Avaya Call Management System

Overview and Specification

Release 18.0.2
February 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 AVAILABLEON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

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

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole

or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third party components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at:

https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com , or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document describes tested product characteristics and capabilities including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.

Intended audience

This document is intended for anyone who wants to gain a high-level understanding of the product features, functions, capacities, and limitations within the context of solutions and verified reference configurations.

Document changes since last issue

The following changes have been made to this document since the last issue:

- Added information about the new features of CMS R18 in the *New in this release* section.
- Updated the capacities table to include the capacity numbers for the new platforms of CMS R18.
- Added the following topics from the *Change Description* document of the previous release. The *Change Description* document has been discontinued and the extra information in the *Change Description* document has been merged with this document:
  - Supported CMS server releases
  - Supported CMS software
  - Non-supported software
  - Cross product interactions
  - Service packs and patches
- Added the following topics from the *Capacities* document of the previous release in order to merge the extra information from *Capacities* with this document as the *Capacities* document has been discontinued:

  - Using the capacity limits
  - Capacity Descriptions
  - Optimizing CMS reporting efficiency
- Updated the Product Compatibility table in the Interoperability section.
- Added a new subsection titled *CMS Agent Licensing Enforcement* in Chapter *Licensing Requirements.*

March 2016

- Added the new features of CMS R18.0.0.1.

July 2016

- Added support for the new HPE platform, DL20 G9.
- Added the latest versions of Tivoli and Netbackup being supported.
- Updated the table describing the upgrade paths.

June 2017

- Added support for Dual IP address.
- Updated the refresh rate for Real time to 3 seconds.

September 2017

- Updated Integrated refresh rates.

October 2017

- Removed section on Integrated refresh rates.

February 2018

- Added support for Vmware 6.5
- Added information about the new features of CMS R18 in the *New in this release* section.

Related resources

Documentation

You can download the document you need from the Avaya Support website at http://support.avaya.com.

The following table lists the documents pertaining to CMS:

Document title	Description	Audience
Administration		
Avaya CMS Administration	Provides instructions on administering a Contact Center using Avaya CMS Supervisor.	Avaya CMS administrators and Split/Skill supervisors with limited access to CMS
Avaya CMS Call History Interface	Describes the format of the Call History data files, and how to transfer these files to another computer.	Avaya support personnel and Contact Center administrators
Avaya CMS Security for Linux®	Describes how to implement security features in CMS.	Avaya support personnel, Avaya factory personnel, and Contact Center administrators
Avaya CMS Switch Connections, Administration, and Troubleshooting	Describes how to connect and administer Avaya communication servers or switches that are used with Avaya CMS.	Avaya support personnel and Contact Center administrators
Installation		
Avaya CMS SIMT for Linux	Describes how to install, configure, and maintain Avaya CMS.	Avaya support personnel, Avaya factory personnel, and Contact Center administrators
Application		
Avaya CMS Database Items and Calculations	Provides CMS users with the knowledge to understand, in detail, how CMS calculates the numbers displayed on CMS and Avaya CMS Supervisor reports within the CMS database.	CMS users who need to understand how CMS calculates numbers for reports
User Guides		
Avaya CMS Supervisor Reports	Describes the purpose and usage of CMS Supervisor reports.	Contact Center administrators and personnel responsible for determining the effectiveness of the contact center

Training

The following courses are available on www.avaya-learning.com. Enter the course code in the **Search** field and click **Go** to search for the course.

Course Code	Course Title
AVA00398WEN	Avaya Call Management System Administration
ATI00684VEN	Call Management System Installation & Maintenance
AVA00399WEN	Avaya Call Management System Report Fundamentals

Avaya Mentor videos

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

Visit http://www.youtube.com/AvayaMentor.

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

Support

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

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site:

http://www.avaya.com/support

For information about the standard Avaya warranty and support for Call Management System during the warranty period, see the Avaya Support website at http://support.avaya.com/ in **HELP & POLICIES** > **Policies & Legal** > **Maintenance and Warranty Information**.

See also **HELP & POLICIES** > **Policies & Legal** > **License Terms**.

Chapter 2: Overview

Avaya Call Management System (CMS) is a software product for businesses and organizations that receive a large volume of telephone calls processed through the Automatic Call Distribution (ACD) feature of the Avaya Aura® Communication Manager system. Avaya CMS collects call-traffic data, formats management reports, and provides an administrative interface to the ACD feature on the Communication Manager system.

Avaya CMS runs on the Red Hat Enterprise Linux® (RHEL) operating systems and uses several operating system utilities to communicate with terminals and printers, log errors, and execute processes. CMS utilizes the INFORMIX database management system, which provides an interface to the CMS historical database.

Avaya CMS stores ACD data in a real-time database as well as a historical database. Real-time databases include tables for the current intrahour interval data and the previous intrahour interval data. The storage interval can be 15, 30, or 60 minutes. Historical databases include tables for the intrahour, daily, weekly, and monthly data. The historical database can store 62 days of intrahour historical data, 5 years or 1825 days of daily historical data, and 10 years or 520 weeks of weekly and monthly historical data.

Avaya CMS provides two options for contact center data resiliency:

- High Availability CMS: For data redundancy with two systems operating in tandem.
- Survivable CMS: For business continuity in multilocation contact centers and continued operation in the event of a disaster at the controlling site.

Avaya CMS is a flexible and scalable software that is ideal for small single-location contact centers, large multilocation application, or contact centers of similar sizes. You can use Avaya CMS to analyze the performance of a single agent, a specific skill, a large number of agents or agent skills on up to eight ACD systems.

Avaya CMS includes the Avaya CMS Supervisor feature to monitor contact center performance and activity from a PC within your contact center, at home, or on the road. Using Avaya CMS Supervisor, managers can monitor, in real time, any area of contact center performance such as the number of abandoned calls, average hold time, and number of calls in a queue. Avaya CMS also includes the Avaya CMS Supervisor Web feature to monitor contact center performance and activity with a web browser.

Feature description

CMS offers the following salient features:

- CMS reporting
- CMS Supervisor PC client
- CMS Supervisor Web client
- CMS Mobile Supervisor
- ACD administration
- Backup support
- IPv6 support
- Dual IP address support

CMS reporting

CMS provides real-time, historical, and integrated reporting to track all activities in the contact center. Using CMS reports, you can make decisions regarding entities like agents, split/skills, vectors, vector directory numbers (VDN), and trunks.

CMS stores all the ACD data received from Communication Manager or the communication server in the real-time and historical databases. Real-time databases include tables for the current intrahour interval data and the previous intrahour interval data. The storage interval can be 15, 30, or 60 minutes. Historical databases include tables for the intrahour, daily, weekly, and monthly data.

CMS Supervisor PC client

The Avaya CMS Supervisor PC client software is a Windows-based interface to the Avaya CMS server. Using this interface, you can carry out nearly all the operations available from the CMS server interface, including:

- Remotely administering most aspects of the CMS server, such as defining Dictionary entries, setting user permissions, and adjusting data storage intervals and capacities.
- Running reports to view the activity in your call center.

CMS Supervisor Web client

You can use Avaya CMS Supervisor Web, or the CMS Web-based reporting tool, to access CMS reports from a wide range of hardware platforms. Avaya CMS Supervisor Web has a single point of installation which eliminates the need to install a client on multiple computers.

Avaya provides CMS Supervisor Web as an alternative to CMS Supervisor PC client so that customers can reduce the overheads associated with traditional CMS Supervisor PC client deployment.

CMS Mobile Supervisor

CMS Mobile Supervisor is an iPad application that the supervisors and operations managers of a contact center can use to monitor the agents and the health of the contact center when the supervisors and operations managers are away from their desks.

CMS Mobile Supervisor is a real-time reporting tool that displays specific real-time summary views of skills and agent activity with the capability to drill through to individual agent details.

ACD administration

CMS provides an administrative interface to the communication server. From the ACD interface, you can view or change parameters related to ACDs, call vectoring, and Expert Agent Selection (EAS) on the communication server. An administrator can also run reports that describe your contact center configuration.

For example, an administrator can:

- Add or remove agents from splits/skills.
- Move extensions between splits/skills.
- Change splits/skills assignments.
- Change trunk group-to-split.
- Change trunk group-to-VDN.
- Change VDN-to-vector assignments.
- Start an agent trace.
- List the agents being traced.
- Create, copy, and edit call vectors.

Backup support

CMS supports backup and restore to and from tape and Tivoli Storage Manager (TSM) LAN backup. CMS also supports backup, restoration, and migration to and from the following:

- Symantec Netbackup 7.5 Server, LAN backup
- Tivoli Storage Manager Server 6.3.3 and Tivoli Storage Manager Client 6.2.1, LAN backup
- USB storage device, nontape backup
- NFS mounted file system, nontape backup

IPv6 support

CMS supports IPv6 connectivity. The integration between CMS and Communication Manager over IPv6 is seamless. You can configure IPv6 Communication Manager or ACD sources by using the `cmsadm` command through the `acd_create` option in the same way as IPv4. This configuration requires the use of IPv6 addresses instead of IPv4 addresses. CMS Supervisor Web and CMS Mobile Supervisor can also use IPv6. CMS also integrates with Supervisor PC Client, Terminal Emulator, and Network Reporting over IPv6. No extra configuration is required to enable the IPv6 capabilities of CMS reporting client applications. IPv6 protocol and name resolution, and connectivity is automatic. Use of IPv6 is transparent to CMS users. All features of CMS work exactly the same with IPv6 as they do with IPv4.

New in this release

CMS R18 supported features

Tenancy: The tenancy feature provides an extension to the current CMS user data access management feature to enable customers to restrict user access to CMS reporting data and functionality within their contact center. The new tenant level access for users introduces restricted data access permissions for the following contact center resources: agents, agent groups, call work codes, split/skills, trunk groups, VDNs, and vectors.

Customers must install the tenancy feature package to use the CMS tenancy feature. Using this feature, customers can partition a subset of the ACD resources and assign the resources to tenants. A tenant or tenant partition enforces restricted access for CMS Supervisor users.

- Additional time zones: Administrators can administer additional time zones for daily, weekly, and monthly archiving. One additional time zone is allowed for an entire ACD and one additional time zone is allowed per tenant partition within the ACD. Time zone selection can be applied for interval, daily, weekly, and monthly reporting. By dividing an ACD into multiple tenant partitions using the multi-tenancy support in this release, customers can associate a specific time zone to a tenant partition instead of the entire ACD.
- Support of Integrated reports and Administration in CMS Supervisor Web: CMS Supervisor Web supports Integrated Reports and the following administrative operations:
  - Change agent skills
  - Multi-Agent skill change
- Support for CM 7.0: CMS supports new features in CM Release 7 resulting in the following changes:
  - 360,000 logged in agent/skill pairs
  - 24,000 measured trunks
  - 2000 location IDs
  - 999 trunks per trunk group
  - Agent attribute sent with login
  - A change in equipment location ID format to match virtual trunk locations
- Support for headless configuration: All new servers supported in this release are configured headless. The new servers are shipped and deployed without a keyboard, monitor, and mouse. All access to the CMS servers will be via remote terminal.

  Upgraded systems will have the option to retain the monitor, keyboard, and mouse if they require.
- Supporting software upgrade:
  - Informix: In order to support the new tenant data access controls, CMS uses Informix version 12 along with data compression. With compression, CMS consumes upto 40% less disk space for the same supported capacities.
  - RHEL 6.6: CMS runs on RHEL 6.6 to support the upgrades to next gen servers.
  - Java 8: CMS supports Java version 8 in this release.
- Supported hardware:
  - Dell R220, R630, and R730 running RHEL.
  - HPE DL380 G9 running RHEL.
  - HPE DL20 running RHEL

Note:
No new orders will be fulfilled for Oracle platforms.

- Supported server upgrades: This version supports upgrades on the Dell R620 and R720, Oracle T4 and X4270, and the HPE DL 380P Gen8 platforms.

Note:
No support of server upgrades for T5120 and T5220.

– Upgrade paths:

			R18 Supported platforms							
Existing platforms			**Oracle**		**Dell**			**HPE**		
Vendor	**Model**	**Release**	**T4**	**X4270**	**Dell R220[1]**	**Dell R620**	**Dell R720**	**DL 380P G8**	**Currently orderable platforms (see list below)**	**VM**
Oracle	**T4**	**R16.x, R17**	CUE[2]	NA	NA	NA	NA	NA	Platform Upgrade	Platform Upgrade
	X4270	**R16.x, R17**	NA	CUE[2]	NA	NA	NA	NA	Platform Upgrade	Platform Upgrade
	T5120	**R16.x, R17**	NA	NA	NA	NA	NA	NA	Platform Upgrade	Platform Upgrade
	T5220	**R16.x, R17**	NA	NA	NA	NA	NA	NA	Platform Upgrade	Platform Upgrade
Dell	**R620**	**R17**	NA	NA	NA	CUE	NA	NA	Platform Upgrade	Platform Upgrade
	R720	**R17**	NA	NA	NA	NA	CUE	NA	Platform Upgrade	Platform Upgrade
HPE	**DL 380P G8**	**R17**	NA	NA	NA	NA	NA	CUE	Platform Upgrade	Platform Upgrade
NA	**VM**	**R17**	NA	NA	NA	NA	NA	NA	Platform Upgrade	CUE

1. The Dell R220 server is a supported platform in R18 but is not available for new sales after July 11, 2016. Though supported in R18, R220 does not have any upgrade paths from the other existing R18 platforms. The EOS link for R220 is https://downloads.avaya.com/css/P8/documents/101020897.
2. CUE is not available for the T4 and X4270 platforms after June 13, 2016. The EOS link for CUE disks is https://downloads.avaya.com/css/P8/documents/101020899.

Currently orderable R18 platforms available for new sales or platform upgrade

- HPE DL20

- HPE DL380 G9
- Dell R630
- Dell R730
- VM (R18)

CMS R18.0.0.1 supported features

- New hardware
  - HPE DL380 G9 server from Hewlett-Packard Enterprise (HPE) running RHEL.
- Added support for R18 CMS and CMS tenant feature.

CMS R18.0.0.2 supported features

- New hardware
  - HPE DL20 server from Hewlett-Packard Enterprise (HPE) running RHEL.

Note:
No new orders will be fulfilled for the Dell R220 server.

- The supported client versions of NetBackup & Tivoli client are as follows:
  - IBM Spectrum Protect (ISP) 7.1.3

Note:
IBM Spectrum Protect (ISP) was previously named Tivoli Storage Manager.

  - Netbackup 7.7.2

CMS R18.0.1 supported features

- Dual IP address.
  - Dual IP was designed and is supported specifically to enhance the CMS HA and Dual Role offers.

CMS R18.0.2 supported features

- VMware 6.5
  - Added support for VMware 6.5
- FIPS 140-2 encryption
  - FIPS 140-2 encryption is used to enhance the CMS security.
- Firewall
  - Linux iptables are used to enforce firewall protection for CMS.

- Support for Veritas Netbackup 7.7.3 and IBM Spectrum Protect 7.1.4 (Note that IBM Spectrum Storage Protect was formerly known as Tivoli Storage Manager).

Chapter 3: Interoperability

Product compatibility

The following table lists the different releases of CMS software that are compatible with the following communication server software releases:

Communication server software release	CMS software release			
	R15	R16.x	R17	R18
Communication Manager 2.x	Yes	Yes	Yes	No
Communication Manager 3.x	Yes	Yes	Yes	No
Communication Manager 4/ 5	Yes	Yes	Yes	No
Communication Manager 5.2	Yes	Yes	Yes	Yes
Communication Manager 6.x	Yes	Yes	Yes	Yes
Communication Manager 7.x	Yes	Yes	Yes	Yes

Supported CMS server releases

CMS R18 Supervisor supports connections to the following CMS server versions:

- R15
- R16.x
- R17
- R18

Supported CMS software

Avaya CMS R18 uses the following software packages:

- RHEL 6.6
- Informix IDS
- Informix ESQL SDK

- Informix ILS
- Avaya CMS Supplemental Services
- Avaya Call Management System
- ODBC and JDBC

Note:
For specific software version information, see the *CMS Software Installation, Maintenance and Troubleshooting for Linux*® documents for this release.

Non-supported software

CMS Supervisor, Network Reporting, or Terminal Emulator does not support the following software and OSs:

- Windows 10 S
- Windows RT
- Windows Vista
- Windows XP and older
- Windows Server 2003 and older

Third-party product requirements

The following table lists some of the third-party products that the customer provides:

Third-party Product	Description	Connectivity
SAS LTO-5 tape drive (hardware)	This tape drive is attached to T4-1 SPARC systems for providing tape backups for CMS data.	The tape drive connects to the CMS server using the external SAS HBA card. CMS software seamlessly integrates with this tape drive for backing up CMS and system data using the tape option for backups.
SAS LTO-4 tape drive (hardware)	This tape drive is attached to the Netra X4270 systems for providing tape backups for CMS data.	The tape drive connects to the CMS server using the external SAS HBA card. CMS software seamlessly integrates with this tape drive for backing up CMS and system data using the tape option for backups.
US Robotics Faxmodem Comsphere 3910 (hardware)	Using this modem, personnel at a remote support center can dial in to a Netra X4270 CMS server and do maintenance.	The modem connects to the CMS server using the remote console port and provides console access to a remote computer.

Cross-products interactions

CMS R18 supports and can connect to the following Avaya products:

NICE Analyzer

NICE Analyzer was discontinued in late 2007. Therefore, any current use of NICE Analyzer is considered Permissive Use by Avaya. For more information on Permissive Use, see " CMS permissive use support policy" in *CMS Security.*

Operational Analyst

A future release of OA will be provided to operate fully with CMS R18.

Avaya IQ

CMS R18 continues to support parallel implementations with Avaya IQ, when CMS and Avaya IQ are connected to the same Communication Manager.

Operating system compatibility

CMS server software runs on Red Hat Enterprise Linux® (RHEL) 6.6.

Operating system compatibility for CMS Supervisor Web client

CMS Supervisor Web client is supported on the following browsers and OS combinations:

- Microsoft Internet Explorer
  - Windows 7: version 10, 11
  - Windows 8.1: version 11
  - Windows 10: version 11
- Microsoft Edge
  - Windows 10: version 38, 39
- Mozilla Firefox
  - Windows 7: version 52, 53
  - Windows 8.1: version 52, 53
  - Windows 10: version 52, 53
  - OS X 10.11 (El Capitan): version 52, 53
  - OS X 10.12 (Sierra): version 52, 53
- Google Chrome
  - Windows 7: version 57, 58
  - Windows 8.1: version 52, 53
  - Windows 10: version 57, 58
  - OS X 10.11 (El Capitan): version 57, 58
  - OS X 10.12 (Sierra): version 57, 58
  - ChromeOS: version 57, 58
- Apple Safari

- OS X 10.11 (El Capitan): version 9, 10
- OS X 10.12 (Sierra): version 10

Note:
Running reports in CMS Supervisor Web requires Adobe Flash support.

Operating system compatibility for CMS Supervisor PC client

CMS Supervisor PC client is supported on the following OS combinations:

- Windows 7
- Windows 8.x
- Windows 10
- Citrix XenApp 6.5 Enterprise on Windows 2008 R2 Enterprise 64-bit SP1
- Citrix XenApp 6.5 Enterprise on Windows 2008 R2 Enterprise 64-bit
- Citrix XenApp 6.0 Enterprise on Windows 2008 R2 Enterprise 64-bit SP1
- Citrix XenApp 6.0 Enterprise on Windows 2008 R2 Enterprise 64-bit

Service packs and patches

To ensure compatibility and security, you must install the latest service packs and security patches for your supported Microsoft operating system prior to installing Avaya CMS R18 Supervisor and Network Reporting.

Chapter 4: Performance specifications

Using the capacity limits

The capacities described in the following topics are the maximum limits that can be supported by a particular CMS hardware platform. You must verify that *none* of the capacity limits is exceeded for a particular hardware platform.

If you exceed even one of the capacity limits for a given hardware platform, you require the next higher capacity hardware platform. For example, if you have less than 200,000 calls per hour, but between 201 and 400 Supervisors, you must purchase a Dell R730 server.

Capacity Descriptions

The following topics describe the measurement you must use to determine which CMS hardware platform is required.

Peak Busy Hour call volume

The busy hour call volume capacity is the call volume during the busiest hour of the day.

Calculate the busy hour call volume by adding each trunk seizure or line appearence seized during the busiest hour for all calls.

Concurrent supervisors

The concurrent supervisors capacity is the total maximum number of CMS supervisors and CMS terminal emulator logins that exist during the peak busy hour. The concurrent supervisors capacity is not the number of authorized logins, but the number of logins actually used.

Note:
This capacity limit is the sum of the login count from each client type: CMS Supervisor PC client, CMS Supervisor Web client and CMS Supervisor Mobile Client, Terminal Emulator, and Network Reporting.

Calculate the number of concurrent supervisors by counting the maximum number of supervisor logins and the terminal emulator logins that exist during the busy hour period. Each login counts as one. Do not count the number of reports. This count must be 1600 or less.

Third-party software

The third-party software capacity is the number of external or third party interface applications. Some examples of third-party interfaces are Blue Pumpkin, ODBC, wallboards, Geotel, Operational Analyst, TCS, and IEX.

Calculate the amount of third-party software by counting the number of third party applications used.

Important:
The one exception to this rule is Geotel, which counts as two applications.

Do not count each instance of the application. If you use wallboards, count the wallboards as one application. Do not add up the total number of wallboards.

Agent/skill pairs

The agent/skill pairs capacity is the total number of agent/skill pairs.

Calculate this capacity by multiplying the number of agents by the number of skills each agent can log in to. The number of agents and the number of skills are based on the switch administration. For example, if there are 20 agents, and each agent is administered with 5 skills, you would multiply agents by their skills for a value of 100 agent/skill pairs. You must count the total number of skills administered for the agent, not the number of skills used by the agent.

Reports per Supervisor session

The reports per Supervisor session capacity is the average number of simultaneous real-time reports each supervisor will run.

Report elements

The report elements capacity is the average number of report elements.

A report element is an entity that is monitored by an average real-time report. Report elements are not the lines of data rendered on the report but the element that is chosen to run the report against. Some examples of elements are VDNs, skills, and vectors.

Calculate this capacity by counting each element. You would count one element if a report is run for one skill. It does not matter if the report has lines of data for each agent in the skill.

Active agent traces

The active agent traces capacity is the number of agent traces running on the CMS.

Integrated Report refresh rate

CMS PC Supervisor refresh rate for Integrated reports is a minimum of 10 seconds. CMS Supervisor Web allows a 3 second refresh rate for Integrated Reports.

Average refresh rate

The average refresh rate capacity is the average refresh rate for real-time reports.

Calculate this capacity by averaging the refresh rates set by your report users. For example, if one-half of the users use a 30-second refresh rate, and the other half use a 10-second refresh rate, you would calculate an average of 20.

Percent refresh rate at three seconds

The percent refresh rate at 3 seconds capacity is the percentage of real-time report users that require a refresh rate of 3 seconds.

Capacity and scalability specifications

Important:
When the FIPS 140-2 encryption feature is activated, the following capacities are reduced by 10% for all models of CMS:

- Concurrent Supervisors
- Reports per Supervisor Session
- Report elements
- 30 Second Average Refresh Rate (including a 10% reduction in the listed 3 second refresh rate capacities)

FIPS 140-2 encryption consumes additional CPU and memory to support the more complex ciphers required by FIPS 140-2 guidelines. CMS applies the encryption for server/client connections where the client is CMS Supervisor PC, or CMS Supervisor Web. Hence, the capacities for CMS between the CMS Server and all client applications is reduced by 10%.

The following tables list the capacities for each hardware platform being sold for new CMS R18 installations or for existing platforms being upgraded to CMS R18. Only Dell R620, Dell R720, HPE DL380P G8, and Netra X4270 systems can be upgraded to CMS R18.

New shipments

Capacity	R18 Low End Hardware Platform (HPE DL20 and Dell R220[1])	R18 Midsize Hardware Platform (Dell R630)	R18 High End Hardware Platform (Dell R730)	R18 High End Hardware Platform (HPE DL380 G9)
Memory	16GB	32GB	64GB	64GB
Peak busy-hour call volume	10,000	200,000	400,000	400,000
Concurrent supervisors[2]	30	200	1,600	1,600
Concurrent Agents	400	5,000	10,000	10,000
Third-party software	3	3	7	7
Agent skill pairs	100,000	200,000	800,000	800,000
Reports per Supervisor session	5	5	10	10
Report elements	5	5	12	12
Active agent traces	200	1,000	5,000	5,000
30 seconds Average refresh rate	10% at 3 seconds	50% at 3 seconds	100% at 3 seconds	100% at 3 seconds
Internal Call History (ICH) records	4,000 per 20 mins	4,000 per 20 mins	4,000 per 20 mins	4,000 per 20 mins
External Call History (ECH) records	300,000 per 20 mins	300,000 per 20 mins	300,000 per 20 mins	300,000 per 20 mins

1. The Dell R220 server is a supported platform in R18 but is not available for new sales after July 11, 2016. Though supported in R18, R220 does not have any upgrade paths from the other existing R18 platforms. The EOS link for R220 is https://downloads.avaya.com/css/P8/documents/101020897.
2. The total capacity of concurrent CMS Supervisors is the combined capacity of CMS Supervisor PC clients, CMS Supervisor Web clients, and CMS Supervisor Mobile clients.

The Dell R720 and Dell R730 introduces new CMS system wide capacities. The new CMS system wide capacities come with restrictions, so review Maximum values with multiple ACD deployment for specific restrictions when using the higher system wide capacities.

Note:
All the per ACD capacities remain unchanged.

New system wide capacities

CMS attribute	System wide capacity	Per ACD capacity (Maximum capacities when CMS R18 is connected to a CM 7.0)
Agent skill pair	800,000	360,000
Total VDNs	54,000	30,000
Total splits or skills	54,000	8,000
Total trunks	80,000	24,000
Total trunk groups	8,000	2,000
Total vectors	32,000	8,000
Total call work codes	4,000	1,999
Agent trace records (AAR)	5,100,000	5,100,000

The following table represents the maximum values with multiple ACD deployment on a Dell R720 system supporting 800,000 agent skill pairs:

Maximum values with multiple ACD deployment

Basic Maximum Values (supported on Dell 720 or Dell 730 only)					
Agent/skill pairs	300,000	300,000	400,000	500,000	800,000
Interval length (minutes)	30	15	30	30	30
Interval data days saved	31	31	15	31	15
Daily data days saved	1,825	730	1,825	730	730

Note:

There is no impact on daily, weekly, and monthly limits. When the capacity limit of agent skill pairs crosses 200,000, there is an impact on the interval data storage.

Capacity	Dell R620 low	Dell R620 mid	Dell R720	HPE DL380P G8	Netra X4270	SPARC T4-1	
Memory	8GB	16GB	64GB	64GB	4 GB	32GB	64GB
Peak busy-hour call volume	10,000	200,000	400,000	400,000	200,000	400,000	400,000
Concurrent supervisors[1]	30	200	1,600	1,600	200	800	1,600
Concurrent Agents	400	5,000	10,000	10,000	5,000	10,000	
Third-party software	3	3	7	7	3	7	7
Agent skill pairs	100,000	200,000	800,000	200,000	200,000	200,000	
Reports per Supervisor session	5	5	10	10	5	10	10
Report elements	5	5	12	12	5	12	12
Active agent traces	200	1,000	5,000	5,000	200	2,000	5,000
30 seconds Average refresh rate	10% at 3 seconds	50% at 3 seconds	100% at 3 seconds	100% at 3 seconds	10% at 3 seconds	100% at 3 seconds	100% at 3 seconds
Internal Call History (ICH) records	4,000 per 20 minutes	4,000 per 20 minutes	4,000 per 20 minutes	4,000 per 20 minutes	4,000 per 20 minutes	4,000 per 20 mins	
External Call History (ECH) records	300,000 per 20 minutes	300,000 per 20 minutes	300,000 per 20 minutes	300,000 per 20 minutes	300,000 per 20 minutes	300,000 per 20 mins	

1. The total capacity of concurrent CMS Supervisors is the combined capacity of CMS Supervisor PC clients and CMS Supervisor Web clients.

Capacities in a VMWare configuration

Parameter	Small VMware configuration No equivalent real hardware machine	Medium VMware configuration — equivalent to mid-sized Linux system	Large VMware configuration — equivalent to high-end Dell 730 platform with Linux
Peak busy-hour call volume	30,000	200,000	400,000
Concurrent supervisor sessions[1]	50	200	1,600[2]
Concurrent Agents	500	5,000	10,000
Third-party software	3	3	7
Agent skill pairs[3]	100,000	200,000	800,000[3]
Reports per Supervisor session	3	5	10
Report elements	5	5	12
Percentage of supervisors that can run reports with a 3 second refresh rate	0%	50%	100%
Active agent traces	250	1,000	5,000
Internal Call History (ICH) records	4,000 per 20 mins	4,000 per 20 mins	4,000 per 20 mins
External Call History (ECH) records	10,000 per 20 mins	60,000 per 20 mins	300,000 per 20 mins

1. This value is the total number of active CMS Supervisor PC client and CMS Supervisor Web client sessions.
2. Of the 1,600 sessions supported, only 800 can be CMS Supervisor Web client sessions.
3. Supporting 800,000 agent skill pairs requires greatly increased disk space for interval data. Customers should create up to 8 additional disk volumes. See *Deploying Avaya Call Management System in an Avaya Customer Experience Virtualized Environment* for full details on disk space usage recommendations.

Optimizing CMS reporting efficiency

Avaya provides a powerful solution with CMS that enables you to create custom reports designed to fit your individual needs. However, the overall capability of the CMS server is limited by the memory and CPU of each server.

Skill based reporting

The CMS server is optimized for skill based reporting. Avaya recommends that you create and use reports on skills instead of Agent Group reports. Skills that do not receive actual calls can be created on the Communication Manager. You can use these skills to provide reporting for the agents that are placed in that skill.

To use Agent Group reports, follow the recommendations provided in Recommendations for custom reports on page 34.

Recommendations for custom reports

When you design and use custom Agent Group reports, consider the following recommendations to optimize system performance:

- Agent Groups
  - The size of agent groups are recommended to be 99 agents or less. Agent groups of size 99 agents or less are recommended because system performance can be adversely affected.

  Note:
  The agent group capacity of 99 agents or less is only available on Dell R730, Dell R720, VMware large configuration, HPE DL380 G9, and Oracle T4.

  - If possible, report on consecutive Agent IDs in the same report
  - If possible, limit Agent Group reports and use skill based reports
- Number of agents or other elements in historical or real time reports
  - Carefully examine the number of agents, skills, VDNs, trunks, or other elements in one report. Limit the number of agents or other elements in a single report as much as possible.
- Custom report design

- In historical reports, there should be no input for multiple dates when running against the interval database tables. Existing reports that allow multiple dates should be modified to gain access to the appropriate daily/weekly/monthly table instead of the interval table.
- Any historical report that takes longer than a few seconds to complete should be reviewed for modification to improve performance.

Any real-time report that takes more than a few milliseconds to refresh should be reviewed or modified to improve performance.

Resources for system performance analysis

Customers can work with Avaya Professional Services to design and use custom reports in a manner that maximizes system performance. The Avaya Professional Services organization provides services that include a performance analysis of custom reports on a CMS system. Avaya Professional Services can also provide recommendations on how to efficiently design current or future reports in a manner that minimizes impact to CMS performance.

Changing the dictionary

Changes to the dictionary must occur during off hours when database updates are minimum. Otherwise, CMS Supervisor users will need to constantly query the database to update the cache on the computer where CMS Supervisor is running. This causes the real-time reports to hang, and users are denied access to CMS Supervisor.

Traffic specifications

See the entry for *Peak busy-hour call volume* in the *New ships* and *Upgrades* tables in Capacity and scalability specifications on page 29.

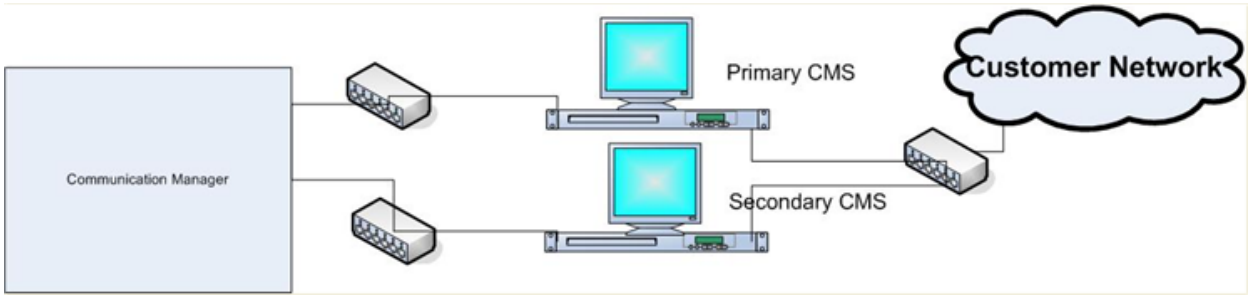
Redundancy and high availability

The primary purpose of the Avaya CMS High Availability (HA) option is to ensure an uninterrupted data stream between the communication server or switch and the CMS server. With HA, two CMS servers are connected to one communication server or switch. This connection eliminates the traditional single point of failure between the CMS server and the communication server or switch.

Both CMS servers collect data independently from the communication server. Both CMS servers provide full CMS capabilities. If either server fails, loses connection to the communication server, or must be brought down for maintenance, the alternate server can carry the entire CMS activity load.

Duplicate hardware is a key component of the CMS HA system. The function of the duplicate hardware is to eliminate a single point of failure in order to prevent data loss due to hardware failures. The dual ACD link feature addresses ACD link failures, and the alternative ACD link provides increased ACD link reliability. A C-LAN circuit pack or an ethernet port provides TCP/IP connectivity between the communication server and the CMS server. Each ACD link requires a separate C-LAN circuit pack or ethernet port that supports different network routes to eliminate as many single points of failure as possible.

The following figure displays a typical CMS HA configuration with a primary or active server and a secondary or standby server:



Dial plan specification

CMS R18 and later supports up to 16 digit extensions for agent, login id, VDN, and station. CM 7.1 is the release scheduled to have the matching 16 digit capability.

Chapter 5: Security

Note:
For detailed information on CMS Security, refer to *Avaya CMS Security for Linux* on the support site.

Security specifications

CMS provides the following security features for secure operation:

- Operating system hardening

  CMS achieves operating system hardening by the following procedures:

  – *Patching and patch qualification*: CMS includes all necessary components including security patches at the time of release. Avaya receives additional patch notifications and certifies new Linux® OS patches. Avaya then assembles these patch clusters and makes the clusters available to customers through Product Change Notices (PCN).

  – *Operating System-level security logs and audit trails*: You can use log files to detect suspicious system activity. The customer can review these log files on a routine basis for signs of unusual activities. For more information, see *CMS Security*.

  – *Banner modifications*: Altering the telnet and ftp network service banners hides operating system information from individuals who want to take advantage of known operating system security holes.

  – *Email and SMTP*: You must not configure CMS as a mail relay and must disable the Simple Mail Transfer Protocol (SMTP) daemon.

  Note:
  For details on FIPS 140-2 encryption, refer to *CMS Software Installation, Maintenance and Troubleshooting for Linux*® document and Release notes.

- Authentication and session encryption

  CMS achieves authentication and session encryption by the following procedures:

  – *User authentication and authorization*: CMS uses login and password security measures provided by the Linux® OS and provides multiple levels of system access. To authenticate users, CMS uses OS capabilities based on Pluggable Authentication Modules (PAM). At the system level, CMS uses the standard UNIX permissions. In CMS, you can administer data permissions for each user.

  - *Password complexity and expiration*: You can enable and modify the password expiration attributes through the CMSADM menu. You can set the expiration intervals from 1 to 52 weeks.
  - *Logging for failed logins*: You can log the failed login attempts in the system message log, `syslog`.
  - *Multiple login prevention*: With the APS hardening offer, you cannot log in more than once concurrently.
  - *Use of ssh*: CMS provides a simplified installation of secure Supervisor client login over a public or unsecured network. To do this installation, CMS uses Secure Shell (SSH), a protocol that encrypts the packets sent between a client workstation and a host server. This procedure secures the transmission of login information and other sensitive data.

- Application security

  CMS achieves application security by SPI link, application-level audit logging, and database security controls.

- Physical security

  CMS achieves physical security by physical server protection and EEPROM/BIOS security.

- Services security and CMS support

  CMS achieves services security and CMS support by remote connectivity and authentication, and services password management.

Setting up the Secure Access Link (SAL) and Alarm Monitoring system

The Avaya default remote access is secure access link (SAL) which allows Avaya personnel to:

- Resolve product issues
- Optimize the performance
- Value the Avaya customer support entitlements

Use the following steps to create a new registration or to onboard a technical personnel:

1. Go to https://support.avaya.com.
2. Login in with the user name and password.
3. On the home page, click **Diagnostics & Tools** and select **Global Registration Tool**.
4. On the **Create A New Registatrion** page, perform one of the following steps:
   - Select **End to End Registration**.

- Select **Technical Onboarding Only**.

5. Enter a the 10-digit functional location number that is sold to the customer.

   Ensure that you include leading zeroes when entering the location number. For instance, if the location number is 12345678, you must add two leading zeroes before 12345678. For example, type 0012345678.

Note:
If the customer has completed the product registration process, then complete only the Technical Onboarding process to allow the SAL connectivity.

To complete the product registration process and prepare the technical onbording, including the SAL Connectivity process, you must understand which product material code is eligible for Technical Onboarding during the product registration process.The GRT Tool Mapping table provides the list of product material codes for your reference.

You can download the GRT Tool Mapping table from the Avaya support site at: https://support.avaya.com/css/P8/documents/100176973.

Note:
Save the Microsoft Excel spreadsheet in your computer.

Port utilization

Call Management System R18 Port Matrix lists all the ports and protocols that CMS uses. Avaya Direct, Business Partners, and customers can find the port matrix document at http://support.avaya.com/security. On the Web page, select the **Avaya Product Port Matrix Documents** link, and click the Port Matrix document for CMS. You can gain access to the port matrix document only after you log in to the Avaya Support site using the valid support site credentials.

Chapter 6: Licensing requirements

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

CMS Agent Licensing Enforcement

Avaya policy is that the number of CMS simultaneous Agent licenses (or Right To Use (RTU)) must be equivalent to or greater than the number of Agent licenses in Communication Manager for simultaneously logged in measured ACD agents.

The ACD agent count is cumulative across all the ACDs monitored by CMS. For example, if CMS is reporting on two ACDs with 400 simultaneously logged in measured ACD agents each, CMS must be licensed for 800 simultaneous agents.

The Agent licenses on CMS are based on the number of simultaneously logged in Agents, not the number of administered Agents. Avaya CMS is capable of reporting on all of the Logged In or Staffed Call Center Agents of any Avaya Communications Manager system which CMS is monitoring. For example, consider that Agent Angela leaves the company. CMS continues to report on Angela and her formerly assigned Agent Login ID even though Angela is an inactive agent on Communication Manager. In this example, Agent Angela does not count as a simultaneously logged in Agent.

While Avaya has no plans to change this policy at this time, Avaya reserves the right to amend or change this policy at its sole discretion.

Third-party components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those product that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/ThirdPartyLicense/

You agree to the Third Party Terms for any such Third Party Components.

Glossary

Automatic Call Distribution (ACD)	1) A switch feature that channels high-volume incoming and outgoing call traffic to agent groups identified by splits or skills. 2) An agent state in which the extension is engaged in an ACD call.
Automatic Number Identification (ANI)	An industry term for notification of the calling party number (CPN). When the calling party is connected through a switch, the CPN can be either a billing number for the switch or the station identification (SID) number.
AUX	An agent state in which the agent is doing non-ACD work, is on a break, or is in a meeting. Agents enter AUX work by pressing the AUX WORK button or dialing the access code from their voice terminal. Agents can also enter AUX work by disconnecting to make or answer an extension call while in AVAIL mode or with a call on hold.
backup	The process of protecting data by writing the contents of the disk to an archive, such as a tape device, that can be removed from the computer environment and stored safely.
Call Prompting	A switch feature that routes incoming calls based on information supplied by the caller such as an account number. The caller hears an announcement, and the system prompts the user to select from the options listed in the announcement.
Call Vectoring	A switch feature that provides a highly flexible method for processing ACD calls using VDNs and vectors as processing points between trunk groups and splits. Using Call Vectoring, the system can route calls independent of splits.
Call Work Code (CWC)	An ACD capability using which the agent can enter a string of digits during or after the call and send the digits to *CMS* for management reporting.
dequeued and abandoned (DABN)	A trunk state in which the trunk quickly becomes idle after the caller abandons the call.
Dictionary	A CMS capability used to assign easily interpreted names to contact center entities such as login IDs, splits/skills, trunk groups, VDNs, and vectors.
direct agent ACD (DACD)	An agent state in which the agent is on a direct agent ACD call.
direct agent ACW (DACW)	An agent state in which the agent is in the after call work (ACW) state for a direct agent ACD call.
direct inward dialing (DID)	The use of an incoming trunk to dial directly from a public network to a communications system without help from an attendant.
entity	A generic term for an agent, split/skill, trunk, trunk group, VDN, or vector.

expected wait time (EWT)	An estimate of how long a caller has to wait to be served by a contact center while in a queue. EWT is based on current and past traffic, handling time, and staffing conditions. EWT does not include time spent in vector processing before being placed in a queue and time spent ringing an agent with manual answering. This calculation is a switch-based calculation.
Expert Agent Selection (EAS)	An optional Communication Manager feature that routes incoming calls to an agent who is a member of the specific skill required to handle the problems of the caller.
forced busy (FBUSY)	A trunk state in which the caller receives a forced busy signal.
forced disconnect (FDISC)	A trunk state in which the caller receives a forced disconnect.
Look Ahead Interflow (LAI)	A switch feature that can be used to balance the call load among multiple contact centers. LAI works with Call Vectoring and ISDN Primary Rate Interface (PRI) trunks to intelligently route calls between contact centers. Using this feature, multiple contact centers can share workloads and expand hours of coverage, and contact centers can transparently handle calls in different time zones.
maintenance busy (MBUSY)	A trunk state in which the trunk is out of service for maintenance purposes.
Outbound Call Management (OCM)	A set of switch and adjunct features using Adjunct/Switch Applications Interface (ASAI) that distributes outbound calls initiated by an adjunct to internal extensions, which are usually ACD agents.
skill	An attribute that is associated with an ACD agent and that qualifies the agent to handle calls requiring the attribute. An agent can be assigned up to 60 skills. For example, the ability to speak a particular language or the expertise to handle a certain product.
split	A group of extensions that receive calls.
switch	A system providing voice or voice and data communication services for a group of terminals.
trunk	A telephone circuit that carries calls between two switches, between a central office and a switch, or between a central office and a telephone.
trunk group	A group of trunks that are assigned the same dialing digits, either a phone number or a direct inward dialed (DID) prefix.
vector	A list of steps that process calls according to a user definition. The steps in a vector can send calls to splits, play announcements and music, disconnect calls, give calls a busy signal, or route calls to other destinations based on specific criteria.

Vector Directory Number (VDN)	An extension number that enables calls to connect to a vector for processing. A VDN can connect calls to a vector when the calls arrive over an assigned automatic-in trunk group or when the calls arrive over a DID trunk group and the final digits match the VDN. The VDN by itself can be dialed to access the vector from any extension connected to the switch.

Index