Avaya Call Management System Overview and Specification

Release 19.0
Issue 3
April 2020

© 2019-2020, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Hosted Service

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

Licenses

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

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

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

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

Heritage Nortel Software

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

for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. 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

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies 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

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER. WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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 for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.
Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

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

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

Issue	Date	Summary of changes
3	April 2020	Added requirement that you must use WebLM 8.0 or later. This appears in several places in the document.
2	October 2019	Updated the agent licensing description in CMS agent licensing enforcement on page 32.

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

Warranty

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

For information about the standard Avaya warranty and support for Call Management System during the warranty period, see the Avaya Support website at http://support.avaya.com/ in **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Overview

An overview of CMS

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

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

CMS stores ACD data in a real-time and a historical database. 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 the intrahour, daily, weekly, and monthly data. The historical database can store 370 days of intrahour historical data, 5 years or 1825 days of daily historical data, and 10 years or 520 weeks of weekly and 120 months of monthly historical data.

CMS provides two options for contact center data resiliency:

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

This flexible and scalable software is ideal for small single location contact centers, large multilocation applications, or contact centers of similar sizes. You can use CMS to analyze the performance of a single agent, a specific skill, or a large number of 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. Using CMS Supervisor, managers can monitor, in real time, any area of contact center performance, such as the number of abandoned calls, average hold time, and number of calls in a queue. CMS also includes the CMS Supervisor Web feature to monitor contact center performance and activity with a web browser. The CMS Supervisor PC Client and Web Client support interfaces in several languages.

New in this release

The following are new features for CMS Release 19.0:

- Added support of LDAP integration.
- Added support of Enhanced Access Security Gateway (EASG).
- Added support for feature licensing through Product License Delivery System (PLDS) and CMS integration with WebLM Release 8.0 or later.
- Added support on RedHat Linux 7.6 OS.
- Added support for Avaya Aura® Communication Manager 8.0.
- Removed support for Avaya Aura® Communication Manager 5.2.
- Removed support for non-EAS ACDs. Non-EAS ACDs can no longer be configured on new installations of CMS. Existing non-EAS ACDs can be migrated to 19.0.
- Changed the ECH file format to add new fields. For more information about ECH, see *Avaya Call Management System Call History Interface*.
- Increased the interval table storage limit from 62 days to 370 days.

CMS feature summary

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

Reporting

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

CMS stores all the ACD data received from a Communication Manager 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 the intrahour, daily, weekly, and monthly data.

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*
- *Avaya Call Management System Administration*
- *Avaya CMS Supervisor Reports*

CMS Supervisor Mobile Client

CMS Supervisor Mobile Client is an Apple iPad application that provides access for CMS reports and administration. The Mobile Client helps supervisors and operations managers of a contact center to monitor the agents and the health of the contact center when they are away from their desks.

For more information about the Mobile Client, see the following documents:

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

CMS Supervisor PC Client

CMS Supervisor PC Client is a Windows-based interface for CMS reports and administration. To use the PC Client, you must install the client software on all user PCs.

ACD administration

CMS provides an administrative interface to Communication Manager systems. Using CMS Supervisor, you can view or change parameters related to ACDs, call vectoring, and Expert Agent Selection (EAS) on a Communication Manager system. 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.

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

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.

Networking with IPv4 or IPv6

CMS supports both IPv4 and IPv6 connectivity. The integration between CMS and Communication Manager over IPv4 or IPv6 is seamless. You can configure IPv4 or IPv6 connections with Communication Manager by using the **cmsadm** command and `acd_create` option whether you are using IPv4 or IPv6. Whichever configuration you use, you must consistently use the IPv4 or IPv6 addresses.

CMS Supervisor Web Client and Mobile Client can also use either IPv4 or IPv6. CMS also 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 and name resolution, and connectivity is automatic. Use of IPv6 is transparent to CMS users. All features of CMS work exactly the same with IPv6 as they do with IPv4.

Communication Manager 8.0 support

Communication Manager 8.0 provides the following additional features:

- Maximum 16 digits in agent login IDs, VDN extensions, and station extensions.
- Maximum 30,000 measured trunks for each Communication Manager instance.

To access the new features, you must administer the CMS link to Communication Manager as Communication Manager 8.0.

Avaya Converged Platform

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

LDAP integration support

CMS supports the use of Lightweight Directory Access Protocol (LDAP) integration for CMS user management. CMS supports Active Directory for the Windows Server 2008, 2008 R2, 2012, and 2012 R2 versions.

You can administer both traditional CMS users (Linux) and LDAP authenticated users with the CMS. When you activate the LDAP feature, the system updates the existing CMS User Data screen to provide an interface and identify the LDAP authenticated users. Once you administer a CMS user, the user gains access to CMS.

With the LDAP integration, CMS users can log on to all CMS interfaces, including:

- CMSASCII interface
- CMS Supervisor PC client
- CMS Supervisor Web client

Note:

The CMS User ID maps to the Active Directory user or person **objectClass: sAMAccountName** field. In CMS, the maximum user ID size is 8 characters. To use the LDAP feature, the **sAMAccountName** field must align with this the maximum 8 character length.

EASG

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

EASG authentication is based on a challenge/response algorithm using a token-based private key-pair cryptographic authentication scheme. Secure auditing is also provided. Logs are available that include information such as successful log on, failed log on, errors, and exceptions.

EASG allows Avaya to control Avaya service engineer privileges when accessing customer products. EASG controls permission levels, such as init, inads, and craft, used by the service engineers.

On a CMS server, a dedicated EASG product certificate is installed under the EASG directory `/etc/asg`. This is mandatory that all Avaya products with EASG support use the `/etc/asg` directory for all EASG associated files and directories. 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 RPM. The EASG product certificate is included in the CMS deployment. Customers need not do additional tasks to set up the certificate.

WebLM and PLDS support

Using the PLDS feature, CMS gets license information through WebLM Release 8.0 and later and enforces the license agreement through WebLM.

Chapter 3: Interoperability

Product compatibility

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

Communication Manager release	CMS software release				
	16.x	17.x	18.0	18.1	19.0
5.2	Yes	Yes	Yes	Yes	No
6.x	Yes	Yes	Yes	Yes	Yes
7.x	Yes	Yes	Yes	Yes	Yes
8.x	No	No	No	Yes	Yes

Supported CMS server releases for CMS Supervisor

CMS Supervisor 19.0 supports connections to the following CMS server releases:

- 15.x
- 16.x
- 17.x
- 18.x
- 19.x

Supported CMS software

CMS 19.0 uses the following software packages:

- Informix IDS
- Informix ESQL SDK
- Informix ILS
- CMS Supplemental Services
- CMS
- ODBC and JDBC

  For specific software version information, see *Maintaining and Troubleshooting Avaya Call Management System*.

Operating system compatibility

Operating system compatibility for the CMS server

CMS server software is compatible with Red Hat Enterprise Linux® (RHEL) 7.6.

Operating system compatibility for CMS Supervisor Web client

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

- Microsoft Internet Explorer
  - Windows 7: version 10, 11
  - Windows 8.1: version 11
  - Windows 10: version 11
- Microsoft Edge
  - Windows 10: version 39, 40
- Mozilla Firefox
  - Windows 7: version 60, 61
  - Windows 8.1: version 60, 61
  - Windows 10: version 60, 61
  - OS X 10.12 (Sierra): version 60, 61
  - OS X 10.13 (High Sierra): version 60, 61
- Google Chrome
  - Windows 7: version 67, 68
  - Windows 8.1: version 67, 68
  - Windows 10: version 67, 68
  - OS X 10.12 (Sierra): version 67, 68
  - OS X 10.12 (High Sierra): version 67, 68
  - ChromeOS: version 67, 68
- Apple Safari
  - OS X 10.12 (Sierra): version 10, 11
  - OS X 10.13 (High Sierra): version 11

Note:

Running reports in CMS Supervisor Web requires Adobe Flash support.

Windows compatibility for the CMS Supervisor PC Client

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

- Windows 8.1
- Windows 10 version 1803 and later

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 — Upgrading from an older CMS software release and retaining 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, then migrate the customer data.
- Platform Upgrades — Upgrading from an older CMS software release and installing a new VMware server, either a customer-provided server or an Avaya Converged Platform 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, then migrate the customer data.

For more information about upgrades on VMware systems, *Deploying Avaya Call Management System*.

Software upgrades

The software upgrade process reuses existing CMS hardware that can support the new CMS 19.0 software. The following models of hardware support CMS 19.0, regardless of their current CMS release:

- Avaya Converged Platform VMware servers
- Customer-provided VMware servers
- Dell R630
- Dell R730
- HPE DL20 G9
- HPE DL380 G9

For information about doing a software upgrade, see *Planning for Avaya Call Management System Upgrades* and *Upgrading Avaya Call Management System* .

Platform upgrades

CMS 19.0 supports platform upgrades from CMS 15.x, 16.x ,17.x and 18.x, regardless of what hardware the CMS software currently resides.

Note:

Contact your Avaya account team if you need to upgrade from CMS releases older than 15.x.

For information about platform upgrades, see *Planning for Avaya Call Management System Upgrades* and *Upgrading Avaya Call Management System* .

Base load upgrades

Note:

Base Load upgrades cannot be used to upgrade to CMS 19.0.

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

Peak Busy Hour call volume

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

Calculate the busy hour call volume by adding each trunk seizure or line 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

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

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

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

Active agent traces

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

Integrated Report refresh rate

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

Average refresh rate

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

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

Percent refresh rate at three seconds

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

Capacity and scalability specifications

Important:

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

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

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

Capacities for new installations on VMware

The following table lists the capacities for new customer-provided VMware servers or Avaya-provided Avaya Converged Platform servers being sold for CMS:

Parameter	Small	Medium	Large
Peak busy-hour call volume	30,000	200,000	400,000
Concurrent Supervisor sessions[1]	50	200	1,600[2]
Concurrent agents	500	5,000	10,000
Third-party software	3	5	7
Agent skill pairs	100,000	200,000	800,000[3]
Reports per Supervisor session	3	5	10
Report elements	5	5	12
Percentage of supervisors that can run reports with a three-second refresh rate	10%	50%	100%
Active agent traces	250	1,000	5,000
Internal Call History (ICH) records	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

Capacities for upgrades on supported older hardware

The following table lists the capacities for existing platforms being upgraded to CMS 19.1. Only Dell R630, Dell R730, HPE DL20 G9, and HPE DL380 G9 systems can be upgraded to CMS 19.1.

Capacity	CMS Low End Hardware Platform (HPE DL20)	CMS Midsize Hardware Platform (Dell R630)	CMS High End Hardware Platform (Dell R730 and HPE DL380 G9)
Peak busy-hour call volume	10,000	200,000	400,000
Concurrent supervisors[4]	30	200	1,600[5]
Concurrent Agents	400	5,000	10,000
Third-party software	3	3	7
Agent skill pairs	100,000	200,000	800,000
Reports per Supervisor session	5	5	10

Table continues…

1 This value is the total number of active CMS Supervisor PC client and CMS Supervisor Web client sessions.
2 Of the 1600 sessions supported, only 800 can be CMS Supervisor Web client sessions
3 Supporting 800,000 agent skill pairs requires greatly increased disk space for interval data. Customers should create up to 8 additional disk volumes.
4 This value is the total number of active CMS Supervisor PC client and CMS Supervisor Web client sessions.
5 Of the 1,600 sessions supported, only 800 can be CMS Supervisor Web client sessions.

Capacity	CMS Low End Hardware Platform (HPE DL20)	CMS Midsize Hardware Platform (Dell R630)	CMS High End Hardware Platform (Dell R730 and HPE DL380 G9)
Report elements	5	5	12
Active agent traces	200	1,000	5,000
30 seconds Average refresh rate	10% at 3 seconds	50% at 3 seconds	100% at 3 seconds
Internal Call History (ICH) records	4,000 per 20 mins	4,000 per 20 mins	4,000 per 20 mins
External Call History (ECH) records	300,000 per 20 mins	300,000 per 20 mins	300,000 per 20 mins

System wide capacities

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

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 Communication Manager. You can use these skills to provide reporting for the agents that are placed in that skill. To use Agent Group reports, follow the recommendations provided in Recommendations for custom reports on page 32.

Recommendations for custom reports

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

- Agent Groups
  - The size of agent groups are recommended to be 99 agents or less. Agent groups of size 99 agents or less are recommended because system performance can be adversely affected.
  - 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 22.

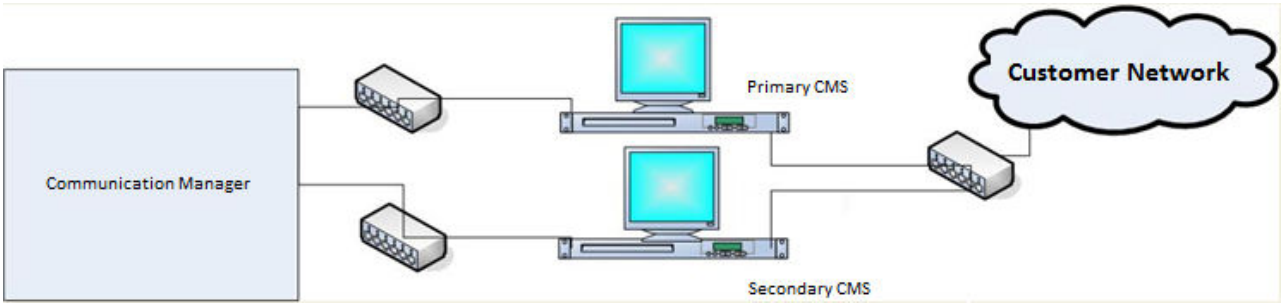
Redundancy and high availability

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

CMS provides the following security features for secure operation:

- Operating system hardening

  CMS achieves operating system hardening by the following procedures:

  - Patching and patch qualification: CMS includes all necessary components including security patches at the time of release. Avaya receives additional patch notifications and certifies new Linux® OS patches. Avaya then assembles these patch clusters and makes the clusters available to customers through Product Change Notices (PCN).
  - Operating System-level security logs and audit trails: You can use log files to detect suspicious system activity. The customer can review these log files on a routine basis for signs of unusual activities. For more information, see CMS Security.
  - Banner modifications: Altering the telnet and ftp network service banners hides operating system information from individuals who want to take advantage of known operating system security holes.
  - Email and SMTP: You must not configure CMS as a mail relay and must disable the Simple Mail Transfer Protocol (SMTP) daemon.

  Note:

  For details on FIPS 140-2 encryption, refer to *Maintaining and Troubleshooting Avaya Call Management System* and *Avaya Call Management System Release Notes*.

- Authentication and session encryption

  CMS achieves authentication and session encryption by the following procedures:

  - User authentication and authorization: CMS uses login and password security measures provided by Linux® OS and provides multiple levels of system access. To authenticate users, CMS uses OS capabilities based on Pluggable Authentication Modules (PAM). At the system level, CMS uses the standard UNIX permissions. In CMS, you can administer data permissions for each user.
  - Password complexity and expiration: You can enable and modify the password expiration attributes through the CMSADM menu. You can set the expiration intervals from 1 to 52 weeks.
  - Logging for failed logins: You can log the failed login attempts in the system message log, `syslog`.
  - Multiple login prevention: With the APS hardening offer, you cannot log in more than once concurrently.

  - Use of ssh: CMS provides a simplified installation of secure Supervisor client login over a public or unsecured network. To do this installation, CMS uses Secure Shell (SSH), a protocol that encrypts the packets sent between a client workstation and a host server. This procedure secures the transmission of login information and other sensitive data.

- Application security

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

- Physical security

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

- Services security and CMS support

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

- GDPR (General Data Protection Regulation)

  CMS stores several categories personal data, Call Center Agent information, CMS User information, and some very limited information about individuals calling into the contact center. The Call Center Agent information and CMS User information is for employees of the company utilizing CMS. The type of personal data is limited to that information that facilitates standard employee work operations.

General Data Protection Requirement (GDPR) 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 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 some limited information about individuals calling into the contact center.

For more details about GDPR, see *Avaya Call Management System Data Privacy Controls Addendum*.

EASG

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

EASG authentication is based on a challenge/response algorithm using a token-based private key-pair cryptographic authentication scheme. Secure auditing is also provided. Logs are available that include information such as successful log on, failed log on, errors, and exceptions.

EASG allows Avaya to control Avaya service engineer privileges when accessing customer products. EASG controls permission levels, such as init, inads, and craft, used by the service engineers.

On a CMS server, a dedicated EASG product certificate is installed under the EASG directory `/etc/asg`. This is mandatory that all Avaya products with EASG support use the `/etc/asg` directory for all EASG associated files and directories. 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 RPM. The EASG product certificate is included in the CMS deployment. Customers need not do additional tasks to set up the certificate.

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

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

Chapter 6: Licensing requirements

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 Communication Manager (Avaya Aura® Call Center Elite).

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 (two Communication Manager systems) 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 of the Logged In or Staffed Call Center Agents of any Communication Manager system 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 Communication Manager. In this example, agent Angela does not count as a simultaneously logged in agent.

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

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 41
Alarms on page 41
Backing up and restoring WebLM on page 41

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 ACD connections to Communication Manager 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 Communication Manager 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 CLIint 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 16^{th} 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 can 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 clears itself if the numbers stay below the limit for 8 days since the last violation. If you do not clear the violation within the 30 days, CMS stays in the License Error mode.

The system clears the ODBC and JDBC license violation and CMS switches back to the License Normal mode if there is no violation for 8 days.

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 license modes

The following table lists the features with the License Enforcement and error 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 getting valid license from WebLM	• Cannot access WebLM • Cannot get CMS license from WebLM • Wrong CMS version • CMS License expired	CMS getting valid license from WebLM	Enter Restricted Mode	• All Supervisor, external CLInt, JDBC/ ODBC sessions terminated • Access to CMS restricted to cms and cmssvc logins via the ASCII interface. Only Set up, Maintenance and Services submenus are available. • New CLInt access blocked • New JDBC/ ODBC access interrupted. • 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	• All Supervisor, external CLInt, JDBC/ ODBC sessions terminated • Access to CMS restricted to cms and cmssvc logins via the ASCII interface. Only Set up, Maintenance and Services submenus are available. • New CLInt access blocked • New JDBC/ ODBC access interrupted. • 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
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	• All Supervisor, external CLInt, JDBC/ ODBC sessions terminated • Access to CMS restricted to cms and cmssvc logins via the ASCII interface. Only Set up, Maintenance and Services submenus are available. • New CLInt access blocked • New JDBC/ ODBC access interrupted. • Data collection continues • ECH data recording stops.
Supervisor Session Count	Supervisor logins are denied if the licensed count is reached.	Licensed count is lowered below the existing number of logged in Supervisors	Supervisors log off and logins are at or below the licensed count	All Supervisor sessions are terminated; Supervisors must re-login	NA

Table continues…

Feature	Normal Mode	Error Mode Occurs When…	Violation Clears Itself When…	If Error Mode Continues for 30 days...	Restricted Mode Behavior
JDBC/ODBC Session Count	JDBC/ODBC sessions are at or below the licensed count	Sessions exceed the licensed count	Licensed count is not exceeded for 8 consecutive days	JDBC/ODBC 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.

Third-party components

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

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

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.	Sales engineers, Administrators
Avaya Call Management System Data Privacy Controls Addendum	Describes how personal data is stored and processed by CMS.	Administrators
Design		
Avaya Customer Experience Virtualized Environment Solution Description	Describes the AvayaCustomer Experience Virtualized Environment market solution from a holistic perspective that focuses on the functional view of the solution architecture.	Sales engineers
Installation, upgrades, maintenance, and troubleshooting		
Deploying Avaya Call Management System	Describes how to plan, deploy, and configure CMS on new VMware-based installations.	Avaya support personnel
Deploying Avaya Call Management System on Amazon Web Services	Describes how to plan, deploy, and configure CMS on new Amazon Web Services installations.	Avaya support personnel
Avaya Call Management System Dell® PowerEdge™ R630 and R730 Hardware Installation, Maintenance and Troubleshooting	Describes how to install, maintain, and troubleshoot Dell® servers used with CMS.	Avaya support personnel
Avaya Call Management System HPE DL20 G9 and DL380 G9 Hardware Installation, Maintenance, and Troubleshooting	Describes how to install, maintain, and troubleshoot HPE servers used with CMS.	Avaya support personnel

Table continues…

Title	Description	Audience
Planning for Avaya Call Management System Upgrades	Describes the procedures customers must plan for before and after upgrading to a new CMS release.	Administrators
Upgrading Avaya Call Management System	Describes the procedures required to upgrade to a new CMS release.	Avaya support personnel
Maintaining and Troubleshooting Avaya Call Management System	Describes how to configure, maintain, and troubleshoot CMS.	Avaya support personnel, Administrators
Avaya Call Management System Switch Connections, Administration and Troubleshooting	Describes how to connect and administer the Communication Manager systems used by CMS.	Avaya support personnel, Administrators
Avaya Call Management System High Availability User Guide	Describes how to install and maintain a CMS HA system.	Avaya support personnel, Administrators
Avaya Call Management System LAN Backup User Guide	Describes how to back up your CMS data using a LAN connection to a remote server.	Administrators
Avaya Call Management System High Availability Connectivity, Upgrade and Administration	Describes how to connect to HA servers and upgrade to HA.	Avaya support personnel, Administrators
Avaya Call Management System High Availability User Guide	Describes how to install and maintain your CMS High Availability (HA) system.	Avaya support personnel, Administrators
Administration		
Avaya Call Management System Administration	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
Avaya Call Management System ODBC and JDBC	Describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS.	Administrators
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, Report designers
Avaya Call Management System Custom Reports	Describes how to design and create custom reports in CMS.	Administrators, Operations personnel, Report designers

Table continues…

Title	Description	Audience
Avaya Call Management System Security for Linux®	Describes how to implement security features in CMS running on the Red Hat Enterprise Linux® (RHEL) operating system.	Avaya support personnel, Administrators
CMS Supervisor		
Avaya CMS Supervisor Clients Installation and Getting Started	Describes how to install and configure CMS Supervisor.	Avaya support personnel, Administrators
Avaya CMS Supervisor Reports	Describes how to use CMS Supervisor reports.	Administrators, Operations personnel
Avaya CMS Supervisor Report Designer	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Administrators, Operations personnel, Report designers

Avaya Converged Platform Documents

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

WebLM Documents

Title	Description	Audience
Deploying standalone Avaya WebLM in Virtual Appliance	Deploy the application in virtual appliance environment by using Solution Deployment Manager	Implementation personnel
Deploying standalone Avaya WebLM in Virtualized Environment	Deploy the application in virtualized environment.	Implementation personnel
Deploying standalone Avaya WebLM in Infrastructure as a Service Environment	Deploy the application on cloud services.	Implementation personnel
Deploying standalone Avaya WebLM in Software-Only Environment	Deploy the application in software-only environment.	Implementation personnel
Upgrading standalone Avaya WebLM	Upgrade the application.	Implementation personnel
Administering standalone Avaya WebLM	Do administration tasks	System administrators

VMware Documents

VMware component or operation	Document description	Document URL
vSphere Virtual Machine Administration	Provides information on managing virtual machines in the VMware vSphere Web Client for vSphere 6.0 or later. This document also provides information of the following: • Deploying OVF templates • Configuring virtual machine hardware and options • Managing Virtual Machines	https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-55238059-912E-411F-A0E9-A7A536972A91.html
vSphere Web Client	Provides information on how through a browser vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.	https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vcenterhost.doc/GUID-A618EF76-638A-49DA-991D-B93C5AC0E2B1.html

Note:

If the document description (link) are no longer active, consult VMware for documents associated with the component or operation.

Related links

Finding documents on the Avaya Support website on page 47

Accessing the port matrix document on page 47
Avaya Documentation Center navigation on page 48

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

Avaya Documentation Center navigation

Customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available at Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content using one of the following:
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release.
  - From **Products & Solutions**, select a solution and product, and select the appropriate document from the list.
- Sort documents on the search results page by last updated dated and relevance.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:
  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

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 **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **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 key word or key words 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 the topic. 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.

Related links

Using the Avaya InSite Knowledge Base on page 50

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 http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

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.

Automatic Number Identification

The billing telephone number from which a voice communication or the telephone number originates.

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.

Backup

The process of protecting data by writing the contents of the disk to an archive, such as a tape device, that can be removed from the computer environment and stored safely.

Call Prompting

A switch feature that routes incoming calls based on information supplied by the caller such as an account number. The caller hears an announcement, and the system prompts the user to select from the options listed in the announcement.

Call 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 a Communication Manager 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

M

N

O

P

R

S

T

U

V

W