving secure email (optional)
143	Email server	Email Manager	IMAP over TLS (optional)	Receiving secure email (optional)
25	Email server	Email Manager	SMTP	Sending email
25	Email server	Email Manager	SMTP over TLS (optional)	Sending secure email (optional)
80	Contact Center Multimedia Server	Any Web services client (Agent Desktop, OCMT, and third-party Web services)	SOAP protocol	Accessing http Web services
29373	Communication Control Toolkit Server	Agent Desktop	Communication Control Toolkit	Remote access from clients to Communication Control Toolkit server (for Agent Desktop application)
57012	System Management and Monitoring Component (SMMC) system tray	System Management and Monitoring Component (SMMC) system tray	System Management and Monitoring Component (SMMC) system tray	Database shadowing

Avaya Aura® Media Server port requirements

The following table shows the port numbers required for Avaya Aura® Media Server on Windows Server 2012 R2.

Table 17: Avaya Aura® Media Server port usage–Windows Server 2012 R2

Port	Type	Permit in TCP Filter	Description
1027	TCP	Yes	License Server
1028	TCP	No	System Monitor mchb
3306	TCP	Yes	MySQL
3389	TCP	Yes	Remote Desktop
3867	SCTP	No	Diameter over SCTP
3868	TCP	No	Diameter over TCP
3869	TCP	No	Diameter over TLS
4001	TCP	No	IvrMP MSLink
4004	TCP	No	Sip UA MSLink
4005	TCP	No	Resource Manager ExtSess
4014	TCP	No	SIP UA cmd i/f
4015	TCP	No	Resource Manager and i/f
6080	TCP	No	Agent Greeting
7080	TCP	No	ConfMP MSLink
7410	TCP	Yes	SoapServer
7411	TCP	Yes	SoapServer TLS
8080	TCP	Yes	EM HTTP
8443	TCP	Yes	EM HTTP(s)
11004	TCP	No	DiamC MSLink
11014	TCP	No	DiamC and i/f
19899	TCP	Yes	Resource Manager CPLink
19999	TCP	Yes	IvrMP ssdata
20005	TCP	Yes	CStore MSLink
20007	TCP	Yes	CStore RTFT
20009	TCP	Yes	IvrMP RTFT
21000	TCP	No	Voice XML Interpreter IPC
51000	TCP	No	Resource Manager IPC
51001	TCP	No	Legacy MPS Alarm deamon
51003	TCP	No	CCXML Interpreter IPC

The following table shows the port numbers required for Avaya Aura® Media Server on Linux.

Table 18: Avaya Aura® Media Server port usage–Linux

Port	Type	Permit in TCP Filter	Description
1027	TCP	Yes	License Server
1028	TCP	No	System Monitor mchb
3306	TCP	Yes	MySQL
3867	SCTP	No	Diameter over SCTP
3868	TCP	No	Diameter over TCP
3869	TCP	No	Diameter over TLS
4001	TCP	No	IvrMP MSLink
4004	TCP	No	Sip UA MSLink
4005	TCP	No	Resource Manager ExtSess
4014	TCP	No	SIP UA cmd i/f
4015	TCP	No	Resource Manager cmd i/f
5060	TCP	Yes	SIP over TCP
5060	UDP	No	SIP over UDP
5061	TCP	Yes	SIP over TLS
6080	TCP	No	Agent Greeting
7080	TCP	No	ConfMP MSLink
7410	TCP	Yes	SoapServer
7411	TCP	Yes	SoapServer TLS
8080	TCP	Yes	EM HTTP
8443	TCP	Yes	EM HTTP(s)
11004	TCP	No	DiamC MSLink
11014	TCP	No	DiamC and i/f
19899	TCP	Yes	Resource Manager CPLink
19999	TCP	Yes	IvrMP ssdata
20005	TCP	Yes	CStore MSLink
20007	TCP	Yes	CStore RTFT
20009	TCP	Yes	IvrMP RTFT
20011	TCP	No	Resource Manager IPC
21000	TCP	No	Voice XML Interpreter IPC

UDP Port Range is required for media processing. All starting UDP ports are configurable.

Table 19: Required UDP Port Range

Operating System	UDP Port Range
Windows Server 2012 R2	20000 to 45499
Linux	6000 to 32599

Index

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W