# Avaya Call Management System Overview and Specification

Release 21.0.2
Issue 4
October 2025

**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 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.

**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.

**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

## Purpose

Learn about the functionality of Avaya Call Management System (CMS), including interoperability, performance specifications, security and certificate details, and licensing requirements.

Use this document to gain a high-level understanding of CMS features, functions, capacities, and limitations in the context of solutions and verified reference configurations.

## Change history

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

| Issue | Date | Summary of changes |
|---|---|---|
| 4 | June 2025 | Updated New in this release on page 9 to include features introduced in version 21.0.2. |
| 3 | November 2024 | Corrected the total trunk capacity for Avaya Aura® Call Center Elite to 30000. |
| 2 | November 2024 | • Revised and reorganized the overview content and feature descriptions for clarity.<br>• Updated Capacity and scalability specifications on page 21 and clarified system-wide and maximum capacity tables. |
| 1 | June 2024 | • Updated New in this release on page 9.<br>• Revised CMS feature summary on page 10 with new information.<br>• Updated interoperability details.<br>• Edited Supported upgrade scenarios on page 18 and added release-specific information.<br>• Removed capacity specifications for hardware-only deployments and performed minor edits in Capacity and scalability specifications on page 21.<br>• Updated Security specifications on page 26 for clarity.<br>• Added certificate information under Certificates for secure communication on page 28. |

# Chapter 2: CMS overview

Avaya Call Management System (CMS) is a software product designed for businesses and organizations that handle a high volume of telephone calls through the Automatic Call Distribution (ACD) feature of the Avaya Aura® Communication Manager system. CMS helps you collect call traffic data, format management reports, and access the ACD feature through an administrative interface.

CMS runs on the Red Hat Enterprise Linux (RHEL) operating system and uses system utilities to communicate with terminals and printers, log errors, and run processes. It uses the Informix database management system to interface with the CMS historical database.

CMS stores ACD data in real-time and historical databases:

- Real-time database: Includes tables for current and previous intrahour interval data. You can configure the storage interval to 15, 30, or 60 minutes.
- Historical database: Includes tables for intrahour, daily, weekly, and monthly data. The historical database can store:
  - Up to 370 days of intrahour data
  - Up to 1825 days (5 years) of daily data
  - Up to 520 weeks (10 years) of weekly data
  - Up to 120 months of monthly data

CMS offers two options to ensure data resiliency in contact center environments:

- High Availability (HA) CMS: Provides data redundancy. You can configure HA if you have two CMS servers, one as the primary and the other as the secondary.

  **Note:**

  The primary and secondary servers can run on the same or different hardware platforms.
- Survivable CMS: Supports business continuity in multi-location contact centers. It ensures continued operation at the controlling site during a disaster.

You can use the CMS Supervisor Web Client and PC Client interfaces to monitor contact center performance and activity. With CMS Supervisor, you can do the following:

- Track real-time metrics such as abandoned calls, average hold time, and queue length.
- Manage reports.

# New in this release

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

### Report scheduling

You can schedule a report in the CMS Web Client. Scheduling options include once, daily, weekly, or monthly. After setting up a schedule, use the Scheduler tab to view and manage your scheduled reports.

### Automated CMS High Availability (HA) configuration

If two CMS servers are installed, use the new HA configuration process. Log in to the CMS server console as root, and enter the `cmsadm` command to access the HA configuration option. You can set up primary and secondary server roles and reverse the roles if needed.

### Informix database upgrade

CMS now uses HCL Informix 14.10, replacing IBM Informix 12.10 used in previous releases.

### Upgrades to Release 21.0

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

### KVM installation

CMS Release 21.0 supports KVM installation on:

- Avaya Solutions Platform 130 R6 server (ASP 130 R6)
- Customer-provided servers

### Discontinued hardware-only platforms

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

- Dell PowerEdge R630 and R730
- HPE ProLiant DL380 Gen9

### 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 details about supported versions, see Supported Communication Manager releases on page 16.

### Changes introduced in CMS R21 Feature Pack 1

- A range of database items has been expanded from integer (4-byte) to int8 (8-byte) format. Refer to the *Avaya Call Management System Database Items and Calculations* document for details.
- The existing VMware image is still supported, but only for installation on customer-provided hardware.

- The ASP 130 R5 server is now end-of-sale.
- The ASP 130 R6 server supports KVM-based virtual machines.

### Changes introduced in CMS R21 Feature Pack 2

- You can configure CMS to use an enterprise authentication service, such as Avaya Identity and Access Management (IAM), to access the CMS Web Client.
- You can schedule administration jobs from the Back Up Data screen.
- You can enable or disable data collection for all ACDs from the Data Collection screen.
- You can enter the enterprise ID on the User data screen.

  The enterprise ID is validated for authentication when the primary user ID does not match a CMS username. Authentication may fail in customer environments where numeric IDs are used as the user principal name (UPN) in the enterprise SSO platform.
- A mechanism that masks failover from Web Client users has been introduced. The cloud-based load balancer uses the CMS session to seamlessly redirect the Web Client link from one CMS server to another.

  Previously, during a failover, users were logged out and had to log in again. With Feature Pack 2, users no longer need to re-enter their username and password after a failover. However, they must click **Enterprise Sign In**. This functionality works with Microsoft Azure and Okta.

# CMS feature summary

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

## ACD administration

CMS provides an administrative interface for supported ACDs. With CMS Supervisor, you can view or change ACD parameters, call vectoring, and Expert Agent Selection (EAS). You can also run reports to analyze the operation of your call center.

You can perform the following administrative tasks:

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

## Reporting

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

From the CMS Supervisor Web Client, you can schedule reports using the following options:

- **Once**: Schedule a one-time report on a specific date and time.
- **Daily**: Schedule a report to run at a specific time every day.
- **Weekly**: Schedule one or more reports each week. For example, every Tuesday and Thursday.
- **Monthly**: Schedule reports on specific days of selected months. For example, on the last Friday of June, July, and August.

CMS stores ACD data from the ACD system in real-time and historical databases. Real-time databases include tables for current and previous intrahour interval data, stored at 15, 30, or 60-minute intervals. 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

**Important:**

Encryption of call 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, administer the relevant release number in CMS. For more information, see *Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting*.

## Managing tenant access

To use CMS tenancy, enable the Tenancy feature package. Tenancy enables you to partition a subset of ACD resources and assign them to specific tenants. Resources assigned to one tenant are isolated from those in other tenant partitions. Therefore, tenants do not share agents, call work codes, splits/skills, trunk groups, VDNs, or vectors. However, some resources can be shared across all tenants.

Tenant users have access only at the tenant level. Each tenant user has access to a restricted set of call center resources and data based on their tenant assignment. You can assign a tenant user to multiple tenants. Tenant users can create custom reports or design reports that only they can access.

### Impact of ACD administration

Although CMS and ACD tenancy features are not directly linked, ACD configuration affects how calls are routed and delivered to agents. This configuration impacts the data shown in CMS tenant reports.

For example:

- Agent 1 and Skill 1 are assigned to CMS Tenant 1.
- Agent 2 and Skill 2 are assigned to CMS Tenant 2.

If Agent 1 logs in to Skill 2 and receives calls for Skill 2, Tenant 1 users will see Skill 2 call data in reports for Agent 1. Even though Tenant 1 users are restricted to running reports for agents assigned to Tenant 1, CMS displays all call data for Agent 1 to ensure report completeness. Hence, Tenant 1 users will see data for skills assigned to other tenants.

To avoid data inconsistencies, plan tenant administration in both ACD and CMS before implementation.

## LDAP integration

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

You can administer traditional CMS Linux users and LDAP-authenticated users. When LDAP is enabled, the User Data page in CMS provides an option to identify LDAP-authenticated users. When users log in to CMS, they are authenticated through the LDAP server. You do not need to manage Linux passwords for LDAP-authenticated users.

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

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

To protect personal data, you can encrypt the connection to the Active Directory server. LDAP data encryption is optional and can be enabled during installation of the LDAP authentication feature package. Certificate setup is required to enable encryption.

**Related links**

LDAP connection encryption on page 29

## Data backup

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

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

**Important:**

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

## CMS Supervisor

CMS Supervisor provides access to CMS reports and administration. It is available through the following interfaces:

- Web Client: A browser-based interface installed with the CMS server software. You do not need to install any software on individual PCs.
- PC Client: A Windows-based interface that must be installed on each user's PC.
- Mobile Client: An iPad application that enables supervisors and operations managers to monitor call center activity while 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

Avaya supports deploying CMS KVM on either an Avaya Solutions Platform 130 R6 server (ASP 130 R6) or a customer-provided server.

For new installations and upgrades, you can deploy CMS as a virtual machine on ASP 130 R6 servers. Avaya supplies these servers pre-installed with Linux R8.10 and configured to support KVM virtual machine deployment.

The CMS OVA file, usable for deploying CMS as a VMware virtual machine, is still supported for installation on customer-provided servers.

## Networking with IPv4 or IPv6

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

The CMS Supervisor Web Client and Mobile Client also support IPv4 and IPv6. CMS integrates with the CMS Supervisor PC Client, the Terminal Emulator, and Network Reporting over IPv4 or IPv6. You do not need to perform additional configuration to enable IPv6 capabilities in CMS reporting client applications. IPv6 protocol, name resolution, and connectivity are automatic. The use of IPv6 is transparent to CMS users. All CMS features work 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 WebLM on a co-

resident Avaya Aura® System Manager. WebLM licenses must support SHA256 digital signatures and use a 14-character host ID.

**Important:**

Use Centralized licensing for CMS. Enterprise licensing is not supported, which means multiple CMS deployments cannot share a single license file. After enabling Centralized licensing, assign each 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*

**Enhanced Access Security Gateway (EASG):** You can enable or disable EASG. When enabled, EASG enables service engineers to access CMS for troubleshooting. EASG supports permission levels such as init, inads, and craft.

# Local and enterprise login options

CMS supports local and enterprise login options.

### Local login

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

### Enterprise login

- CMS supports authentication through Microsoft Azure and OKTA.
- This option is available only with the CMS Web Client.
- If Microsoft Azure or OKTA is configured for multifactor authentication (MFA), CMS enforces MFA.
- The LDAP package is not required for enterprise login.
- You must have a login ID configured in CMS.
- CMS must be administered to be recognized by Microsoft Azure or OKTA.

CMS also supports login authentication using personal certificates. The method of using personal certificates is required for Joint Interoperability Test Command (JITC) certification. For Federal and Department of Defense employees, Common Access Card (CAC) encodes and provides personal certificates.

CMS does not require certificates to be stored on CACs. Personal certificates can also reside in standard certificate stores, such as the Microsoft Certificate Store.

# Simplified CMS HA configuration

If you have two CMS servers installed, use the simplified command process to configure high availability (HA).

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

When setting up server roles for the first time, ensure you have the details of the CMS server 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 | No | No | Yes |

### 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 | • Windows 10<br>• Windows 11 |
| Google Chrome | • Windows 10<br>• Windows 11<br>• macOS 13 (Ventura)<br>• macOS 14 (Sonoma)<br>• ChromeOS |
| Mozilla Firefox | • Windows 10<br>• Windows 11<br>• macOS 13 (Ventura)<br>• macOS 14 (Sonoma) |
| Apple Safari | • macOS 13 (Ventura): Version 16 and 17<br>• 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 virtual machine. You can do this by backing up the customer data, installing the new CMS server, and then migrating 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 ASP 130 R6 server. You can do this by backing up the customer data, installing the new CMS server, and then migrating the customer data.

- **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 upgrade directly to CMS R21.0 from R16.x, R17.x, R18.x, R19.x and R20.0. Contact your Avaya account team if you need to upgrade from a CMS release older than R16.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 ASP 130 R6 servers.
- Customer-provided VMware servers.
- Customer-provided KVM 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:

- *Deploying Avaya Call Management System*
- *Upgrading 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 VM configuration can support. Select the profile size that provides the capacities you require. If you require a higher capacity for any parameter, upgrade to the larger configuration profile. For example, if you are using a small VM configuration, you must move up to a medium or large 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:**

The 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. The count must be 1600 or less.

## Third-party software

Determine third-party software capacity by counting the number of external or third-party interface applications in use.

Examples of third-party interfaces include Blue Pumpkin, ODBC, wallboards, Geotel, Operational Analyst, TCS, and IEX.

Count each application only once, regardless of how many instances are used.

**Important:**

- Count Geotel as two applications.
- Count wallboards as one application, regardless of the number of wallboards in use.

## Agent/skill pairs

The agent-to-skill pair capacity is the total number of agent-to-skill combinations.

To calculate this capacity, multiply the number of agents by the number of skills each agent is assigned. These values are determined by switch administration settings.

For example, if you have 20 agents and each agent is assigned 5 skills, multiply 20 by 5 to get a total of 100 agent-to-skill pairs.

Ensure that you count all skills assigned to each agent, not just the ones they actively use.

## 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 equals running the Skill Status report with a three-second refresh rate and retrieving 100 rows of data.

You can access the report from **Realtime** > **Split/Skill** > **Skill Status report**.

The Skill Status report includes the following two queries:

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 fields. One field uses a synonym lookup.

Query data2 returns ten fields. In this example, the query returns 100 rows.

Six fields use synonym lookups, and two fields use keyword lookups. Synonym and keyword lookups are approximately twice as resource-intensive as plain data fields.

Adding a summary query increases the load on the CMS.

If you run the Skill Status report with a three-second refresh rate and the report returns 200 rows, it counts as two report elements.

Integrated queries place a higher load on the server when they start. However, after initialization, they retrieve data similar to real-time reports except at interval, day, and start-of-day boundaries.

Historical reports impact server performance 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

The refresh rate for Integrated Report in CMS Supervisor PC is at least 10 seconds. CMS Supervisor Web supports a 3-second refresh rate for the same report.

## Average refresh rate

The average refresh rate capacity refers to the average refresh rate used for real-time reports.

To calculate this capacity, average the refresh rates set by your report users. For example, if half of the users set a 30-second refresh rate and the other half set a 10-second refresh rate, the average refresh rate is 20 seconds.

## Percent refresh rate at three seconds

The percent refresh rate at 3 seconds capacity is the percentage of real-time report users who require data to refresh every 3 seconds.

# Capacity and scalability specifications

Before installing CMS, review the server capacity requirements outlined in this section. You can also find general system capacity information for CMS.

CMS encrypts server/client connections, where the client is the CMS Supervisor PC or Web Client. When FIPS 140-2 encryption is enabled, it uses additional CPU and memory to support more complex ciphers. Therefore, the following CMS capacities are reduced by 10%:

- Concurrent supervisor sessions
- Reports for each supervisor session
- Report elements
- Average refresh rate (30 seconds), including a 10% reduction in the listed 3-second refresh rate capacities

### Capacity requirements for new installations

Select the appropriate profile size for your deployment.

| Parameter | Small | Medium | Large |
|---|---|---|---|
| **Peak busy-hour call volume** | 30000 | 200000 | 400000 |
| **Concurrent CMS Supervisor sessions**[1] | 50 | 200 | 2999 |
| **Concurrent agents** | 500 | 5000 | 10000 |
| **Third-party software** | 3 | 3 | 3 |
| **Agent skill pairs** | 100000 | 200000 | 800000 [2] |
| **Reports per CMS Supervisor session** | 3 | 5 | 10 [3] |
| **Report elements** [4] | 5 | 5 | 12 |
| **Percentage of supervisors that can run reports with a three-second refresh rate** | 10% | 50% | 100% |
| **Active agent traces** | 250 | 1000 | 5000 |
| **Internal Call History (ICH) records - per 20 minutes** | 4000 | 4000 | 4000 |
| **External Call History (ECH) records - per 20 minutes** | 10000 | 60000 | 300000 |

1. You can view the total number of active CMS Supervisor client sessions using this value.
2. If your storage exceeds 800 GB, create additional disk volumes.
3. You can access up to three real-time reports and the specified amount of historical data.
4. To understand the different report elements, see Report elements on page 20.

### System-wide capacities (specific to Avaya Aura® Call Center Elite)

| CMS attribute | System wide capacity | Per ACD maximum capacity |
|---|---|---|
| **Agent skill pair** | 800000 | 360000 |
| **Total VDNs** | 54000 | 30000 |
| **Total splits or skills** | 54000 | 8000 |
| **Total trunks** | 100000 | 30000 |
| **Total trunk groups** | 8000 | 2000 |
| **Total vectors** | 32000 | 8000 |
| **Total call work codes** | 4000 | 1999 |
| **Agent trace records (AAR)** | 5100000 | 5100000 |

### Maximum values (specific to Avaya Aura® Call Center Elite)

| Agent/skill pairs | 300000 | 300000 | 400000 | 500000 | 800000 |
|---|---|---|---|---|---|
| **Interval length (minutes)** | 15 | 30 | 30 | 30 | 30 |
| **Interval data days saved** | 31 | 31 | 15 | 31 | 15 |
| **Daily data days saved** | 730 | 1825 | 1825 | 730 | 730 |

**Note:**

Daily, weekly, and monthly limits remain unaffected. However, when the capacity of agent skill pairs exceeds 2,00,000, there is an impact on the interval data storage.

# CMS reporting efficiency

Use Avaya CMS to create custom reports that meet your specific requirements. However, the performance of the CMS server depends on its available memory and CPU capacity.

## Skill-based reporting

The CMS server is optimized for skill-based reporting. Avaya recommends creating and using reports based on skills rather than Agent Group reports. You can create skills on the Automatic Call Distribution (ACD) system, even if they do not receive actual calls. You can use these skills to provide reports for agents assigned to that skill. To use Agent Group reports, follow the guidance provided in Recommendations for report customization on page 23.

## Recommendations for report customization

When you design and use custom Agent Group reports, follow these recommendations to optimize system performance:

- Agent Groups:
  - Limit agent groups to 99 agents or fewer to maintain system performance.
  - Use consecutive Agent IDs in the same report when possible.
  - Prefer skill-based reports over Agent Group reports when feasible.
- Report Elements:
  - Minimize the number of agents, skills, VDNs, trunks, or other elements in a single report.
  - Review and reduce report complexity.
- Custom Report Design:
  - For historical reports, avoid using multiple dates when querying interval database tables.
  - Modify existing reports to use daily, weekly, or monthly tables instead.
  - Review any historical report that takes longer than a few seconds to complete and optimize it.
  - Review or modify any real-time report that takes more than a few milliseconds to refresh.

## Resources for system performance analysis

You can work with Avaya Professional Services to design and use custom reports that optimize system performance. Avaya Professional Services offers performance analysis for custom reports on a CMS server and provides recommendations to help you design current or future reports efficiently, minimizing impact on CMS performance.

## Changing the dictionary

Make changes to the dictionary during off-hours when database activity is minimal. Otherwise, CMS Supervisor users must repeatedly query the database to update the cache on the computer running CMS Supervisor. This behavior can cause real-time reports to stop functioning and prevent users from accessing CMS Supervisor.

# Traffic specifications

Refer to the **Peak busy-hour call volume** entry in the table under the Capacity requirements for new installations section of Capacity and scalability specifications on page 21.

# Redundancy and high availability

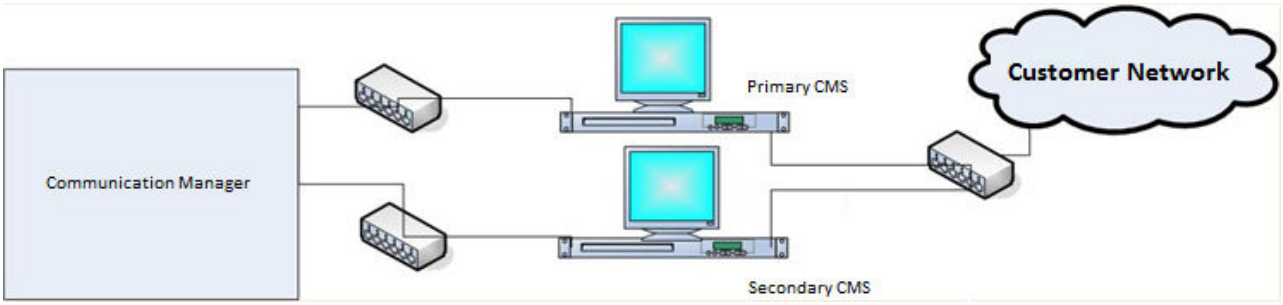
Avaya CMS High Availability (HA) ensures uninterrupted data flow between the communication server or switch and the CMS servers. In an HA configuration, two CMS servers connect to a single communication server or switch. This setup eliminates the traditional single point of failure between the CMS server and the communication server or switch.

Each CMS server independently collects data from the communication server and provides full CMS functionality. If one CMS server fails, loses its connection to the communication server, or must be brought down for maintenance, the other CMS server automatically manages all CMS operations.

Duplicate hardware plays a crucial role in preventing data loss resulting from hardware failures. By eliminating single points of failure, the HA system enhances reliability. The dual ACD link feature addresses potential ACD link failures, while the alternative ACD link improves overall link stability.

A C-LAN circuit pack or Ethernet port provides TCP/IP connectivity between the communication server and the CMS server. Each ACD link requires a dedicated C-LAN circuit pack or Ethernet port, with separate network routes to minimize the risk of failure.

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



# Dial plan specification

CMS supports extensions of up to 16 digits for agents, login IDs, VDNs, and stations.

# 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 measures:

- Patch management and qualification: CMS includes all necessary components, including security patches, in each 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).
- Security logs and audit trails: You can use operating system-level log files to detect suspicious activity. Review these log files routinely to identify unusual behavior.
- Banner modifications: Modify Telnet and FTP service banners to hide operating system details from potential attackers.
- Email and SMTP configuration: Do not configure CMS as a mail relay. Disable the Simple Mail Transfer Protocol (SMTP) daemon.

### Authentication and session encryption

CMS uses the following methods for authentication and session encryption:

- 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. You can administer data permissions for each user within CMS.
- Password complexity and expiration: You can enable and modify password expiration attributes through the CMSADM menu. Set expiration intervals from 1 to 52 weeks.
- Failed login logging: You can log the failed login attempts in the system message log, `syslog`.
- Concurrent login prevention: With the APS hardening offer, you cannot log in more than once concurrently.
- Secure login using SSH: CMS simplifies the installation of a secure Supervisor client login over public or unsecured networks using Secure Shell (SSH). This protocol encrypts packets between the client workstation and host server, securing login credentials 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 for handling personal data. For example, the European Union issued the General Data Protection Regulation (GDPR), and the State of California created the California Consumer Privacy Act (CCPA). To support these policies, CMS encrypts personal data at rest and in transit. CMS also 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 data in transit can be encrypted between CMS and its connected ACD systems. CMS encrypts the SPI link automatically when you administer the connection between systems. This encryption is invisible to the user.

Encryption of personal data in transit is available with CMS Release 19.1 and later, as well as 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 also 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 ensures services security and CMS support through remote connectivity, authentication, and password management for services.

### Personal data in CMS

CMS stores the following types of personal data:

- Information about call center agents.
- Information about CMS users.
- Phone numbers dialed by individuals placing calls into the call center.
- Phone numbers dialed by agents placing calls outside the call center.

The agent and user information applies to company employees who use CMS. CMS stores only the personal data required to support standard employee operations.

For callers and agents, CMS stores only the dialed digits.

You can use CMS logs and tools to manage personal data. For more information, see *Maintaining and Troubleshooting Avaya Call Management System*.

# General Data Protection Regulation support

The European Union (EU) established the General Data Protection Regulation (GDPR) to enhance and unify data protection laws for individuals throughout the EU. If your organization processes personal data of individuals in the EU, GDPR applies to you.

GDPR affects daily operations in departments within organizations that act as data controllers. The regulation regards data controllers as entities that collect personal data from data subjects.

CMS stores several categories of personal data, including information about call center agents, CMS users, and individuals who contact the center.

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

# Certificates for secure communication

CMS uses certificates to enable secure communication in the following components:

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

## Web Client encryption

To encrypt communication between browsers and the Web Client CMS server, install a security certificate.

For 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 integrates with CMS to provide secure authentication and auditing for remote access to maintenance ports. EASG authentication

uses a challenge-response algorithm based on a token-based private key-pair cryptographic authentication scheme. You can view logs that include successful and failed login attempts, errors, and exceptions.

Service engineers can use EASG to access customer products. EASG supports permission levels such as init, inads, and craft.

On the CMS server, a dedicated EASG product certificate is installed in the `/etc/asg` directory. Use this directory for all associated files. The certificate uniquely identifies major CMS releases to the Avaya EASG server.

CMS derives the product certificate from the Avaya IT Root Certificate Authority (CA) and intermediate CAs. The Avaya EASG server uses these CAs to generate a response. CMS verifies the response using the public key in the EASG product certificate through the EASG Common Red Hat Package Manager (RPM). The CMS deployment includes the product certificate, so you do not need to perform any additional certificate configuration tasks.

## LDAP connection encryption

You can use LDAP Active Directory in CMS to manage users. To avoid exposing personal data, encrypt the connection to the Active Directory server. Encryption of the LDAP connection requires setting up a certificate.

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 CMS network ports 50000 and 50001 to support Informix TLS and SSL encryption. These ports also support Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) connections. To enable TLS and SSL encryption, install a PKCS #12 certificate.

For 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

In the SPI link, ACD acts as the server and CMS as the client. You do not need to configure any additional certificates on the CMS client.

# Setting up the Secure Access Link and Alarm Monitoring system

Avaya uses Secure Access Link (SAL) as the default method for remote access. SAL enables Avaya personnel to do the following:

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

Use the following steps to create a new registration or onboard technical personnel using the Global Registration Tool (GRT):

1. Go to https://support.avaya.com/.
2. Log in with your username and password.
3. On the home page, click **Diagnostics & Tools**, then select **Global Registration Tool**.
4. On the Create A New Registration page, choose one of the following options:
   - **End to End Registration**
   - **Technical Onboarding Only**
5. Enter the 10-digit functional location number or sold-to number for the customer.

   Include leading zeroes. For example, if the location number is 12345678, enter it as 0012345678.

**Note:**

If the customer has already completed product registration, complete only the Technical Onboarding process to enable SAL connectivity.

To complete product registration and prepare for technical onboarding, including SAL connectivity, identify which product material codes are eligible for onboarding. Refer to the GRT Tool Mapping table for a list of supported product material codes.

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 file as a Microsoft Excel spreadsheet for future reference.

# Port utilization

The *Port Matrix for Avaya Call Management System* document lists all ports and protocols used by CMS. To access the document, sign in to the Avaya Support site at https://support.avaya.com/support/en/public with valid credentials and navigate to **Product Support** > **Documents**.

# Chapter 6: Licensing requirements

## CMS agent licensing enforcement

To comply with Avaya policy, ensure that the number of CMS agent licenses for simultaneously logged-in ACD agents is equal to or greater than the number of agent licenses configured in the ACD.

**Important:**

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

The total number of simultaneously logged-in ACD agents is cumulative across all ACDs monitored by CMS. For example, if CMS monitors two ACDs with 400 simultaneously logged-in measured agents each, you must license CMS for 800 simultaneous agents.

The agent licenses on CMS depend on the number of simultaneously logged-in agents, not the number of administered agents. CMS can report on all logged-in or staffed call center agents for any ACD it monitors. For example, if agent Angela Smith leaves the company, CMS continues to report on her formerly assigned Agent Login ID. However, because Angela is an inactive agent, she does not count toward the number of simultaneously logged-in agents.

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 Avaya CMS licenses. WebLM helps you track and manage licenses efficiently. To use WebLM, download 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 32
CMS license modes on page 32
License management on page 33
License enforcement on page 34
License log file on page 38

Alarms on page 38
Backing up and restoring WebLM on page 39

# 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 a High Availability (HA) or Survivable CMS (including dual-role systems)

- HA or Survivable system

  CMS application running on an HA or Survivable system uses the HA feature license, 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 apply to primary and HA or Survivable CMS systems.

  ODBC and JDBC access is available on the primary CMS and an HA or Survivable CMS. You require separate ODBC and JDBC licenses for each CMS in the deployment.
- Number of Command Line Interface (CLInt) external sessions
- Number of CLInt internal sessions

# CMS license modes

CMS operates in three license modes:

- License Normal
- License Error
- License Restricted

The logs record transitions between these modes and generate alarms when entering the License Error or License Restricted mode.

### License Normal mode

The License Normal mode indicates that there are no license violations. In this mode:

- The CMS instance connects to WebLM.

- The CMS instance shares the latest license information.

### License Error mode

The License Error mode indicates a license violation. In this mode, CMS performs the following actions:

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

If the CMS instance remains in the License Error mode for more than 30 days, CMS performs one of the following actions:

- Attempts to resolve the violations.
- Transitions to the License Restricted mode, depending on the nature of the violations.

When the CMS instance clears all license violations for eight consecutive days, CMS returns to the License Normal mode.

### License Restricted Mode

When CMS enters the License Restricted mode, the CMS instance enforces the following restrictions:

- Closes and blocks all user interface sessions.
- Enables limited access through the ASCII interface:
  - The cms user can access only the System Setup and Maintenance submenus.
  - The cmssvc user can access the Services submenu in addition to System Setup and Maintenance.
- Closes all external and internal CLInt sessions and prevents new CLInt sessions from starting.
- Closes all JDBC and ODBC sessions and blocks new sessions.
- Stops External Call History.

After the CMS instance clears all license violations, CMS returns 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:

- Retrieve the newest license information from WebLM.
- Retrieve the number of ACDs and renew, acquire, or release ACD licenses.
- Retrieve agent login information and renew, acquire, or release agent licenses.
- Retrieve supervisor login information and renew, acquire, or release supervisor licenses.
- Retrieve CLInt usage information and renew or acquire CLInt licenses.
- Retrieve ODBC and JDBC usage information and renew, acquire, or release the ODBC and JDBC session licenses as needed.

- Calculate the license status and perform the following actions:
  - Log to elog on detection of a new license violation.
  - Log to elog when the license status changes.
  - Log the current license status.
- Take appropriate action based on the calculated license status.

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

# License enforcement

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

- License Validity
- ACD Count
- Agent Count

The CMS instance remains in the License Restricted mode until all violations are resolved.

Other licenses, such as Supervisor Session Count, JDBC or ODBC Session Count, and CLInt Session Count, can trigger the CMS instance to enter the License Error mode if violated. However, the License Error mode does not cause the CMS instance to enter the License Restricted mode. Instead, the CMS instance attempts to resolve the error by disconnecting sessions that exceed the licensed count.

## License validity

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

- CMS cannot connect to WebLM.
- CMS connects to WebLM but cannot obtain a license.
- The CMS license has expired.
- The CMS license version is older than the running CMS version.

If CMS cannot initially obtain a license, the system ignores maximum capacity limits. Otherwise, it uses the previous capacities. If the license has expired or is incorrectly versioned and no previous capacities exist, the system uses the capacities specified in the invalid license.

## ACD count

When you create an ACD, CMS ensures the total number of ACDs does not exceed the licensed limit. If you reduce the licensed ACD count, CMS enters the License Error mode. Remove the extra ACDs within 30 days to avoid restrictions. Otherwise, CMS enters the License Restricted mode. To resolve the issue, remove the extra ACDs or update the license to include more ACDs.

**Note:**

The ACD count includes all administered ACDs, not just active ones. Even if data collection is off or the link is down for an ACD, the system counts the ACD towards the limit. The system does not include the pseudo ACDs in the ACD count.

Administered ACDs consume licenses even when CMS is not running. However, CMS does not report license usage to WebLM when CMS is not running.

To clear the ACD license violation, do the following:

- Remove ACDs to match 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 automatically if the number of agents remains below the limit for eight consecutive days.

For example, if the number of agents exceeds the limit on days 1, 4, and 7, CMS clears the error on day 16, provided no violations occur between days 7 and 16.

If the system does not clear the violation within 30 days, CMS enters the License Restricted mode upon the subsequent violation. For instance, if violations occur on days 1, 7, 14, 21, 28, and 33, CMS enters the License Restricted mode on day 33.

CMS returns to the License Normal mode if:

- No violations occur between days 33 and 41.
- The system updates the CMS license to include an increased agent count, ensuring no further violations occur.

In summary, you can clear an agent license violation if:

- No violations occur for eight consecutive days.
- You update the CMS license with an increased agent count.

## Supervisor session count

When a supervisor logs in, CMS checks the current session count against the licensed limit. If the session count exceeds the limit, the system blocks the login to prevent overuse.

In rare instances, if the system decreases the licensed count and the current sessions exceed the new limit, CMS enters the License Error mode.

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

## ODBC and JDBC session count

CMS cannot block excessive ODBC and JDBC sessions. If the number of sessions exceeds the licensed count, CMS enters the License Error mode. The violation clears automatically if the session count stays below the limit for 8 consecutive days after the last violation.

If you do not clear the violation within 30 days, CMS remains in the License Error mode and randomly ends ODBC and JDBC sessions to stay within the threshold. After you clear the license

violation and no further violations occur for 8 consecutive days, CMS returns to the License Normal mode.

## CLInt session count

CLInt sessions use two types of counts:

- External use: Used by non-CMS applications.
- Internal use: Used by CMS applications such as RTA and ECH_handler.

For example, the following command applies to the external count:

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

You can run the `clint` program only if either of the counts is greater than zero (0). The session count applies only to real-time reporting. When a CLInt session starts a real-time report, the system requests a license. The session ends after the license limit is reached.

## License enforcement with different license modes

The following table shows how CMS enforces licensing for various features across different licensing modes:

| Feature | Normal Mode | Error Mode occurs when | Violation clears when | If Error Mode continues for 30 days | Restricted Mode behavior |
|---|---|---|---|---|---|
| **WebLM Licensing** | CMS receives a valid license from WebLM. | • CMS cannot access WebLM.<br>• CMS cannot get a license from WebLM.<br>• CMS version is wrong.<br>• CMS license has expired. | CMS receives a valid license from WebLM. | System enters Restricted Mode. | • All CMS Supervisor, CLInt, ODBC, and JDBC sessions end.<br>• Only cms and cmssvc logged-in users can access CMS through the ASCII interface. Only the Setup, Maintenance, and Services sub-menus are available.<br>• New CLInt, ODBC, and JDBC access are blocked.<br>• Data collection continues.<br>• ECH data recording stops. |
| **ACD Count** | You can add ACDs if within the licensed limit. | The licensed count is reduced below the number of existing ACDs. | You remove excess ACDs or increase the licensed count to match the existing ACD count. | System enters Restricted Mode. | Same as above. |
| **Agent Count** | Monitor agent logins. | Agent logins exceed the licensed count on a given day. | The licensed count does not exceed for 8 consecutive days, or the count is increased. | System enters Restricted Mode upon next violation. | Same as above. |

*Table continues…*

| Feature | Normal Mode | Error Mode occurs when | Violation clears when | If Error Mode continues for 30 days | Restricted Mode behavior |
|---|---|---|---|---|---|
| **CMS Supervisor Session Count** | CMS Supervisor logins are enabled up to the licensed count. | The licensed count is reduced below the number of logged-in CMS Supervisor users. | CMS Supervisor users log off, and the number of logged-in users is within the licensed count. | All CMS Supervisor sessions end. CMS Supervisor users must log in again. | NA |
| **ODBC and JDBC Session Count** | ODBC and JDBC sessions are within the licensed count. | ODBC and JDBC sessions exceed the licensed count. | The licensed count does not exceed for 8 consecutive days. | ODBC and JDBC sessions end randomly until within the licensed count. | NA |
| **CLInt Session Count** | CLInt sessions running real-time reports end if the sessions exceed the licensed count. | The CLInt license limit is reduced below the existing number of CLInt sessions. | CLInt sessions end within the licensed count. | All CLInt sessions end. Users must restart sessions. | NA |

# License log file

CMS saves the licensing log file at 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 alarms either through a socket connection or an SNMP agent to INADS. Also, the system may forward alarms to the network management system of the customer.

CMS supports the following three alarm levels:

- Warning
- Minor
- Major

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

# Backing up and restoring WebLM

You can back up or restore the current license state of the CMS instance. To recover from a critical failure, restart the CMS instance. CMS retrieves license data from WebLM to determine the license state.

# Chapter 7: Resources

## Documentation

### CMS and CMS Supervisor documents

| Title | Description | Audience |
|---|---|---|
| **Overview** | | |
| *Avaya Call Management System Overview and Specification* | Describes tested product characteristics and product capabilities including feature descriptions, interoperability, performance specifications, security, and licensing requirements. | All users |
| **Installation and maintenance** | | |
| *Deploying Avaya Call Management System* | Describes how to install and configure CMS in a virtualized VMware or KVM environment. | Implementation engineers, administrators |
| *Deploying Avaya Call Management System in an Infrastructure as a Service Environment* | Describes how to deploy CMS in an Amazon Web Services or Google Cloud Platform environment. | Implementation engineers, administrators |
| *Maintaining and Troubleshooting Avaya Call Management System* | Describes how to configure, maintain, and troubleshoot CMS. | Administrators, support personnel |
| *Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting* | Describes how to connect and administer the Automatic Call Distribution (ACD) systems used by CMS. | Administrators, installation personnel, support personnel |
| *Avaya Call Management System High Availability Connectivity, Upgrade and Administration* | Describes how to connect to HA servers and upgrade to HA. | Administrators, installation personnel, software specialists involved with HA |
| *Using Avaya Call Management System High Availability and Admin-Sync* | Describes how to install and maintain your CMS High Availability (HA) system. | Administrators, support personnel |
| **Upgrading** | | |

*Table continues…*

| Title | Description | Audience |
|---|---|---|
| *Upgrading Avaya Call Management System* | Describes the procedures required to upgrade to a new CMS release. This document is focused on full software or platform upgrades. | System administrators, implementation engineers |
| *Avaya Call Management System Base Load Upgrade* | Describes how to perform a simplified base load upgrade. You can perform a base load upgrade within a CMS release or for other approved scenarios. Not all releases support base load upgrades. | System administrators, implementation engineers |
| **Administration** | | |
| *Administering Avaya Call Management System* | Provides instructions on administering a call center using CMS Supervisor. | Avaya support personnel, Administrators |
| *Avaya Call Management System Call History Interface* | Describes the format of the Call History data files and how to transfer these files to another computer. | Administrators, supervisors |
| *Using ODBC and JDBC with Avaya Call Management System* | Describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS. | Administrators, support personnel |
| *Avaya Call Management System Database Items and Calculations* | Describes each database item and calculation that CMS tracks and how CMS calculates the values displayed on CMS reports and CMS Supervisor reports. | Administrators, support personnel |
| *Avaya Call Management System Custom Reports* | Describes how to design and create custom reports in CMS. | Administrators, report designers |
| *Avaya Call Management System Security* | Describes how to implement security features in CMS. | Administrators, support personnel |
| **CMS Supervisor** | | |
| *Avaya CMS Supervisor Clients Installation and Getting Started* | Describes how to install and configure CMS Supervisor. | Implementation engineers, system administrators |
| *Avaya CMS Supervisor Reports* | Describes how to use CMS Supervisor reports. | Supervisors, administrators |
| *Avaya CMS Supervisor Report Designer* | Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard. | Supervisors, administrators |

### Avaya Solutions Platform Documents

| Title | Description | Audience |
|---|---|---|
| *Avaya Solutions Platform Overview and Specification* | Describes the key features of Avaya Solutions Platform server | All users |

*Table continues…*

| Title | Description | Audience |
|---|---|---|
| *Installing the Avaya Solutions Platform 130 Series* | Describes how to install Avaya Solutions Platform 130 Series servers. | Implementation engineers, solution architects, support personnel |
| *Maintaining and Troubleshooting Avaya Solutions Platform 130 Series* | Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers. | Implementation 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.

# 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.

# 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