



Avaya Call Management System Overview and Specification

Release 21.0
Issue 1
June 2024

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided 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](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 Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, 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. Unless otherwise stated, 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

The following applies only 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](http://www.mpegla.com).

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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 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](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply 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, please contact your Avaya Sales Representative.

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 LLC.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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	7
Purpose.....	7
Change history.....	7
Chapter 2: CMS overview	8
New in this release.....	9
CMS feature summary.....	9
ACD administration.....	10
Reporting.....	10
ACD integration.....	10
CMS tenancy.....	11
LDAP integration.....	12
Data backup.....	13
CMS Supervisor.....	13
Avaya Solutions Platform.....	13
Networking with IPv4 or IPv6.....	13
WebLM and PLDS.....	14
Local and enterprise login options.....	14
Simplified CMS HA configuration.....	15
Chapter 3: Interoperability	16
CMS product compatibility.....	16
Operating system compatibility for the CMS server.....	17
Operating system support by browser type for the CMS Supervisor Web Client.....	17
Windows compatibility for the CMS Supervisor PC Client.....	17
Windows service packs and patches.....	18
Supported upgrade scenarios.....	18
Chapter 4: Performance specifications	19
Capacity limits.....	19
Capacity descriptions.....	19
Peak Busy Hour call volume.....	19
Concurrent supervisors.....	19
Third-party software.....	20
Agent/skill pairs.....	20
Reports per Supervisor session.....	20
Report elements.....	20
Active agent traces.....	21
Integrated Report refresh rate.....	21
Average refresh rate.....	21
Percent refresh rate at three seconds.....	21
Capacity and scalability specifications.....	21

CMS reporting efficiency.....	23
Skill based reporting.....	23
Recommendations for report customization.....	24
Resources for system performance analysis.....	24
Changing the dictionary.....	24
Traffic specifications.....	24
Redundancy and high availability.....	25
Dial plan specification.....	25
Chapter 5: Security	26
Security specifications.....	26
General Data Protection Regulation support.....	28
Certificates for secure communication.....	28
Web Client encryption.....	28
EASG.....	29
LDAP connection encryption.....	29
ODBC and JDBC network connections.....	29
SPI link.....	30
Setting up the Secure Access Link (SAL) and Alarm Monitoring system.....	30
Port utilization.....	31
Chapter 6: Licensing requirements	32
CMS agent licensing enforcement.....	32
Licensing overview.....	32
Licensed features in CMS.....	33
CMS license modes.....	33
License management.....	34
License enforcement	35
License log file.....	39
Alarms.....	39
Backing up and restoring WebLM.....	40
Chapter 7: Resources	41
Documentation.....	41
Finding documents on the Avaya Support website.....	43
Accessing the port matrix document.....	43
Avaya Documentation Center navigation.....	44
Viewing Avaya Mentor videos.....	45
Support.....	46
Using the Avaya InSite Knowledge Base.....	46
Upgrade Advantage Preferred.....	47
Glossary	48
Call Prompting.....	48
Call Work Code (CWC).....	48
dequeued and abandoned (DABN).....	48
Dictionary.....	49

direct agent ACD (DACD).....	49
direct agent ACW (DACW).....	49
direct inward dialing (DID).....	49
entity.....	49
forced busy (FBUSY).....	50
forced disconnect (FDISC).....	50
maintenance busy (MBUSY).....	50
Outbound Call Management (OCM).....	50
skill.....	51
switch.....	51
trunk.....	51
trunk group.....	51

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.

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 will find the document useful.

Change history

The following table summarizes the changes in this document for Release 21.x:

Issue	Date	Summary of changes
1	June 2024	<ul style="list-style-type: none">• Updated New in this release on page 9.• Revised the feature information under CMS feature summary on page 9 and added new information.• Updated interoperability information.• Updated Supported upgrade scenarios on page 18 with various edits and added information for this release.• Removed the capacity specifications for hardware-only deployments and other minor edits in Capacity and scalability specifications on page 21.• Updated Security specifications on page 26 with layout and rephrasing changes for clarity.• Added information about certificates under Certificates for secure communication on page 28.

Chapter 2: CMS overview

Avaya Call Management System (CMS) is a software product for businesses and organizations that receive a large volume of contacts processed through the Automatic Call Distribution (ACD) systems. Avaya Call Management System supports the following ACDs:

- Avaya Aura[®] Communication Manager
- Avaya Contact Center – Extended Capacity Routing Core

CMS collects call traffic data, formats management reports, and supports an administrative interface to the supported ACDs.

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

CMS stores ACD data in a real-time and historical database. Real-time databases include tables for the current and previous intra-hour interval data. The storage interval can be 15, 30, or 60 minutes. Historical databases include intrahour, daily, weekly, and monthly data tables. The historical database can store 370 days of intrahour historical data, five years or 1825 days of daily historical data, and ten years or 520 weeks of weekly and 120 months of monthly historical data.

CMS provides the following 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 multi-location contact centers and continued operation at the controlling site during a disaster.

This flexible and scalable software is ideal for small single-location contact centers, large multi-location applications, or contact centers of similar sizes. For example, you can use CMS to analyze the performance of a single agent, a specific skill, or multiple agents or agent skills on up to eight ACD systems.

CMS includes the Avaya CMS Supervisor (CMS Supervisor) feature to monitor contact center performance and activity from a PC within your contact center, at home, or on the road. Managers can use CMS Supervisor to monitor any area of contact center performance in real-time, such as the number of abandoned calls, average hold time, and number of calls in a queue. CMS also includes the CMS Supervisor Web feature to monitor contact center performance and activity with a web browser. In addition, the CMS Supervisor PC Client and Web Client support interfaces in several languages.

New in this release

The following is a summary of new content for CMS Release 21.0:

Report scheduling

You can schedule a report on the CMS Web Client. The available scheduling options are once, daily, weekly, or monthly. After setting up scheduling, use the Scheduler tab to view and manage your scheduled reports.

Automated CMS HA configuration

Use the new High Availability (HA) configuration process if two CMS servers are installed. After logging in to the CMS server console as root, enter the `cmsadm` command to access the HA configuration option. You can use this HA configuration process to set up the primary and secondary server roles. You can also reverse the roles.

Informix database upgrade

In previous releases, CMS used IBM Informix 12.10. It now uses HCL Informix 14.10.

Upgrades to Release 21

Perform a full software or platform upgrade from Release 20.0 or an earlier release to Release 21.0. You can upgrade directly to Release 21.0 from Release 16.x and later.

Discontinued hardware-only platforms

CMS no longer supports hardware-only installations and upgrades. The following hardware-only platforms are no longer supported:

- Dell 630 and 730
- HPE DL380 G9

Data backup

The following backup products are no longer supported:

- IBM Spectrum Protect (formerly Tivoli Storage Manager)
- Veritas NetBackup (formerly Symantec NetBackup)

Communication Manager interoperability

Communication Manager Release 6.x is no longer supported. For more information about CMS interoperability with Communication Manager, see [Supported Communication Manager releases](#) on page 16.

CMS feature summary

This section provides a high-level description of key CMS features.

ACD administration

CMS provides an administrative interface to the ACD system. Using CMS Supervisor, you can view or change parameters related to ACD, call vectoring, and Expert Agent Selection (EAS) on ACD systems. An administrator can also run reports that analyze the operation of your call center.

For example, an administrator can:

- Add or remove agents from splits or skills.
- Move extensions between splits or skills.
- Change split or skill 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.

Reporting

CMS provides real-time, historical, and integrated reporting to track all activities in the contact center. Using the reports available in CMS Supervisor, you can make business decisions based on entities such as agents, split/skills, vectors, vector directory numbers, and trunks.

From the CMS Supervisor Web Client, you can set up scheduling for a report. The available scheduling options are:

- **Once:** Use this option to schedule a single, one-time report on a specific date and at a specific time.
- **Daily:** Use this option to schedule a report at a specific time every day.
- **Weekly:** Use this option to schedule one or more reports every week. For example, you can schedule a report every Tuesday and Thursday.
- **Monthly:** Use this option to schedule reports on specific days of specific months. Select the month or months and also specify the days when you want a report to run. For example, you can schedule reports to be run on the last Friday of June, July, and August.

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

ACD integration

CMS interfaces with the following ACD systems:

- Communication Manager Release 7.x
- Communication Manager Release 8.x

- Communication Manager Release 10.x
- Routing Core Server

! **Important:**

Encryption of personal data in transit is available with CMS Release 19.1 and later, and Communication Manager Release 8.1.2 and later.

To use all the features of a particular Communication Manager release, you must administer the appropriate release number in CMS. For more information, see *Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting and Deploying Avaya Contact Center – Extended Capacity*.

CMS tenancy

The CMS Tenancy feature is an extension of the CMS user data access management feature. Use this feature to restrict user access to CMS reporting data and functionality within your call center. The new tenant level access for users introduces restricted data access permissions for the following call center resources: Agents, call work codes, split/skills, trunk groups, VDNs, and vectors.

Each tenant partition is assigned call center resources, which are isolated from resources in the other tenant partitions. A tenant partition can be assigned a subset of call center resources, but not all call center resources must be assigned to a tenant partition. Some call center resources can be assigned across all tenants.

A user with tenant level access only has permission to access CMS resources that are assigned to the tenant partition. A user can be assigned permission to access more than one tenant.

You must install the Tenancy feature package to use the CMS Tenancy feature. Use this feature to 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. Within a tenant, each tenant user has access to a restricted set of call center resources and data based on their tenant assignments.

The CMS and ACD Tenancy features are unrelated. All administrative and tenant user actions for CMS Tenancy are carried out independent of ACD Tenancy. Ensure that you carefully administer ACD to achieve effective CMS tenant partitioning and tenant reporting.

ACD tenant partitioning is administered on the ACD system and CMS tenant partitioning administration does not modify or impact ACD tenant partitioning administration. Tenant feature administration on CMS assigns resources such as agents, VDNs, and skills to a CMS tenant and defines how CMS tenant users can access call data that is stored in the CMS database.

CMS does not control the actual call operation or call delivery to agents and skills. Only ACD administration controls how calls are handled and delivered to agents. Therefore, ACD administration impacts data in CMS tenant reports, despite the restrictions imposed by CMS tenant administration.

For example, create CMS tenant 1 and assign agent 1 and skill 1 to CMS tenant 1, and create CMS tenant 2 and assign agent 2 and skill 2 to CMS tenant 2. If agent 1 logs in to skill 2 and receives calls for skill 2, the tenant 1 users will see the skill 2 call data in reports run for agent 1. Even though the tenant user is restricted to running reports for agents assigned to tenant 1, CMS will display all the call data for agent 1. This implies that the tenant user will see call data for skills assigned to a different tenant. CMS must display all the data for an agent or the summary data will

be incomplete. Therefore, you must carefully plan tenant administration on both ACD and CMS prior to implementation.

The resources shared between tenants must be mutually exclusive. You cannot assign the same call center resource to different tenants. Different tenants on an ACD cannot share an agent, call work code, split/skill, trunk group, VDN, and vector.

There are three types of users:

- **Administrator:** An administrator is a user who has access to all the functions of CMS, all CMS reports, and all CMS data. Administrators can provide admin level access, normal user access, or tenant level access to other users. Administrators can also create and administer tenant users.
- **Normal user:** A normal user is given read, write, and exception permissions by the administrator for ACDs, splits/skills, trunk groups, VDNs, and vectors.
- **Tenant user:** This user has tenant level access, which can span multiple tenant partitions. This user has permissions for viewing or working with CMS resources within the assigned tenant partitions. A tenant user is also assigned permission to access the split/skills, trunk groups, VDNs, and vectors within the tenant partition. Additional restrictions within a tenant can be assigned to each individual tenant user. Note that a tenant user can also create custom reports or design reports that only they can access.

Examples of Tenancy usage

- Service Providers can use Tenancy to partition their ACDs so CMS can be used by multiple tenants or customers within the same ACD, but without access to each other's data.
- A call center with multiple departments or business units that have separate independent functions can create tenants to allocate each business unit a different set of tenant partitions.
- Customers that have a hierarchical reporting structure can use tenancy to enable supervisors and report users to manage only a subset of the call center resources.

LDAP integration

CMS supports LDAP Active Directory for user management. You can integrate CMS with Active Directory on Windows Server. CMS can only integrate with a single Active Directory system. Azure Active Directory is not supported.

You can administer traditional CMS Linux users and LDAP-authenticated users with CMS. When LDAP is enabled, the CMS User Data page provides an option to identify LDAP-authenticated users. When logging in to CMS, users are authenticated with the LDAP server. Linux password administration is not required for LDAP-authenticated users.

With LDAP integration, you can log in to all CMS interfaces, including:

- CMS Supervisor Web Client
- CMS Supervisor PC Client
- CMS ASCII

You can encrypt the Active Directory server connection to avoid exposing personal data. Data encryption with LDAP is an optional feature you can enable when installing the LDAP authentication feature package. Certificate setup is required to encrypt the LDAP connection.

Related links

[LDAP connection encryption](#) on page 29

Data backup

CMS supports data backup, migrations, and restores using several different methods:

- Tape
- USB storage device, non-tape backup
- NFS mounted file system, non-tape backup

Important:

When using NFS for backups on CMS 18.0.2 or later, you must use NFS Version 4 (v4). When upgrading from an older version of CMS that supports an older version of NFS, you must upgrade your NFS setup to NFS v4 after you upgrade your system.

CMS Supervisor

CMS Supervisor provides access for CMS reports and administration. It is available in several different interfaces:

- **Web Client** — The Web Client is a browser-based interface that is installed with the CMS server software. You do not have to install any software on individual PCs.
- **PC Client** — The PC Client is a Windows-based interface. To use the PC Client, you must install it on all user PCs.
- **Mobile Client** — The Mobile Client is an Apple iPad application that helps supervisors and operations managers in a call center monitor activity when they are away from their desks.

For more information about CMS Supervisor, see the following documents:

- *Avaya CMS Supervisor Clients Installation and Getting Started*
- *Administering Avaya Call Management System*
- *Avaya CMS Supervisor Reports*

Avaya Solutions Platform

CMS can be installed on Avaya Solutions Platform 130 Appliance servers for new installs and upgrades. The Avaya Solutions Platform servers are pre-installed with VMware ESXi software. The CMS OVA file is installed on the Avaya Solutions Platform server at the customer location.

Networking with IPv4 or IPv6

CMS supports IPv4 and IPv6 connectivity. You can configure IPv4 or IPv6 connectivity with ACD using the `cmsadm` command and `acd_create` option. You must consistently use either IPv4 or IPv6 addresses.

CMS Supervisor Web Client and Mobile Client can also use either IPv4 or IPv6. CMS integrates with CMS Supervisor PC Client, Terminal Emulator, and Network Reporting over IPv4 or IPv6. No extra configuration is required to enable the IPv6 capabilities of CMS reporting client applications.

IPv6 protocol, 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.

WebLM and PLDS

Avaya products use WebLM Release 8.0 or later to manage product licenses obtained through PLDS. For CMS licensing, use either a standalone WebLM server or install the WebLM server on a coresident Avaya Aura® System Manager. Licenses installed for WebLM must support SHA256 digital signatures and a 14-character host ID.

Important:

Use Centralized licensing for CMS. Enterprise licensing is not supported. This means that multiple CMS deployments cannot share one license file. After enabling Centralized licensing, you must assign every license file to the license ID in WebLM.

For more information about installing license files, see the following documents:

- *Administering Avaya Aura® System Manager*
- *Administering standalone Avaya WebLM*

For WebLM licensing, you have 30 days to provide a valid host name to a WebLM Release 8.0 or later server where the CMS license is installed. If you cannot provide a valid host name, CMS enters the License Error mode for 30 days. After 30 days, CMS enters the License Restricted mode.

Local and enterprise login options

Avaya Call Management System supports local and enterprise login.

Local login

- Use the administered CMS user ID and password.
- You can optionally administer users through Microsoft Active Directory for LDAP password authentication.

Enterprise login

- Microsoft Azure and OKTA are supported for login authentication.
- This login option is only available for use with the CMS Web Client.
- Multifactor authentication (MFA) is enforced if Microsoft Azure or OKTA is configured for MFA.
- The LDAP package is not required.
- You must have a login ID configured in CMS.
- CMS administration is required to enable CMS to be recognized by Microsoft Azure or OKTA.

Login authentication through a personal certificate is also available. This is a requirement of the Joint Interoperability Test Command (JITC) certification. For Federal and Department of Defense employees, personal certificates are encoded and provided by Common Access Card (CAC).

The CMS implementation does not limit support to requiring certificates to be on CACs. Personal certificates can be in a regular certificate store, such as the Microsoft Certificate Store.

Simplified CMS HA configuration

If you have two raw CMS servers installed, you can use a simplified command process to configure High Availability. On the CMS server console, run the `cmsadm` command to access the HA configuration option. You can use this HA configuration process to do the following:

- Set up the primary and secondary server roles.
- Reverse the primary and secondary server roles.

When you first set up the server roles, you must have the details of the CMS server that you want to designate as the secondary server.

Chapter 3: Interoperability

CMS product compatibility

Supported Communication Manager releases

Communication Manager release	CMS release								
	16.x	17.x	18.0	18.1	19.0	19.1	19.2	20.0	21.0
7.x	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8.x	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
8.1.2+ Secure	No	No	No	No	No	Yes	Yes	Yes	Yes
10.x	No	No	No	No	No	No	Yes	Yes	Yes

Supported Avaya Contact Center – Extended Capacity releases

Avaya Contact Center – Extended Capacity Routing Core release	CMS release
10.x	21.0

CMS server releases supported by CMS Supervisor

- 16.x
- 17.x
- 18.x
- 19.x
- 20.x
- 21.x

Software provided with CMS

- CMS server software
- CMS supplemental services
- Informix

Operating system compatibility for the CMS server

CMS server software is compatible with Red Hat Enterprise Linux (RHEL) 8.x.

Operating system support by browser type for the CMS Supervisor Web Client

The following table lists the web browsers you can use to access the CMS Supervisor Web Client and the supported operating systems for each browser. Ensure that your browser is up-to-date. Use the latest browser version or the previous version.

Web browser	Supported operating systems
Microsoft Edge	<ul style="list-style-type: none"> • Windows 10 • Windows 11
Google Chrome	<ul style="list-style-type: none"> • Windows 10 • Windows 11 • macOS 13 (Ventura) • macOS 14 (Sonoma) • ChromeOS
Mozilla Firefox	<ul style="list-style-type: none"> • Windows 10 • Windows 11 • macOS 13 (Ventura) • macOS 14 (Sonoma)
Apple Safari	<ul style="list-style-type: none"> • macOS 13 (Ventura): Version 16 and 17 • macOS 14 (Sonoma): Version 17

Windows compatibility for the CMS Supervisor PC Client

The CMS Supervisor PC Client supports the following Windows operating systems:

- Windows 10 version 22H2 and later
- Windows 11 version 22H2 and later

*** Note:**

Windows 10 S and Windows 11 S are not supported.

Windows service packs and patches

To ensure compatibility and security, install the latest service packs and security patches for your supported Windows operating system before installing CMS Supervisor or Network Reporting.

Supported upgrade scenarios

CMS supports the following upgrade scenarios:

- **Software Upgrades:** Upgrade from an older CMS software release and retain the same hardware server or VMware server. You will back up the customer data, use software discs and a CMS OVA file to install the new Linux OS and CMS software, and then migrate the customer data.
- **Platform Upgrades:** Upgrade from an older CMS software release and install a new customer-provided VMware server or an Avaya Solutions Platform 130 Appliance VMware server. You will back up the customer data, use a CMS OVA file to install the new Linux OS and CMS software, and then migrate the customer data onto the new software release.
- **Base Load Upgrades:** Simplified upgrade process, which is available for CMS upgrades within the same minor release and other approved scenarios. You will use a software disc or a CMS ISO image file to install the new Linux OS and CMS software.

Upgrades to R21

Perform a full software or platform upgrade from Release 20.0 to Release 21.0. You can also upgrade directly to Release 21.0 from the following earlier releases: 16.x, 17.x, 18.x, or 19.x. Contact your Avaya account team if you need to upgrade from a CMS release older than 16.x.

Upgrades on Avaya Enterprise Cloud™ are also supported.

Software upgrades

The software upgrade process reuses existing CMS hardware that supports the new CMS software. The following models of hardware support CMS Release 21.0:

- Avaya Solutions Platform 130 Appliance VMware servers
- Customer-provided VMware servers
- Customer-provided Amazon Web Services (AWS) servers
- Customer-provided Google Cloud Platform (GCP) servers

Additional information

For more information about upgrades, see the following documents:

- *Planning for Avaya Call Management System Upgrades*
- *Upgrading Avaya Call Management System*
- *Deploying Avaya Call Management System*
- *Avaya Call Management System Base Load Upgrade*

Chapter 4: Performance specifications

Capacity limits

Capacities are the maximum limits that a particular CMS hardware platform or VMware configuration can support. You must verify that none of the capacity limits are exceeded for a particular hardware platform. If you do, then you must use the next higher capacity hardware platform or configuration. For example, if you are using a small VMware configuration, you must move up to a medium or large VMware configuration.

Capacity descriptions

The following sections describe capacity measurements. Use this information to determine the type of CMS platform you need.

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 appearance 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

One Report Element is equivalent to running the Skill Status report with a three-second refresh rate and the report returning one hundred rows of data. The Skill Status report is available from Realtime > Split/Skill > Skill Status report.

For context, there are two queries in the report:

1. Query **data1**: select csplit.INQUEUE + csplit.INRING, csplit.OLDESTCALL, csplit.EWTTOP, csplit.EWTHIGH, csplit.EWTMEDIUM, csplit.EWTLOW, SKSTATE from csplit
2. Query **data2**: select cagent.LOGID, cagent.LOGID, cagent.AUXREASON, cagent.AWORKMODE, cagent.DIRECTION, cagent.WORKSKILL, cagent.WORKSKLEVEL, cagent.AGTIME, cagent.VDN, cagent.AWORKMODE from cagent

Query **data1** returns one row with seven data fields, one of which has a synonym lookup.

Query **data2** returns ten fields; in our example, it would return 100 rows.

Six data fields have synonym lookups, and two are keyword lookups. (synonym and keyword lookups are approximately twice as expensive as plain data)

If you add a summary query, it adds to the load on the CMS.

If you run the Skill Status report with a three-second refresh rate and the report returns two hundred rows of data, this would be considered two report elements.

Integrated queries create a greater load on the server when started; however, they pull around the same amount of data as a real-time report after that time except for interval, day, and start-of-day boundaries.

Historical reports put a load on the server when you run, refresh or restart them.

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

Review the server capacity requirements outlined in this section before installing CMS. This section also provides general CMS system capacity information.

When FIPS 140-2 encryption 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)

! Important:

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

Capacity requirements for new installations

The following table lists the capacity requirements for customer-provided VMware servers or Avaya-provided Avaya Solutions Platform 130 Appliance servers being sold for CMS:

Parameter	Small	Medium	Large	Extended
Peak busy-hour call volume	30,000	200,000	400,000	500,000
Concurrent CMS Supervisor sessions ¹	50	200	1,999	1,999
Concurrent agents	500	5,000	10,000	30,000
Third-party software	3	5	7	3
Agent skill pairs	100,000	200,000	800,000 ²	1,500,000 ²
Reports per CMS Supervisor session	3	5	10 ³	15 ³
Report elements ⁴	5	5	12	12
Percentage of supervisors that can run reports with a three-second refresh rate	10%	50%	100%	100%
Active agent traces	250	1,000	5,000	5,000
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
External Call History (ECH) records	10,000 per 20 minutes	60,000 per 20 minutes	300,000 per 20 minutes	300,000 per 20 minutes

1. This value is the total number of active CMS Supervisor PC and Web Client sessions.
2. For more than 800GB of storage, create additional disk volumes.
3. Three real-time reports and up to the listed value for historical data.
4. For a definition of report elements, see [Report elements](#) on page 20.

System-wide capacities

CMS attribute	System wide capacity	Per ACD maximum capacity
Agent skill pair	800,000	360,000
Total VDNs	54,000	30,000

Table continues...

CMS attribute	System wide capacity	Per ACD maximum capacity
Total splits or skills	54,000	8,000
Total trunks	100,000	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

Maximum values with multiple ACD deployments

Basic Maximum Values					
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.

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 Automatic Call Distribution (ACD). 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 32.

Recommendations for report customization

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.
 - 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 server. 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 installation and upgrade tables in [Capacity and scalability specifications](#) on page 21.

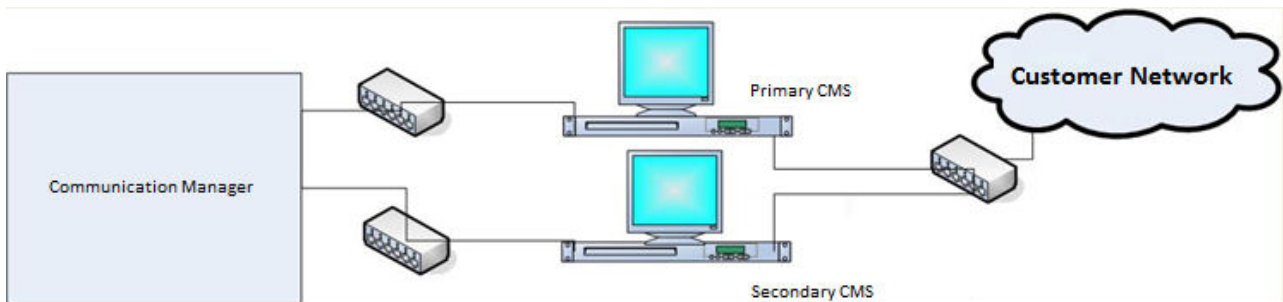
Redundancy and high availability

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 supports up to 16 digit extensions for agent, login id, VDN, and station.

Chapter 5: Security

Security specifications

The following sections outline CMS security features. For more information about security best practices, see *Avaya Call Management System Security*.

Operating system hardening

CMS achieves operating system hardening through the following:

- Patching and patch qualification: CMS includes all necessary components, including security patches during release. Avaya receives additional patch notifications and certifies new Linux® OS patches. Avaya then assembles these patch clusters and makes them 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 routinely for signs of unusual activities.
- Banner modifications: Altering the Telnet and FTP network service banners hides operating system information from individuals wanting to exploit known security issues.
- Email and SMTP: Do not configure CMS as a mail relay and disable the Simple Mail Transfer Protocol (SMTP) daemon.

Authentication and session encryption

CMS achieves authentication and session encryption through the following:

- User authentication and authorization: CMS uses Linux® OS login and password security measures 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 operating system 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 install this, 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.

*** Note:**

For information about FIPS 140-2 encryption, see *Maintaining and Troubleshooting Avaya Call Management System* and *Avaya Call Management System Release Notes*.

Data privacy regulations

Many organizations have policies related to personal data handling. For example, the European Union issued the General Data Protection Regulation (GDPR) and the USA State of California created the California Consumer Privacy Act (CCPA). To support these policies, CMS supports the encryption of data at rest and data in transit. CMS provides tools and guidelines to manage personal data. For more information about how CMS protects personal data, see *Product Privacy Statement for Avaya Call Management System*.

Encryption of personal data at rest

CMS supports encryption for personal data at rest. Supported platforms encrypt disks by default or with minimal configuration.

Encryption of personal data in transit

Personal in transit can be encrypted between CMS and its connected ACD systems. The SPI link encryption is invisible to the user and is automatically implemented when you administer the link between the systems.

Encryption of personal data in transit is available with CMS Release 19.1 and later, and with Communication Manager Release 8.1.2 and later.

Optional data encryption features

- You can encrypt data sent over LDAP connections to an Active Directory server.
- You can encrypt data sent over ODBC and JDBC connections.

Application security

CMS provides application security through the SPI link, application-level audit logging, and database security controls.

Physical security

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

Services security and CMS support

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

Personal data in CMS

CMS stores the following types of personal data:

- Call center agent information.
- CMS user information.
- Phone numbers dialed by individuals placing calls into the call center.
- Phone numbers dialed by agents placing calls outside the call center.

The call center agent information and CMS user information are for company employees using CMS. The type of personal data that is stored is limited to information that facilitates standard employee work operations.

Information about individuals calling the call center is specific to dialed digits. Information about agents calling outside the call center is also specific to dialed digits.

CMS provides logs and tools to manage personal data in CMS. For more information about managing personal data, see *Maintaining and Troubleshooting Avaya Call Management System*.

General Data Protection Regulation support

General Data Protection Regulation (GDPR) is European Union (EU) legislation designed to strengthen and unify data protection laws for all individuals within the EU. This regulation applies to any organization that processes the personal data of individuals in the EU.

GDPR affects the everyday operations of any department within organizations that act as data controllers. The regulation regards data controllers as entities that collect data from data subjects.

CMS stores several categories of personal data, such as Call center agent information, CMS user information, and limited information about individuals calling the contact center.

For more information about GDPR, see *Product Privacy Statement for Avaya Call Management System*.

Certificates for secure communication

Certificates are required for secure communication in various scenarios. CMS uses certificates for the following:

- Web Client
- EASG
- LDAP
- ODBC/JDBC
- SPI

Web Client encryption

You must install a security certificate to encrypt communication between browsers and the Web Client CMS server.

For more information about:

- Activating the CMS Supervisor Web Client software, see *Deploying Avaya Call Management System*.
- Certificate management, see *Maintaining and Troubleshooting Avaya Call Management System*.

EASG

The Enhanced Access Security Gateway (EASG) package is integrated into CMS and provides secure authentication and auditing for remote access to maintenance ports.

EASG authentication is based on a challenge-response algorithm that uses a token-based private key-pair cryptographic authentication scheme. Logs include information about successful and failed logins, errors, and exceptions.

EASG enables control of Avaya service engineer privileges when accessing customer products. EASG controls permission levels, such as init, inads, and craft, which service engineers use.

On a CMS server, a dedicated EASG product certificate is installed under the EASG directory `/etc/asg`, which must be used for all associated files. The EASG product certificate uniquely identifies CMS major releases to the Avaya EASG server.

The product certificate is derived from the Avaya IT Root Certificate Authority (CA) and intermediate CAs. The Avaya EASG server uses CAs to create a response, and CMS uses the EASG product certificate public key to verify the response through the EASG Common Red Hat Package Manager (RPM). The product certificate is included with the CMS deployment so you do not need to perform additional certificate configuration tasks.

For information about configuring EASG, see *Maintaining and Troubleshooting Avaya Call Management System*.

LDAP connection encryption

CMS supports LDAP Active Directory for user management. You can encrypt the Active Directory server connection to avoid exposing personal data. Encryption of the LDAP connection requires a certificate setup.

For information about:

- Administering LDAP, see *Administering Avaya Call Management System*.
- Updating the LDAP authentication package configuration, see *Maintaining and Troubleshooting Avaya Call Management System*.

Related links

[LDAP integration](#) on page 12

ODBC and JDBC network connections

You can configure the CMS network ports 50000 and 50001 for Informix TLS and SSL encryption. You can also use these CMS network ports for Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) connections. For TLS and SSL encryption, you must install a PKCS 12 certificate.

For more information about:

- Encrypting ODBC and JDBC connections, see *Using ODBC and JDBC with Avaya Call Management System*.
- Installing PKCS certificate files, see [PSN006046u – CMS ODBC Driver support for Signature Algorithm attribute](#).

SPI link

For the SPI link, ACD is the server and CMS is the client. No additional certificate configuration is required on the CMS client.

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 product performance
- Value the Avaya customer support entitlements

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

1. Go to <https://support.avaya.com>.
2. Log on 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 Registration page, do one of the following steps:
 - Select **End to End Registration**.
 - Select **Technical Onboarding Only**.
5. Enter the 10-digit functional location number (sold-to number) for 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, 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 onboarding, 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.

Port utilization

The *Port Matrix for Avaya Call Management System* document 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/products> under **Product Documents**. You can view the port matrix document only after you log in to the Avaya Support site using valid support site credentials.

Chapter 6: Licensing requirements

CMS agent licensing enforcement

Avaya policy states that the number of CMS agent licenses for simultaneously logged-in ACD agents must be equivalent to or greater than the number of agent licenses in the ACD.

! Important:

An agent license in CMS is consumed for each agent logged in to at least one measured skill. Regardless of the number of skills assigned to an agent, only one CMS agent license is consumed when an agent logs in to one or more measured skills.

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. CMS is capable of reporting on all Logged In or Staffed Call Center Agents for any ACD that CMS is monitoring. For example, consider that agent Angela Smith leaves the company. CMS continues to report on Angela and her formerly assigned Agent Login ID even though Angela is an inactive agent on the ACD. In this example, agent Angela does not count as a simultaneously logged-in agent.

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

Licensing overview

Avaya provides a Web-based License Manager (WebLM Release 8.0 or later) to manage licenses of Avaya CMS. WebLM facilitates easy tracking of licenses. To track and manage licenses, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com>.

Related links

[Licensed features in CMS](#) on page 33

[CMS license modes](#) on page 33

[License management](#) on page 34

[License enforcement](#) on page 35

[License log file](#) on page 39

[Alarms](#) on page 39

[Backing up and restoring WebLM](#) on page 40

Licensed features in CMS

CMS supports the following licensed features through PLDS licensing:

Features for a primary CMS

- Number of agents for a primary system
- Number of CMS Supervisor sessions for a primary system
- Number of Automatic Call Distribution (ACD) connections to ACD systems for a primary system

Features for an HA or Survivable CMS (including dual role)

- HA or Survivable system

The CMS application that it is on an HA or Survivable system. The system uses the HA feature license and not the primary feature license.

- Number of agents for an HA or Survivable system
- Number of CMS Supervisor sessions for an HA or Survivable system
- Number of ACD connections to ACD systems for an HA or Survivable system

Other features

- Number of ODBC and JDBC subscriptions

The ODBC and JDBC subscriptions are used for both primary and HA or Survivable CMS systems.

ODBC and JDBC access is available on both the primary CMS and an HA or Survivable CMS. Separate ODBC and JDBC licenses are required for each CMS in the deployment.

- Number of Command Line Interface (CLInt) external sessions
- Number of CLInt internal sessions

CMS license modes

CMS uses the following three modes for license checking:

- License Normal mode
- License Error mode
- License Restricted mode

The logs record any transitions among the modes and issue alarms for transition into Error and Restricted modes.

License Normal mode

The License Normal mode is a condition of no license violations. In this mode, the CMS instance gains access to WebLM and shares the latest license information.

License Error mode

The License Error mode is a condition of license violation. In the License Error mode, CMS:

- Issues a warning message when an administrative user logs in or when the user invokes `cmssvc` or `cmsadm`.
- Issues a daily alarm.

If the system is in License Error mode for more than 30 days, CMS takes actions to eliminate the violations or move the CMS into the License Restricted mode depending on the violations.

When the system clears all license violations for 8 consecutive days, CMS goes back to License Normal mode.

License Restricted Mode

When CMS switches into the License Restricted mode, the CMS instance:

- Terminates and blocks all user interface sessions.

The `cms` and `cmssvc` users may log back on using the ASCII interface. Using `cms`, you can gain access only to the System Setup and Maintenance submenus. Using `cmssvc`, you can gain access to the additional Services submenu.
- Terminates all external and internal CLInt sessions. The CMS instance blocks CLInt sessions from getting started.
- Terminates all JDBC or ODBC sessions and denies subsequent JDBC or ODBC sessions.
- Stops External Call History.

Once the system clears all license violations, the CMS instance switches back to the License Normal mode.

License management

CMS uses license enforcement to manage license checking. The system checks for license violations and performs the following tasks every 9 minutes:

- Retrieves the newest license information from WebLM.
- Retrieves the number of ACDs and renew, acquire, or release ACD licenses.
- Retrieves the agent login information and renew, acquire, or release agent licenses.
- Retrieves the supervisor login information and renew, acquire, or release supervisor licenses.
- Retrieves CLInt usage information and renew or acquire CLInt licenses
- Retrieves ODBC and JDBC usage information and renew, acquire, or release the ODBC and JDBC session licenses, as needed.
- Calculates the license status:
 - Log to eLog when new license violation is detected
 - Log to eLog when license status changed
 - Log the license status
- Takes appropriate action based on the calculated license status.

If the system cannot get the latest licensing information from WebLM, the system uses the existing license information for license checking.

License enforcement

The CMS instance enters License Restricted mode when any of the following license conditions are violated for 30 consecutive days:

- License Validity
- ACD Count
- Agent Count

The system stays in License Restricted mode until all license violations are corrected.

Other licenses, such as Supervisor Session Count, JDBC or ODBC Session Count, and CLInt Session Count, might cause the CMS instance to enter License Error mode if violated. However, the License Error mode does not cause the CMS instance to enter the License Restricted mode. Instead, CMS instance attempts to clear the errors by disconnecting any sessions above the valid license count.

License Validity

If CMS fails to get a valid license, any of the following conditions are true:

- CMS cannot connect to WebLM
- CMS cannot obtain a CMS license after connecting to WebLM
- CMS license expired
- CMS license has a version less than the currently running version

If CMS cannot obtain a license initially, the system does not consider the maximum capacity. Otherwise, it considers the previous capacities. In case of expired licenses or incorrectly versioned licenses without previous capacities, you can use the capacities specified in the improper license.

ACD Count

When you create an ACD, CMS ensures the number of ACD does not exceed the limit. However, if the licensed ACD count is lowered, CMS enters the License Error mode. If you do not remove the additional ACDs within 30 days, CMS enters the License Restricted mode. If you increase the number of ACDs in the license or remove the extra ACDs, the system removes the restriction.

Note:

The ACD count applies to the number of administered ACDs and not the number of active ACDs. Even if data collection is off or link is down for a ACD, the system counts ACD towards the limit. The system does not include the pseudo ACDs in the ACD count.

Furthermore, even if CMS is not up and running, technically the administered ACDs consume the ACD licenses. However, CMS does not maintain the license usage information with WebLM when CMS is not running.

In summary, you can clear the ACD license violation if you:

- Remove ACD(s) to the level of the licensed count

- Update the CMS license with an increased ACD count

Agent Count

CMS enters the License Error mode when the number of logged in agents exceeds the licensed count, the violation clears itself if the numbers stay below the limit for 8 days since the last violation.

For example, if the number of agents exceeds the limit on 1st, 4th, and 7th day, CMS clears the error on the 16th day if the system does not detect violation between 7th days and 16th day.

When the system does not clear the violation in 30 days, CMS enters the License Restricted mode upon the next violation. For example, if the number of agents exceeds the limit on 1st, 7th, 14th, 21st, 28th, and 33rd, CMS enters the License Restricted mode on the 33rd day. If there is no violation between 33rd and 41st day, CMS returns to the License Normal mode. If at any time during the 33rd and 41st day, the system updates the CMS license with an increased agent count, CMS returns to the License Normal mode if it does not experience other license violations.

In summary, you can clear the agent license violation when:

- No violation for eight consecutive days
- CMS license is updated with increased agent count

Supervisor session count

When a supervisor logs in, CMS checks the current session count against the latest licensed count. The system blocks the login to avoid going beyond the limit.

In a rare case, if the system decreases the licensed count and if the current login sessions exceed the decreased count, CMS enter the License Error mode.

If the supervisor session count exceeds the limit for 30 days, the system terminates all supervisor sessions. Supervisors must log in again.

ODBC and JDBC session count

CMS cannot block excessive ODBC and JDBC sessions. When the number of ODBC and JDBC sessions exceed the licensed count, CMS enters the License Error mode. The violation automatically clears if the number of sessions stays below the limit for 8 days since the last violation.

If you do not clear the violation within 30 days, CMS stays in the License Error mode. However, CMS randomly terminates ODBC and JDBC sessions to keep the count below threshold. After clearing the ODBC and JDBC license violation, if there are no further violations for 8 days, CMS switches back to the License Normal mode.

CLInt session count

There are two counts for CLInt sessions:

- For external use by non-CMS applications
- For internal use by CMS applications, such as RTA and ECH_handler

For example, the existing invocation now applies to the external count:

```
/cms/toolsbin/clint -u cmssvc
```

You can execute the `clint` program only if either of the counts is greater than zero (0). However, the session count only applies to real-time reporting. As soon as the CLInt session starts a real-time report, the system applies for the license. The session ends if it meets the limit.

License enforcement with different license modes

The following table lists how the licensing for different features are enforced in the different licensing modes:

Feature	Normal Mode	Error Mode occurs when...	Violation clears itself when...	If Error Mode continues for 30 days...	Restricted Mode behavior
WebLM Licensing	CMS is getting a valid license from WebLM	<ul style="list-style-type: none"> • Cannot access WebLM • Cannot get CMS license from WebLM • Wrong CMS version • CMS license expired 	CMS is getting a valid license from WebLM	System enters Restricted Mode	<ul style="list-style-type: none"> • All CMS Supervisor, CLInt, ODBC, and JDBC sessions terminated • Access to CMS is restricted to cms and cmssvc logins via the ASCII interface. Only Setup, Maintenance, and Services submenus are available. • New CLInt access blocked • New ODBC and JDBC access blocked. • Data collection continues. • ECH data recording stops.

Table continues...

Feature	Normal Mode	Error Mode occurs when...	Violation clears itself when...	If Error Mode continues for 30 days...	Restricted Mode behavior
ACD Count	Adding of ACDs are denied if over the limit	Licensed count is lowered below the number of existing ACDs	Excess ACD(s) are removed or License count is increased to match the existing ACD count.	Enter Restricted Mode	<ul style="list-style-type: none"> • All CMS Supervisor, CLInt, ODBC, and JDBC sessions terminated • Access to CMS is restricted to cms and cmssvc logins via the ASCII interface. Only Setup, Maintenance, and Services submenus are available. • New CLInt access blocked • New ODBC and JDBC access blocked. • Data collection continues. • ECH data recording stops.
Agent Count	Agent logins monitored	Agent logins exceed licensed count on a given day	Licensed count is not exceeded for 8 consecutive days or Licensed count is increased	Enter Restricted Mode upon next violation	<ul style="list-style-type: none"> • All CMS Supervisor, CLInt, ODBC, and JDBC sessions terminated • Access to CMS is restricted to cms and cmssvc logins via the ASCII interface. Only Setup, Maintenance, and Services submenus are available. • New CLInt access blocked • New ODBC and JDBC access blocked. • Data collection continues. • ECH data recording stops.

Table continues...

Feature	Normal Mode	Error Mode occurs when...	Violation clears itself when...	If Error Mode continues for 30 days...	Restricted Mode behavior
CMS Supervisor Session Count	CMS Supervisor log ons are denied if the licensed count is reached.	Licensed count is lowered below the existing number of logged on CMS Supervisor users	CMS Supervisor users log off and log ons are at or below the licensed count	All CMS Supervisor sessions are terminated; CMS Supervisor users must log on again	NA
ODBC and JDBC Session Count	ODBC and JDBC sessions are at or below the licensed count	Sessions exceed the licensed count	Licensed count is not exceeded for 8 consecutive days	ODBC and JDBC sessions are randomly terminated until at the licensed count	NA
CLInt Session Count	CLInt sessions running real time reports are terminated if the licensed count is exceeded	The CLInt license limit is lowered below existing number of CLInt sessions	CLInt sessions terminate to at or below the licensed count	All CLInt sessions are terminated; sessions must be restarted	NA

License log file

The system saves a licensing log file in the following location to record the status of licensing:

```
/cms/env/lm/license.log
```

You can configure CMS to store the status log for up to 45 days.

Alarms

Based on the AOM settings, the system forwards the alarms either through the socket connection or through SNMP agent to INADS and/or customer network management system.

CMS provides three levels of alarms:

- Warning
- Minor
- Major

When CMS enters the License Error mode, the system triggers a Minor alarm. When the server enters the Restricted mode, the system triggers a major alarm. The Major alarm stays until the server returns to the Normal mode.

Backing up and restoring WebLM

The CMS instance does support backing up or restoring the current license state. To restore CMS from a catastrophic loss, you must restart the CMS instance. The system gets the license data from WebLM and determines the license state.

Chapter 7: Resources

Documentation

CMS and CMS Supervisor Documents

Title	Description	Audience
Overview		
<i>Avaya Call Management System Overview and Specification</i>	Describes tested product characteristics and product capabilities including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Sales engineers, Administrators
<i>Product Privacy Statement for Avaya Call Management System</i>	Describes how personal data is stored and processed by CMS.	Administrators
Installation, upgrades, maintenance, and troubleshooting		
<i>Deploying Avaya Call Management System</i>	Describes how to plan, deploy, and configure CMS on new VMware-based installations.	Avaya support personnel
<i>Deploying Avaya Call Management System on an Infrastructure as a Service Environment</i>	Describes how to plan, deploy, and configure CMS on new Amazon Web Services and Google Cloud Platform environments.	Avaya support personnel
<i>Planning for Avaya Call Management System Upgrades</i>	Describes the procedures customers must plan for before and after upgrading to a new CMS release.	Administrators
<i>Upgrading Avaya Call Management System</i>	Describes the procedures required to upgrade to a new CMS release.	Avaya support personnel
<i>Maintaining and Troubleshooting Avaya Call Management System</i>	Describes how to configure, maintain, and troubleshoot CMS.	Avaya support personnel, Administrators
<i>Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting</i>	Describes how to connect and administer the Automatic Call Distribution (ACD) systems used by CMS.	Avaya support personnel, Administrators

Table continues...


Title	Description	Audience
<i>Avaya Call Management System Base Load Upgrade</i>	Describes the procedures to upgrade from one base load (for example, 19.1.0.0) to another base load (for example, 19.1.0.1). Not all releases support base load upgrades.	Administrators
<i>Avaya Call Management System High Availability Connectivity, Upgrade and Administration</i>	Describes how to connect to HA servers and upgrade to HA.	Avaya support personnel, Administrators
<i>Using Avaya Call Management System High Availability and Admin-Sync</i>	Describes how to install and maintain your CMS High Availability (HA) system.	Avaya support personnel, Administrators
Administration		
<i>Administering Avaya Call Management System</i>	Provides instructions on administering a call center using CMS Supervisor.	Avaya support personnel, Administrators
<i>Avaya Call Management System Call History Interface</i>	Describes the format of the Call History data files and how to transfer these files to another computer.	Administrators
<i>Using ODBC and JDBC with Avaya Call Management System</i>	Describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS.	Administrators
<i>Avaya Call Management System Database Items and Calculations</i>	Describes each database item and calculation that CMS tracks and how CMS calculates the values displayed on CMS reports and CMS Supervisor reports.	Administrators, Report designers
<i>Avaya Call Management System Custom Reports</i>	Describes how to design and create custom reports in CMS.	Administrators, Operations personnel, Report designers
<i>Avaya Call Management System Security</i>	Describes how to implement security features in CMS.	Avaya support personnel, Administrators
CMS Supervisor		
<i>Avaya CMS Supervisor Clients Installation and Getting Started</i>	Describes how to install and configure CMS Supervisor.	Avaya support personnel, Administrators
<i>Avaya CMS Supervisor Reports</i>	Describes how to use CMS Supervisor reports.	Administrators, Operations personnel
<i>Avaya CMS Supervisor Report Designer</i>	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Administrators, Operations personnel, Report designers

Avaya Solutions Platform Documents

Title	Description	Audience
<i>Avaya Solutions Platform Overview and Specification</i>	Describes the key features of Avaya Solutions Platform server	IT Management, sales and deployment engineers, solution architects, support personnel
<i>Installing the Avaya Solutions Platform 130 Appliance</i>	Describes how to install Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel
<i>Maintaining and Troubleshooting Avaya Solutions Platform 130 Appliance</i>	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel
<i>Avaya Solutions Platform 130 Series iDRAC9 Best Practices</i>	Describes procedures to use the iDRAC9 tools on the Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Accessing the port matrix document

Procedure

1. Go to <https://support.avaya.com>.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.

4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Choose Release**, select the required release number.
9. In the **Content Type** filter, select one or both the following categories:
 - **Application & Technical Notes**
 - **Design, Development & System Mgt**The list displays the product-specific Port Matrix document.
10. Press **Enter**.


Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.


Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** () in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

You can select multiple items in each filter category. For example, you can select a product and multiple user roles.

- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** () to share a topic by email or copy the URL.

- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (📌). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.
- Click **Watch** (👁️) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
- Unwatch the selected content or all topics.
- Send feedback for a topic.

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.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

 **Note:**

Videos are not available for all products.

Support

Go to the Avaya Support website at <https://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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.

6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Upgrade Advantage Preferred

You must subscribe to Upgrade Advantage Preferred to receive major software upgrades when they become available during your contract term. This offer provides investment protection for your communications systems. Use it to reduce risks and costs, and meet business objectives by staying up-to-date with the latest technologies in a predictable operating expense model. Upgrade Advantage subscription includes:

- New and additional licenses
- Upgrading of base licenses
- Moving, merging, and un-parking of licenses

Glossary

Automatic Call Distribution

A programmable feature at the contact center. Automatic Call Distribution (ACD) handles and routes voice communications to queues and available agents. ACD also provides management information that can be used to determine the operational efficiency of the contact center.

From the perspective of CMS, when you describe “an ACD”, you are describing a Communication Manager system.

Aux-Work

In Avaya Agent and Avaya Agent Web Client, the agent status in which the agent is logged in but unavailable to receive a new contact.

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 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

An estimate of how long a caller will have to wait to be served by a call center while in queue considering the current and past traffic, handling time, and staffing conditions. Time spent in vector processing before being queued and the time spent ringing an agent with manual answering operation is not included in the Expected Wait Time (EWT) prediction. With an Avaya communication server and CMS, the EWT is a communication server-based calculation.

Expert Agent Selection

A standard feature that bases call distribution on agent skill, such as language capability. Expert Agent Selection (EAS) matches the skills required to handle a call to an agent who has at least one of the required skills.

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

A switch feature that can be used to balance the call load among multiple contact centers. Look Ahead Interflow (LAI) works with Call Vectoring and ISDN PRI trunks to intelligently route calls between contact centers. With LAI, multiple contact centers can share workloads, expand hours of coverage, and handle calls transparently 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.

switch

A system providing voice or voice and data communication services for a group of terminals. From the perspective of CMS, a “switch” is an ACD system.

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 Directory Number (VDN)

An extension to the Avaya Aura[®] Communication Manager automatic call distributor that directs an incoming call to a vector. A vector is a user-defined sequence of functions, such as routing the call to a destination, giving a busy signal, or playing a recorded message.

Index

A

accessing port matrix	43
ACD	35
ACD integration	10
Agent Count	36
agent group customized reports	24
agent license enforcement	32
agent traces	21
Automatic Call Distribution	35
Avaya InSite Knowledge Base	46
Avaya Solutions Platform	13
Avaya support website	46
average rate capacity	21

B

backup	13
backup WebLM	40

C

call volume	19 , 24
capacity and scalability	21
capacity descriptions	19
certificates	28
certificates for secure communication	
EASG	29
JDBC	29
LDAP	29
ODBC	29
SPI	30
Web Client	28
CLInt session count	36
CMS	33
CMS license modes	
License Error mode	33
License Normal mode	33
License Restricted Mode	33
CMS operating system	
RHEL	17
CMS performance	24
CMS reporting	10
CMS supervisor	24
CMS Supervisor	
Mobile Client	13
PC Client	13
Web Client	13
CMS supervisors	19
CMS tenancy feature	11
collection	
delete	44
edit	44

collection (<i>continued</i>)	
generating PDF	44
sharing content	44
communication manager	23
Communication Manager support	10
content	
publishing PDF output	44
searching	44
sharing	44
sort by last updated	44
watching for updates	44
CPU	23
customizing reports	24

D

data backup	13
document changes	7
documentation	41
documentation center	44
finding content	44
navigation	44
documentation portal	44

E

EASG	29
Enhanced Access Security Gateway	29
extensions for agent	25

F

features	9
finding content on documentation center	44
finding port matrix	43

G

GDPR	28
General Data Protection Regulation	28
Geotel	20

H

HA configuration feature	15
high availability	25

I

installation capacity	21
Integrated Report refresh rate	21

