Avaya Aura® Communication Manager Overview and Specification

Release 7.1.3
Issue 4
May 2018

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named

User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

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

Contents

Chapter 1: Introduction

Purpose

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

This document is intended for anyone who wants to gain a high-level understanding of the product features and functions.

Change history

Issue	Date	Summary of changes
4	May 2018	• Updated the “Scalability” section for Spectre and Meltdown fixes. • Added the “New in Release 7.1.3” section to include Release 7.1.3 features.
3	December 2017	• Added the “New in Release 7.1.2” section to include Release 7.1.2 features. • Updated the “Supported footprints of Communication Manager on VMware” section. • Updated the “Supported footprints of Communication Manager on KVM” section. • Updated the “Supported footprints of Communication Manager on AWS” section.
2	August 2017	• Added the “New in Release 7.1.1” section to include Release 7.1.1 features. • Updated the “Operating System compatibility” section to include Release 7.1.1 updates.
1	May 2017	Initial release.

Chapter 2: Overview

Overview

Communication Manager overview

Avaya Aura® Communication Manager is the open, highly-reliable, and extensible IP Telephony foundation on which Avaya delivers intelligent communications to large and small enterprises. Communication Manager can scale from less than 100 users up to 36,000 users on a single system.

Communication Manager is a core component of the Avaya Aura® platform and the foundation for delivering real-time voice, video, messaging, mobility, and other services. Communication Manager software is part of all the Avaya Aura® editions. This software is available with a single-user licensing fee.

Communication Manager provides centralized call control for a distributed network of gateways and a wide range of analog, digital, and IP-based communication devices. Communication Manager comes with several built-in mobility applications, call center features, advanced conference calling, and E911 capabilities.

With support for SIP, H.323, and other industry-standard communications protocols, Communication Manager provides centralized voice mail and attendant operations to organizations and call centers, across multiple locations.

You can configure Communication Manager as a feature server or as an evolution server.

Feature server

When Communication Manager is configured as a feature server, it supports only SIP endpoints that are registered with Avaya Aura® Session Manager. It uses the IP Multimedia Subsystem half-call model for full application sequencing.

Evolution server

When Communication Manager is configured as an evolution server, it supports both SIP and non-SIP endpoints. It uses the full-call model to provide Communication Manager features to SIP and non-SIP endpoints.

Avaya Aura® overview

Avaya Aura® is a flagship communications solution that uses an IP and SIP-based architecture to unify media, modes, networks, devices, applications, and real-time, actionable presence across a common infrastructure. This architecture provides on-demand access to advanced collaboration services and applications that improve employee efficiency. Avaya Aura® is available under Core or Power Suite Licenses. Each suite provides customized set of capabilities designed to meet the needs of different kinds of users. Customers might mix Core and Power licenses on a single system based on their needs.

The following are some of the capabilities that Avaya Aura® solution provides:

- Support for up to 28 instances of Session Manager and 250,000 users and 350,000 devices
- Support for up to 18,000 H.323 endpoints on a single Communication Manager server and 350,000 SIP endpoints in an enterprise
- Converged voice and video call admission control
- SIP features, including E911, which reports the desk location of the caller
- Avaya Communication Server 1000 SIP networking and feature transparency
- Session Manager SIP routing adaptations
- A central management application, System Manager, for all Avaya Aura® applications and Avaya Communication Server 1000, with single authentication
- Support for Avaya common servers, S8300E server, and customer-provided servers

Features

Administration features

Avaya Aura® Communication Manager supports several administration interfaces for ease of use.

- System Access Terminal: Uses a Command Line Interface(CLI) interface for telephony administration. System Access Control is available through the Avaya Site Administration package. The system-level limit on the number of concurrent System Access Control sessions is 22. This limit is only for login profiles 18 to 69 and not for system logins. A user can have up to 5 concurrent System Access Control sessions.
- System Management Interface: Uses graphical user interface screens for telephony administration. Using System Management Interface, you can perform system management tasks.
- System Manager: Provides central administration for Communication Manager and other Avaya Aura IP Telephony products. Using System Manager, you can deploy, migrate, and upgrade to Communication Manager.
- Solution Deployment Manager: This utility resides in System Manager. With Solution Deployment Manager, you can install the Avaya OVAs and perform administrative activities.

Communication Manager labels each point-to-point session with a globally unique identifier by generating a 128-bit identifier and inserting the identifier in the Global Session ID (GSID) header of the request. To troubleshoot call flows, you can use a tracing tool and filter GSIDs from the relevant logged messages.

For more information on administering the Communication Manager features, see *Administering Avaya Aura® Communication Manager*.

Attendant features

Communication Manager contains many features that provide easy ways to communicate through your telephone system attendant (operator). In addition, attendants can connect to their console (switchboard) from other telephones in your system, thereby expanding the attendant capabilities.

- Attendant backup. The attendant backup feature allows you to access most attendant console features from one or more specially-administered backup telephones. This allows you to answer calls more promptly, thus providing better service to your guests and prospective clients.
- Attendant room status. Communication Manager allows an attendant to see whether a room is vacant or occupied, and what the housekeeping status of each room is.

  Note:

  This feature is available only when you have enhanced hospitality enabled for your system.

- Attendant functions using the Distributed Communications System protocol.
  - Control of trunk group access allows an attendant at any node in the Distributed Communications System to take control of any outgoing trunk group at an adjacent node.
  - Direct trunk group selection allows the attendant direct access to an idle outgoing trunk in a local or remote trunk group by pressing the button assigned to that trunk group.
  - Inter-PBX attendant calls allows attendants for multiple branches to be concentrated at a main location.
- Call handling.
  - Attendant intrusion. Use the attendant intrusion feature to allow an attendant to intrude on an existing call. The Attendant Intrusion feature is also called Call Offer.
  - Attendant lockout - privacy. This feature prevents an attendant from re-entering a multiple-party connection held on the console unless recalled by a telephone user.
  - Attendant split swap. The attendant split swap feature allows the attendant to alternate between active and split calls. This operation may be useful if the attendant needs to transfer a call but first must talk independently with each party before completing the transfer.
  - Attendant vectoring. Attendant vectoring provides a highly flexible approach for managing incoming calls to an attendant. For example, with current night service operation, calls redirected from the attendant console to a night station can ring only at that station and will not follow any coverage path.
  - Automated attendant. Automated attendant allows the calling party to enter the number of any extension on the system. The call is then routed to the extension. This allows you to reduce cost by reducing the need for live attendants.
  - Backup alerting. The backup alerting feature notifies backup attendants that the primary attendant cannot pick up a call.
  - Call waiting. Call waiting allows an attendant to let a single-line telephone user who is on the telephone know that a call is waiting. The attendant is then free to answer other calls. The attendant hears a call waiting ringback tone and the busy telephone user hears a call waiting tone. This tone is heard only by the called telephone user.
  - Calling of inward restricted stations. A telephone with a class of restriction (COR) that is inward restricted cannot receive public network, attendant-originated, or attendant-extended calls. This feature allows you to override this restriction.
  - Conference. The conference feature allows an attendant to set up a conference call for as many as six conferees, including the attendant. Conferences from inside and outside the system can be added to the conference call.
  - Enhanced Return Call to (same) Attendant. Communication Manager provides individual queuing functions for each attendant supporting a multiplicity of waiting calls at a given time.
  - Listed directory number. Allows outside callers to access your attendant group in two ways, depending on the type of trunk used for the incoming call.

  - Override of diversion features. The override of diversion feature allows an attendant to bypass diversion features such as send all calls and call coverage by putting a call through to an extension even when these diversion features are on. This feature, together with attendant intrusion, can be used to get an emergency or urgent call through to a telephone user.
  - Priority queue. Priority queue places incoming calls to the attendant in an orderly queue when these calls cannot go immediately to the attendant.
  - Release loop operation. Release loop operation allows the attendant to hold a call at the console if the call cannot immediately go through to the person being called. A timed reminder begins once the call is on hold.
  - Selective conference mute. Selective conference mute allows a conference call participant, who has a display station, to mute a noisy trunk line. Selective conference mute is also known as far end mute.
  - Serial calling. The serial calling feature enables an attendant to transfer trunk calls that return to the same attendant after the called party hangs up. The returned call can then transfer to another station within the switch. This feature is useful if trunks are scarce and direct inward dialing services are unavailable.
  - Timed reminder and attendant timers. Attendant timers automatically alert the attendant after an administered time interval for the certain types of calls.
- Centralized attendant service. Centralized attendant service enables attendant services in a private network to be concentrated at a central location. Each branch in a centralized attendant service has its own listed directory number or other type of access from the public network. Incoming calls to the branch, as well as calls made by users directly to the attendants, are routed to the centralized attendants over release link trunks.
- Display. The display feature shows call-related information that helps the attendant to operate the console. This feature also shows personal service and message information.
- Making calls.
  - Auto Start and Do Not Split. The Auto Start feature allows the attendant to make a telephone call without pushing the start button first. If the attendant is on an active call and presses digits on the keypad, the system automatically splits the call and begins dialing the second call.
  - Auto Manual Splitting. Auto Manual Splitting allows an attendant to announce a call or consult privately with the called party without being heard by the calling party on the call. It splits the calling party away so the attendant can confidentially determine if the called party can accept the call.
- Monitoring calls.
  - Attendant control of trunk group access. Use the Attendant Control of Trunk Group Access feature to allow the attendant to control outgoing and two-way trunk groups.
  - Attendant direct extension selection. This feature allows the attendant to keep track of extension status - whether the extension is idle or busy - and to place or extend calls to extension numbers without having to dial the extension number.

- Attendant direct trunk group selection. With this feature, the attendant directs access to an idle outgoing trunk by pressing the button assigned to the trunk group. This feature eliminates the need for the attendant to memorize, or look up, and dial the trunk access codes associated with frequently used trunk groups.
- Crisis alerts to an attendant console. Crisis alert uses both audible and visual alerting to notify attendant consoles when an emergency call is made. Audible alerting sounds like an ambulance siren. Visual alerting flashes the CRSS-ALRT button lamp and displays the caller's name and extension (or room).
- Trunk group busy/warning indicators to attendant. This feature provides the attendant with a visual indication that the number of busy trunks in a group has reached an administered level. A visual indication is also provided when all trunks in a group are busy. This feature is particularly helpful to show the attendant that the attendant control of trunk group access feature needs to be invoked.
- Trunk identification by attendant. Trunk identification allows an attendant or display-equipped telephone user to identify a specific trunk being used on a call. This capability is provided by assigning a trunk ID button to the attendant console or telephone. This feature is particularly helpful for identifying a faulty trunk. That trunk can then be removed from service and the problem quickly corrected.
- Visually Impaired Attendant Service. Visually Impaired Attendant Service provides voice feedback to a visually impaired attendant. Each voice phrase is a sequence of one or more single-voiced messages. This feature defines six attendant buttons to aid visually impaired attendants.

Customization features

Using the Communication Manager, you can customize interfaces with Avaya and third-party adjuncts and solutions.

- Application Programming Interface (API): Allows numerous software applications to work with Communication Manager. APIs also allows a client programmer to create their own applications that work with Communication Manager.
- Application Enablement Services (AE Services): Provides connectivity between applications and Communication Manager. This connector allows development of new applications and new features without having to modify Communication Manager or expose its proprietary interfaces.

  Note:

  AE Services has its own set of customer documentation, including an overview. This overview of Communication Manager does not outline the changes to AE Services.
- Device and media control API: Provides a connector to Communication Manager that clients can use to develop applications that provide first-party call control. Applications can register as IP extensions on Communication Manager and then monitor and control those extensions.

  Device and media control API consists of a connector server software and a connector client API library. The connector server software runs on a hardware server that is independent of

Communication Manager. That is, device and media control API does not run co-resident with Communication Manager.

Tip:

Contact your Avaya representative for a complete set of device and media control API documentation.

- Co-resident branch Gateway: Enables communication between TCP/IP clients and Communication Manager call processing. The Branch Gateway is an application that routes internetwork messages from one protocol to another (ISDN to TCP/IP) and bridges all ASAI message traffic by way of a TCP/IP tunnel protocol.
- Java telephony application programming interface (JTAPI): Enables integration with Communication Manager ASAI.
- Telephony Services Application Programming Interface (TSAPI): An open API supported by Avaya computer telephony that allows integration to Communication Manager ASAI. TSAPI is based on international standards for CTI telephony services. Specifically, the European Computer Manufacturers Association (ECMA) CTI standard definition of Computer-Supported Telecommunications Applications (CSTA) is the foundation for TSAPI.
- Automatic Number Identification (ANI): Displays the telephone number of the calling party on your telephone. The system uses ANI to interpret calling party information that is signaled over multifrequency (MF) or Session Initiation Protocol (SIP) trunks. Any display telephone can use ANI.
- For H.323 and DCP endpoints, the caller information on the bridged call appearances can be set to be the same as the caller information on the principal station. To enable this feature, set the Match BCA Display to Principal field on page 2 of the Class of Service screen to y.

Scalability

For the entire list of system capacities, see *Avaya Aura® Communication Manager System Capacities Table*.

Note:

The introduction of Spectre and Meltdown fixes with the Avaya Aura® Release 7.1.3 has an impact on S8300D scalability performances. A Survivable Remote configuration for Communication Manager LSP with the Spectre and Meltdown fixes enabled can only support 200 users with up to 500 BHCC traffic.

Since the Spectre and Meltdown fixes are enabled by default, consider the configuration changes to upgrade to the Release 7.1.3.

Consider the following options if the higher capacity is required from the S8300D:

- Disable Spectre and Meltdown fixes on S8300D. This allows the S8300D to deliver the same level of capacity as in the Avaya Aura® Release 7.1.2 and before.

- Upgrade the embedded server to the latest S8300E model if disabling fixes on the S8300D is not viable.

For more information about Spectre and Meltdown fixes included in Avaya Aura® Release 7.1.3, see PSN020346u on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101048606.

Reliability

Communication Manager supports a wide range of servers, gateways, and survivability features enabling maximum availability for customers. The software is capable of mirroring processor functions, providing alternate gatekeepers, supporting multiple network interfaces, and ensuring survivability at remote and central locations.

The reliability feature includes:

- Alternate gatekeeper: Provides survivability between Communication Manager and IP communications devices such as IP telephones and IP softphones.
- Auto fallback to primary for branch gateways: Automatically returns a fragmented network, where a number of branch gateways are being serviced by one or more Communication Manager Survivable Remote sites, to the primary server. This feature is targeted for Branch Gateways only.
- Connection preserving failover/failback for branch gateways: Preserves existing bearer or voice connections while Branch Gateways migrate from one Communication Manager server to another. Migration might be caused by a network or server failure.
- Connection preserving upgrades for duplex servers: Provides connection preservation on upgrades of duplex servers for:
  - Connections involving IP telephones
  - Connections involving TDM connections on port networks
  - Connections on branch gateways
  - IP connections between port networks and branch gateways
- Communication Manager Survivable Core: Provides survivability by allowing backup servers to be placed in various locations in the customer network. The backup servers supply service to port networks where the main server or server pair fails or connectivity to the main server or server pair is lost.
  - When the Survivable Core is in control due to a network fragmentation or catastrophic main server failure, the return to the main server is automatic. It is provided by the scheduled, manual, and automatic options.
  - Dial Plan Transparency for Survivable Remote and Survivable Core preserves users' dialing patterns if a branch gateway registers with Survivable Remote, or when a port network registers with Survivable Core.

- IP bearer duplication using the TN2602AP circuit pack: Provides high-capacity voice over Internet protocol (VoIP) audio access to the switch for local stations and outside trunks.
  - Load balancing. Up to two TN2602AP circuit packs can be installed in a single port network for load balancing. The TN2602AP circuit pack is also compatible with and can share load balancing with the TN2302 and TN802B IP Media Processor circuit packs.
  - Bearer signal duplication. Two TN2602AP circuit packs can be installed in a single port network for bearer signal duplication. In this configuration, one TN2602AP is an active IP media processor and the other is a standby IP media processor.
- IP endpoint Time-to-Service: Improves a customer's IP endpoint time to service, especially where the system has many IP endpoints trying to register or re-register. With this feature, the system considers that IP endpoints are in-service immediately after they register. The feature of TTS-TLS supports TTS over a secure TLS connection. This is the recommended configuration choice.
- Survivable processor: A survivable processor is an Internal Call Controller (ICC) with an integral branch gateway, in which the ICC is administered to function as a spare processor rather than the main processor. The standby Avaya S8300 Server runs in standby mode with the main server ready to take control in an outage with no loss of communication.
- Handling of split registrations: Occurs when resources on one network region are registered to different servers. For example, after an outage activates the Survivable Remote server (Local Survivable Processors) or Survivable Core server (Enterprise Survivable Server), telephones in a network region register to the main server, while the branch gateways in that network region are registered with the Survivable Remote server. The telephones registered with the main server are isolated from their trunk resources. Communication Manager detects a split registration and moves telephones to a server that has trunk resources.
- Power failure transfer: Provides service to and from the local telephone company central office (CO), including wide area telecommunications system, during a power failure. This allows you to make or answer important or emergency calls during a power failure. This feature is also called emergency transfer.
- Standard Local Survivability: Provides a local Avaya G430 or G450 Branch Gateway and Juniper J4350 or J6350 gateway with a limited subset of Communication Manager functionality when there is no IP-routed WAN link available to the main server or when the main server is unavailable.
- SRTP for video call flows: This support is available only when the call-originating and the receiving endpoints are SIP-registered and the IP-codec-set administration on Communication Manager is SRTP. SRTP for video does not work for H.323 signaling. H.323-registered endpoints always send video RTP. SIP-H.323 interworking with video encryption is not supported and video is blocked in this case. However, if the SIP signaling follows the Best effort SRTP mode, Communication Manager allows video RTP to pass through in SIP to H.323 interworking.

Localization

Communication Manager supports a range of language features, such as administrable language displays and country-specific localization.

Communication Manager localization features include:

- Administrable language displays: Allows a message that appear on telephone display units to be shown in the language spoken by the user. These messages are available in English (the default), French, Italian, Spanish, user-defined, or Unicode; where user-defined can be almost any language using the Latin, Russian or Katakana writing scripts, and Unicode can be almost any language in the world. Administrator configures the language to be displayed for messages for each user. The feature requires 40-character display telephones.
- Administrable loss plan: Provides the ability to administer signal loss and gain for telephone calls. This capability is necessary because the amount of loss allowed on voice calls can vary by country.
- Bellcore calling name ID: Allows the system to accept calling name information from a Local Exchange Carrier network that supports the Bellcore calling name specification. The system can send calling name information in the format if Bellcore calling name ID is administered. The following caller ID protocols are supported:
  - Bellcore (default) - US protocol (Bellcore transmission protocol with 212 modem protocol).
  - V23-Bell - Bahrain protocol (Bellcore transmission protocol with V.23 modem protocol).
- Busy tone disconnect: In some regions of the world, the central office sends a busy tone for the disconnect message. With busy tone disconnect, the switch disconnects analog loop-start central office trunks when a busy tone is sent from the central office.
- Country-specific localization
  - Brazil — Block collect call: Blocks collect calls on class-of-restriction basis. This feature is available for any switch that uses the Brazil country code.
  - Italy — Distributed Communication Systems protocol: Italian DCS adds features to the existing Distributed Communication Systems capabilities and requires the use of Italian TGU/TGE tie trunks.
  - Japan
    - National private networking provides support for Japanese private ISDN networks.
    - Katakana character set Communication Manager supports the Katakana character set.
  - Russia
    - Central Office support on branch gateways: Communication Manager supports central office trunks in Russia using Avaya branch gateways.
    - ISDN/DATS network support: Supports ISDN/DATS trunk networks when the tone generated field is set to 15 (Russia) on the system-parameters tone—generation screen. It modifies the overlap sending delay and ISDN T302 and T304 timers to support the Russian trunk network.

    - Multi-Frequency Packet signaling: Multi-Frequency Packet (MFP) address signaling is provided in Russia on outgoing central office trunks. Calling party number and dialed number information is sent on outgoing links between local and toll switches.
- E&M signaling: E&M trunks are used to provide analog communication links. Continuous and pulsed Continuous and pulsed E&M signaling is a modification to the E&M signaling used in the United States. Continuous E&M signaling is intended for use in Brazil, but can also be used in Hungary. Pulsed E&M signaling is intended for use in Brazil.
- Multinational Locations: For customers who operate in more than one country, the Multinational Locations feature provides the ability to use a single Enterprise Communication Server (ECS) across multiple countries.
- Public network call priority: Provides call retention, forced disconnect, intrusion, mode-of-release control, and re-ring to switches on public networks. Different countries frequently refer to these capabilities by different names.
- QSIG support for Unicode: Extends the Unicode support on a single server to multi-node Communication Manager networks. This feature allows Unicode support across large campus configurations.
- World class tone detection: Enables Communication Manager to identify and handle different types of call progress tones, depending on the system administration.
- XOIP Tone Detection Bypass: The X over IP Tone Detection Bypass feature (where X = modem, fax, TTY-TDD, and so on) serves customers using older or non-standard external equipment such as modems, fax, TTY devices which are not easily recognized by VoIP resources within Communication Manager.

Call Center

The Avaya Aura® Call Center provides a fully integrated telecommunications platform that supports a powerful assortment of features, capabilities, and applications designed to meet all of your customers' Call Center needs.

Call Center applications, such as Avaya Call Management System for real-time reporting and performance statistics, and Avaya Business Advocate for expert predictive routing based on incoming calls rather than historical data, are easily integrated.

Communication Manager supports the Agent ID feature using which telephones can retrieve specific agent greetings and play the greetings when calls are received.

Communication Manager also supports the Restrict Call Joining feature on Avaya Aura® Contact Center. If enabled, Communication Manager restricts the agents from initiating a transfer or a conference operation. The restriction is applicable only to outbound calls. With the Restrict Second Agent Consult feature, agents can use only one consult operation, transfer or conference, at a time.

For a complete description of Call Center features for Communication Manager, see the following documents:

- *Avaya Aura® Call Center Overview*
- *Planning an Avaya Aura® Call Center Implementation*
- *Administering Avaya Aura® Call Center Features*
- *Avaya Aura® Call Center Feature Reference*
- *Programming Call Vectoring Features in Avaya Aura® Call Center*

Related links

Avaya Call Center on branch gateways on page 19

Avaya Call Center on branch gateways

Avaya Call Center functionality is supported on branch gateways with Communication Manager evolution server configuration, with an S8300D Server, S8300E Server, Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360 G7, or HP ProLiant DL360 G9 Server, and the G650 port network gateway with the Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360 G7, or HP ProLiant DL360 G9 Server.

Avaya Call Center Basic software is included with Communication Manager capability along with optional Computer Telephony Integration (CTI). This package provides a low-cost call center solution for small or branch offices.

More robust call center capabilities are provided with the optional Avaya Call Center Elite, which features Avaya Expert Agent Selection and services as the foundational software for the optional Avaya Business Advocate and Avaya Dynamic Advocate software.

The call center capabilities found in the Elite Call Center software package allows Communication Manager Call Center customers to enhance their customer service, help desk, travel, and other operations by providing powerful, integrated call routing through call vectoring and resources selection.

Related links

Call Center on page 18

Computer Telephony Integration

Computer Telephony Integration (CTI) enables Communication Manager features to be controlled by external applications, and allows integration of customer databases of information with call control features.

Avaya Computer Telephony is server software that integrates the premium call control features of Communication Manager with customer information in customers' databases. It is a local area network (LAN)-based CTI solution consisting of server software that runs in a client/server configuration. Avaya Computer Telephony delivers the CTI architecture and platform that supports

contact center application requirements, along with emerging applications programming interfaces (APIs). For more information, see *Avaya Aura® Application Enablement Services Overview*.

Automatic Call Distribution

Automatic Call Distribution (ACD) is the basic building block for call center applications. ACD offers you a method for distributing incoming calls efficiently and equitably among available agents. With ACD, incoming calls can be directed to the first idle or most idle agent within a group of agents. ACD along with Call Center Elite provides a very feature rich complement of routing and call handling capabilities. For detail information, see the *Avaya Aura® Call Center Overview* and *Avaya Aura®Call Center Feature Reference* guides.

Avaya Basic Call Management System

The Avaya Basic Call Management System (BCMS) helps you fine tune your call center operation by providing reports with the data necessary to measure your call center agents performance integrated with Communication Manager software.

The BCMS feature offers call management control and reporting at a low cost for call centers of up to 3000 agents. BCMS collects and processes ACD call data (up to seven days) within the system; an adjunct processor is not required to produce call management reports.

Communication Manager can generate real-time and historical reports.

Related links

Avaya Business Advocate on page 20

Avaya Business Advocate

Avaya Business Advocate is the collection of features that provide flexibility in the way a call is selected for an agent in a call surplus situation, and in the way an agent is selected for a call in agent surplus situations. Instead of the traditional “first in, first out” approach, the needs of the caller, potential business value, and the desire to wait are calculated. The system then decides what agents should be matched to the callers.

The Avaya Business Advocate features include:

- Auto reserve agents. Auto reserve agents allows the system to use the percent allocation distribution feature for agent skills.
- Call selection override per skill. Call selection override is determined by skill. Call center supervisors can override the normal call handling activity either on particular skills only, or for the entire call center.
- Dynamic percentage adjustment. The dynamic percentage adjustment feature allows the system to compare actual levels of service with service targets. The system can then adjust the service target so that the overall use of the skill is more efficient.

- Dynamic queue position. Dynamic queue position allows the system to put calls from multiple vector directory numbers (VDNs) into a skill queue. This feature ensures balanced call handling across VDNs.
- Dynamic threshold adjustment. Dynamic threshold adjustment allows the system to compare actual levels of service with service targets, and to adjust overload thresholds. This feature makes the use of overload agents more efficient.
- Logged-in advocate agent counting. The logged-in advocate agent counting feature counts agents toward the advocate agent limit if a service objective, percent allocation, or a reserved skill is assigned to the agent login ID, or if one of the agent skills is assigned least occupied agent or service level supervisor.
- Percent allocation distribution. Percent allocation distribution allows the system to distribute calls to auto reserve agents by comparing a reserve agent work time in a skill with the target allocation for that skill.
- Reserve agent time in queue activation. This feature activates a reserve agent either if the expected wait time (EWT) exceeds a pre-determined threshold, or if the call time in the queue exceeds the administered service level supervisor threshold.

Related links

Avaya Basic Call Management System on page 20

Mobility

Communication Manager supports extensive mobility features — Extensive in-building or in/out building wireless choices and hot desking features like Extension to Cellular (EC500), Personal Station Access (PSA) and Automatic Customer Telephone Rearrangement (ACTR) extend Communication Manager features to users, no matter where they are working.

Communication Manager mobility features include:

- Administration Without Hardware allows you to administer telephones that are not yet physically present on the system. This greatly facilitates the speed of setting up and making changes to the telephones on the system.
- Automatic Customer Telephone Rearrangement (ACTR) allows a telephone to be unplugged from one location and moved to a different location without additional switch administration. The switch automatically associates the extension to the new port.
- Avaya Wireless Telephone Solutions (AWTS) is fully integrated with Communication Manager, and allows a user full access to Communication Manager features from a mobile telephone.

  Note:

  Avaya Wireless Telephone Solutions (AWTS) replaces the DEFINITY Wireless Business System (DWBS).
- The Avaya Extension to Cellular (EC500) feature provides the expansion of mobile services, including one-number availability, increased user capacities, flexibility across facilities and

hardware, more control over unauthorized usage, enhanced enable/disable capability, increased serviceability, and support of IP trunk facilities. To define call treatment options for EC500 calls, you can use up to 99 configuration sets that are defined in the system. If you set the **Cellular voice mail detection** field, an EC500 call does not cover to the cellular voice mail. When the call server detects that the call is covered to the cellular voice mail, the call server returns the call to the server.

Note:

In the One-X mobile environment, you can edit the values of only the **Cellular voice mail detection** field and the **Call log notify** field. All other fields are read-only.

Communication Manager 6.3.2 introduces additional security for the EC500/One-X Mobile Lite call (AEFSC) feature. With this feature, when a user makes an FNE call from a cellular phone, the system authenticates the call with the station security code (SSC). The call fails without the valid SSC. When a caller wants to make an EC500 call, the caller must dial the SSC after the FNE number. For example, <FNE> [Dial tone] <SSC> # [Dial tone or confirmation tone] <Subsequent digit or extension>.

The integration of Microsoft Office Communicator (MOC) with Communication Manager through ASAI supports bridging, that is, having two user functions simultaneously. For example, the user can be on an active call on a desk phone and, at the same time, be on an active call on an off-PBX destination, such as a mobile phone.

- E911 ELIN for IP wired extensions automates the process of assigning an emergency location information number (ELIN) through an IP subnetwork (“subnet”) during a 911 call. The ELIN is then sent over either CAMA or ISDN PRI trunks to the emergency services network when 911 is dialed.
- The Personal Station Access (PSA) feature allows you to transfer your telephone station preferences and permissions to any other compatible telephone. PSA has several telecommuting applications. For example, several telecommuting employees can share the same office on different days of the week. The employees can easily and remotely make the shared telephone “theirs” for the day.
- The SIP Visiting User (SIP VU) feature enables users with the 9620 or 9630 SIP telephone to log in to any SIP telephone in the enterprise and receive their own individualized services, including menus, contacts, and buddy lists.

  The SIP Visiting User feature relies on specialized firmware on the telephone, and also requires SIP VU administration.
- Use the Terminal Translation Initialization (TTI) feature to merge an X-ported extension to a valid port, or to separate an extension from a port. You usually use TTI to move telephones. However, you can also use TTI to connect and move attendants and data modules. Terminal Translation Initialization (TTI) also works with Administration Without Hardware (AWOH).
- The TransTalk 9000 is a single-zone or dual-zone, in-building wireless system that provides a mobility solution on Communication Manager-based systems. It delivers the benefits and accessibility of a wireless telephone with all the power and functionality of a wired desk telephone.

- X-station mobility allows remote users to access switch features. That is, X-station mobility allows certain OEM wireless telephones remoted over a PRI trunk interface to be controlled by Communication Manager as if the telephones were directly connected to the switch.
- With the Multiple Device Access (MDA) feature, a SIP user can register more than one SIP device with a single extension. For example, a user has ADVD at his desk, 96X1 in his lab, and one-X® Communicator on his laptop and all the devices are registered with the same extension 123456. When a call arrives at extension 123456, all the devices are alerted. The user can answer the call from any one of the devices. If required, the user can bridge on to the call from one of the idle devices by using the Simulated Bridge Appearance (SBA) feature. Therefore, the call can be handed off between devices without parking the call.

Collaboration

Communication Manager contains a variety of features aimed at providing easy ways to collaborate with groups of peers, customers, and partners such as executives, sales people, and professional specialists. These key work groups require a high level of effective interaction, and Communication Manager delivers.

Conferencing:

- Abort conference. When you press the conference button and for any reason you hang up before you complete the conference, you will cancel the conference. The original call that was put on soft-hold is put on hard-hold
- Conference - three party. The conference button allows single-line telephone users to make up to three-party conference calls without attendant assistance.
- Conference - six party. The conference button allows multi-appearance telephone users to make up to six-party conference calls without attendant assistance.
- Conference/transfer display prompts are based on the display prompts are based on the user class of restriction (COR), independent of the select line appearance conferencing and no-dial-tone conferencing feature.
- The conference/transfer toggle/swap feature allows users to toggle between two parties in the middle of setting up a conference call prior to connecting all parties together, or to consult with both parties prior to transferring a call.
- The group listen feature simultaneously activates your speakerphone in listen-only mode, and your handset or headset in listen-and-speak mode. This allows you to serve as spokesperson for a group. You can participate in a conversation while everyone else in the room is listening to what is said.

  Note:

  This feature is not supported on IP telephones.
- Hold/unhold conference allows a user to use the Hold button to bring the held party back to the conversation.

Note:

This feature is not available for BRI stations or attendant consoles.

- The Meet-me Conferencing feature allows a person to set up a dial-in conference of up to six parties. The Meet-me Conferencing feature uses call vectoring to process the setup of the conference call.
- Expanded Meet-me Conferencing. Use the Expanded Meet-me Conferencing application to set up multi-party conferences consisting of more than six parties. The Expanded Meet-me Conferencing application supports up to 300 parties.
- No dial tone conferencing. This feature can eliminate user confusion over receiving dial tone when trying to conference two existing calls.
- No hold conference. This feature allows a user to automatically add another party to a conference call while continuing the conversation of the existing call.
- Select line appearance conferencing. If you are in a conversation on line “b”, and another line is on hold or an incoming call is alerting on line “a”, then pressing the CONF button bridges the calls together. Using the select line appearance feature on Communication Manager, the user has the option of pressing a line appearance button to complete a conference instead of pressing CONF a second time.
- The selective conference party display feature allows any user on a digital station with display or on an attendant console to use the display to identify all of the other parties on a two-party or conference call.
- Selective party drop allows a user to selectively drop the party currently shown on the display with a single button push. This can be useful during conference calls when adding a party that does not answer and the call goes to voice mail.
- Selective conference mute allows a conference call participant, who has a display station, to mute a noisy trunk line. Selective conference mute is also known as far end mute.
- Enhanced SIP Signaling. Using the Enhanced SIP Signaling feature, you can:
  - see a roster of conference participants and drop the selected participants for Communication Manager-based conferences.
  - enable audio conferences, facilitated by Avaya Aura® Conferencing Release 7.0.
  - enhance the behavior of sequenced applications in a Communication Manager Feature Server environment.

Multimedia calling:

Multimedia calls are initiated with voice and video only. Once a call is established, one of the parties may initiate an associated data conference to include all of the parties on the call who are capable of supporting data.

- Multimedia Application Server Interface. The multimedia Application Server Interface (ASA) provides a link between Communication Manager and one or more multimedia communications eXchange nodes. A Multimedia Communications Exchange (MMCX) is a stand-alone multimedia call processor produced by Avaya.

- Multimedia call early answer on vectors and stations. Early answer is a feature applied to multimedia calls in conjunction with conversion to voice.
- Multimedia call redirection to multimedia endpoint. A dual port multimedia station may be a destination of call redirection features such as call coverage, forwarding, and station hunting. The station can receive and accept full multimedia calls or data calls converted to multimedia.
- Multimedia data conferencing (T.120) through an ESM. The data conference is controlled by an adjunct device called an Expansion Services Module (ESM). For more information on ESM, see *Installation for Adjuncts and Peripherals for Avaya Aura™ Communication Manager.*
- Multimedia hold, conference, transfer, and drop. Station users can activate hold, conference, transfer, or drop on multimedia calls. Multimedia endpoints and voice-only stations may participate in the same conference.
- Multimedia queuing with voice announcement. When multimedia callers queue for an available member of a hunt group, they are able to hear an audio announcement.

Paging and intercom:

- Code calling access allows attendants, users, and tie trunk users to page with coded chime signals.
- Group paging allows a user to make an announcement to a group of people using speakerphones. The speakerphones are automatically turned on when the user begins the announcement.
- Intercom - automatic. With this feature, users who frequently call each other can do so by pressing one button instead of dialing an extension number.
- Intercom - dial. This feature allows multi-appearance telephone users to easily call others within an administered group. The calling user lifts the handset, presses the dial intercom button, and dials the one-digit or two-digit code assigned to the desired party.
- Loudspeaker paging access provides attendants and telephone users dial access to voice paging equipment. As many as nine paging zones can be provided by the system, and one zone can be provided that activates all zones at the same time.
- Manual signaling allows one user to signal another user. The receiving user hears a two-second ring. The signal is sent each time the button is pressed by the signaling user. The meaning of the signal is prearranged between the sender and the receiver. Manual signaling is denied if the receiving telephone is already ringing from an incoming call.
- Whisper page allows an assistant or colleague to bridge onto your telephone conversation and give you a message without being heard by the other party or parties you are talking to. Whisper page works only on certain types of telephones.

Team button:

The Team button feature is used to monitor members of a team of stations. Monitoring station is notified about the general redirection state of the monitored station. Starting Release 6.3.6 of Communication Manager, direct transfer, transfer upon hang-up, and override SAC/CFWD/EC features can be used with the **Team** button feature.

Call routing

Call routing features are designed to reduce networking costs through effective use of IP Trunking over WAN or LAN links.

Call Routing features include:

- Automatic routing: Communication Manager provides a variety of automatic routing features for public and private networks. Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) are the foundation for these automatic-routing features. They route calls based on the preferred (normally the least expensive) route available at the time the call is placed.
- Enbloc Dialing and Call Type Digit Analysis: With this feature, users can automatically place outgoing calls based on the telephone number information in the telephone's call log, without the user having to modify the telephone number.
- Generalized route selection: This feature provides voice and data call-routing capabilities. You use it to select not only the least-cost routing, but also optimal routing over the appropriate facilities. It enhances AAR and ARS by providing additional parameters in the routing decision and maximizing the chance of using the right facility to route the call.
- Multiple Location Support: This feature enables local user time, local ARS Public Analysis Tables for local trunking, automatic Daylight Savings Time, enhances shared resource algorithms (touch tone receivers), and other features, when Remote Expansion Port Networks (EPNs), ATM Port Networks, and Avaya Media Gateways are remoted off of a central server at a different location.
- Alternate facility restriction levels: These levels allow Communication Manager to adjust facility restriction levels or authorization codes for lines or trunks. Each line or trunk is normally assigned a facility restriction level. With this feature, Alternate Facility Restriction Levels are also assigned.
- Traveling Class Marks: A mechanism for passing the facility restriction level of a caller from one Electronic Tandem Network switch to another. Traveling Class Marks allow privilege checking to be passed across switches through the Electronic Tandem Network.
- Answer detection: For purposes of Call-Detail Recording (CDR), it is important to know when the called party answers a call. Communication Manager provides three ways to determine whether the called party has answered an outgoing call — answer supervision by time-out, call-classifier board and network answer supervision.
- Source-based routing: With the source-based routing feature, Communication Manager sends the location information of H.323, DCP, and analog stations to Session Manager. Session Manager uses the IP address to select the matching trunk or route pattern and then routes the call to destination stations.
- With the Multiple Call Handling feature, the rerouted or the forwarded-switched calls use the call coverage path of the diverted-to party. Based on the Communication Manager configuration, the greeting of the administered party is played to the caller.

- Delayed drop: With Communication Manager Release 6.3.6, you can use the **Interworking of ISDN Clearing with In-Band Tones** field on the SIP Trunk form to communicate the reason of the call drop to the caller. After knowing that the called party will not answer the call, the caller or the Voice Portal agent can decide whether to wait for the announcement to complete or drop the call.
- Inter-Gateway Alternate Routing: IGAR provides enhanced Quality of Service (QoS) to large distributed single-server configurations. You can use IGAR for configurations where the IP network is not reliable enough to carry bearer traffic. If you have more than one IP network available, you can use H.323 or SIP trunks for IGAR instead of the PSTN. Communication Manager Release 6.3.5 and earlier supported IGAR for analog, DCP, and H.323 endpoints. From Release 6.3.6 onwards, IGAR support is extended to SIP endpoints.

Telecommuting and Remote Office

Telecommuter capabilities route calls appropriately and give employees access to the full Avaya Aura Communication Manager feature set whether working at home, in the office or on the road.

Communication Manager supports the following telecommuting features:

- Coverage of calls redirected off-net. Coverage of calls redirected off-net (CCRON) allows calls that have been redirected to locations outside of the switch to return to the switch for further processing.
- Extended user administration of redirected calls (telecommuting access). Extended user administration of redirected calls (also called telecommuting access) allows you to change the lead call coverage path or forwarding extension from any on-site or off-site location.
- Off-premises station. A trunk-data module connects off-premises private-line trunk facilities and Communication Manager.
- Remote access permits authorized callers from remote locations to access the system via the public network and then use its features and services. There are a variety of ways of accessing the feature.

Telephony

Communication Manager provides comprehensive end user telephony features (such as, auto attendant, call transfer, call forward, and so on) that facilitate effective communications among employees, customers and partners.

Mid-call features:

Communication Manager ensures that mid-call call telephony features work when Avaya endpoints establish video calls with Radvision endpoints. Customers can use video mute and unmute, transfers, and conferences during a video call.

Exclusion:

Users can maintain privacy of their telephonic conversations and ensure that unwanted parties will be unable to join the call. You can use Exclusion with Extension To Cellular, Bridge Call Appearance, and Service Observing.

Concurrent call management:

If the Limit Number of Concurrent Calls (LNCC) feature is enabled on a station, Communication Manager restricts the number of incoming calls to one call at a time. If the user is busy, the subsequent incoming calls receive a busy tone. Communication Manager Release 6.2 and earlier supported this feature on H.323 and DCP telephones. Communication Manager Release 6.3 extends this support to SIP telephones.

Call log support

Communication Manager records all missed calls in the missed call log of 94xx deskphones.

Call log support for busy 94xx deskphones

Communication Manager 6.3.2 records all incoming calls when a 94xx deskphone is busy because:

- All but one call appearances reserved for incoming calls are in the non-idle state. The last call appearance is reserved for outgoing calls.
- All call appearances are in the non-idle state.
- The Do Not Disturb feature is active on the endpoint.
- One call appearance is busy on a call because a remote user has put the call on hold or started a transfer or a conference call.

Supported number of digits in a call log

For a direct incoming external call from an ISDN or a SIP network, Communication Manager displays up to 21 digits of the calling-party number on a DCP, an H.323, or a SIP endpoint. Earlier, Communication Manager displayed only 7 digits of the calling-party number.

The missed call log and the answered call log of the endpoints display all 21 digits. Communication Manager also stores all 21 digits of an incoming external call from an ISDN or SIP network that is redirected by coverage, forwarding, bridging, or a similar feature in the missed call log and the answered call log of the endpoints

Online/Offline Call Journal (Call History)

With the Online/Offline Call Journal (Call History) feature, the SIP and H.323 phone users can view the call log entries when the user logs in from a different H.323 or SIP device. The SIP and H.323 users receive the logs for all answered and unanswered calls while the phones were in the logged-out state. With this enhancement, the H.323 and SIP desk phones back up all the call logs and restore them when the user logs in.

Communication Manager backs up up to 10 calls for the logged out H.323 users. Communication Manager does not back up or restore the log for calls that are answered or unanswered by the H. 323 phones when in the logged-in state. The H.323 phones continue to use HTTP for this purpose.

Call notification

SIP undelivered call notification:

The SIP undelivered call notification feature provides a notification about the undelivered call to the endpoint. Communication Manager initiates the SIP undelivered call notification feature when a SIP endpoint receives a call in one of the following situations:

- All call appearances are busy.
- LNCC is activated and the endpoint is busy.
- Call Forward Busy or Call Forward All is enabled.
- Enhanced Call Forward (ECF) unconditional or ECF busy is enabled.
- Cover All Calls is enabled.

Codec support

Communication Manager supports G.722 wideband audio codec between H.323 endpoints and SIP video and audio endpoints.

Survivability specification

Communication Manager supports two survivability options: survivable core and survivable remote.

Survivable core server

With survivable core servers, the system continues to operate in the events of network outage. A survivable core server provides survivability support to IP port networks and to Processor Ethernet for registering gateways and IP endpoints. This survivability option is available only for Communication Manager.

Survivable remote server

Survivable remote servers provide enhanced redundancy for branch gateways operating within networks. Survivable remote servers take over segments that lose connection from their primary call server and provide those segments with Communication Manager operation until the outage is resolved. A survivable remote server provides survivability support to IP and SIP telephones and to branch gateways when the connection to the core server fails. This survivability option is available for both Communication Manager and Session Manager.

For more information about survivability options, see *Avaya Aura® Communication Manager Survivability Options*.

Dial plan specification

The Dial Plan feature supports intra-server dialing for extensions at the main server as well as for extensions at remote locations. To support inter-server dialing, Communication Manager uses the uniform dial plan (UDP) to route a call from the local server. With the Dial Plan feature, you can set extensions of maximum 13 digits. You can further extend the extension length to 18 digits by using uniform dial plans.

To preserve the dial plan for extensions and attendants in a multiple independent node network that is being migrated to a single distributed server, Communication Manager provides the Multi-location Dial Plan feature.

To assign short extensions to different branches and administer the same numbering format across all the branches, you can use the Per-Location Dial Plan feature.

Define the dial plan information for each type of call, including:

- Attendant
- Automatic Alternate Routing (AAR)
- Automatic Route Selection (ARS)
- Dial access codes, including feature access codes (FACs) and trunk access codes (TACs)
- En bloc extensions (enb-ext)
- Extensions
- FACs only
- Prefixed extensions

For more information about the dial plan feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

SIP

SIP provides the foundation for multimedia communications and collaboration for voice, video, and customer contact. SIP based presence and Instant Messaging (IM) lets users inform others of their status, availability and allows immediate responsiveness to important business issues.

In conjunction with Avaya Aura® Session Manager, Communication Manager provides complete feature enablement for SIP devices, support for SIP trunking, and integration of third party SIP solutions.

Emergency calling services

Communication Manager allows you to manage and respond to unforeseen emergency situations. Enhanced 911 (E911) feature allows you to quickly access your local public safety agency. The

public safety agency can dispatch the appropriate response team in cases of a fire, accident, crime, or medical agency.

New in Release 7.1.3

Alarms, events, and log reference guides are merged

In Communication Manager Release 7.1.3, the following guides are merged and the new guide is named as *Avaya Aura® Communication Manager Alarms, Events, and Logs Reference* guide, and are removed from the Avaya Support site:

- *Avaya Aura® Communication Manager Denial Events*
- *Avaya Aura® Communication Manager Server Alarms*
- *Maintenance alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*

Support for 9000 announcements for a single Avaya Aura® Media Server

In earlier releases, Communication Manager supported 1024 announcements only from a single announcement source. With Communication Manager Release 7.1.3, you can configure up to 9000 announcements for a single Avaya Aura® Media Server instance.

Malicious Call Trace support on SIP

Communication Manager Release 7.1.3 can send Malicious Call Trace (MCT) notifications over SIP trunks.

Malicious Call Trace notification passes over SIP trunk groups through Session Manager to a Session Border Controller. The Session Border Controller can adapt the Malicious Call Trace notification to the format required by the SIP service provider.

Alphanumeric URI dialing support

In Communication Manager Release 7.1.3:

- You can assign alphanumeric URIs to hunt groups and vector directory numbers (VDNs)
- You can dial a hunt group and a VDN using the SIP URI
- When a call is made from a station to a hunt group or a VDN using SIP URI, the call is sent to respective hunt group or VDN
- You can use alphanumeric handles for the following features:
  - Call forwarding
  - Priority calling
  - Whisper page
  - Directed call pickup
  - CPN block and unblock
  - Call unpark

Note:

Communication Manager supports alphanumeric URI dialing for SIP phones only.

Support for VMware vSphere 6.7

Communication Manager Release 7.1.3 adds support for the following VMware software in the Virtualized Environment:

- VMware vSphere ESXi 6.7
- VMware vCenter Server 6.7

Security hardening commands enhancement

The following security hardening commands used in Communication Manager Release 7.1.2 are renamed in Communication Manager Release 7.1.3:

Security hardening command name in Communication Manager Release 7.1.2	Security hardening command name in Communication Manager Release 7.1.3
`MUDG_part1`	`setCMHardening`
`sudo updateRegistry UseAIDE=enabled` `sudo setPlatformAttributes`	`setCMAide`
`sudo updateRegistry UseClamav=enabled` `sudo setPlatformAttributes`	`setCMClamav`

Support for SIP attendant

In Communication Manager Release 7.1.3, you can route attendant console calls to Avaya Breeze™—based Avaya Equinox® Attendant.

Linux kernel configuration

Communication Manager Release 7.1.3 includes the Red Hat updates to support mitigation of the Meltdown and Spectre vulnerabilities. However, this can affect the performance of Communication Manager. So, a script **`kernel_opts.sh`** is introduced that allows the setting of kernel options to control how these vulnerabilities are handled. The effect of running the kernel configuration script is immediate and will continue across reboots. You can run the script as an admin user by using the CLI.

The script has the following arguments:

- status — Displays the current status of the kernel options.
- enable — Enables all flags to provide maximum protection.
- disable — Disables all flags to provide maximum performance.

Impact of Spectre and Meltdown fixes on S8300D

The introduction of Spectre and Meltdown fixes with the Avaya Aura® Release 7.1.3 has an impact on S8300D scalability performances. A Survivable Remote configuration for Communication Manager LSP with the Spectre and Meltdown fixes enabled can only support 200 users with up to 500 BHCC traffic.

For more information, see Scalability on page 14

New in Release 7.1.2

Product Description guide is merged into Overview and Specification guide

In Communication Manager Release 7.1.2, the *Avaya Aura® Communication Manager Product Description* guide is merged into the *Avaya Aura® Communication Manager Overview and Specification* guide, and the *Avaya Aura® Communication Manager Product Description* guide is removed from the Avaya Support site.

Support for alphanumeric URI dialing

Communication Manager Release 7.1.2 supports placing and receiving calls using alphanumeric URIs. An alphanumeric URI consists of alphanumeric handles that are used to identify a directory number. Communication Manager supports alphanumeric handles on both SIP and H.323 desk phones.

Support for Extended Security Hardening

Communication Manager Release 7.1.2 supports Extended Security Hardening to reduce vulnerabilities and enhance the security of the Communication Manager application.

New in Release 7.1.1

Support to tandem MIME for PIDF-LO

Communication Manager Release 7.1.1 can tandem Multipurpose Internet Mail Extensions (MIME) attachments for Presence Information Data Format Location Object (PIDF-LO) in a SIP message. Communication Manager can also pass the PIDF-LO information in the SIP message.

Support for deployment on Kernel-based Virtual Machine

You can deploy Communication Manager Release 7.1.1 on Kernel-based Virtual Machine (KVM).

KVM is a virtualization infrastructure for the Linux kernel that turns the Linux kernel into a hypervisor. You can remotely access the hypervisor to deploy applications on the KVM host.

KVM virtualization solution is:

- Cost effective for the customers.
- Performance reliable and highly scalable.
- Secure as it uses the advanced security features of SELinux.
- Open source software that can be customized as per the changing business requirements of the customers.

For information about deployment on KVM, see *Deploying Avaya Aura® Communication Manager on Kernel-based Virtual Machine*.

Support for Channel Type identification over ASAI to CTI application

Communication Manager Release 7.1.1 supports channel type identification over ASAI to a CTI application. For incoming SIP trunk calls, Communication Manager Release 7.1.1 identifies the channel type as voice, video, or unknown when the call:

- Enters a monitored Vector Directory Number (VDN) or hunt group (skill/split).
- Is monitored and is alerting at a deskphone or Agent.

For this feature to work, the CTI link between Communication Manager and Application Enablement Services must be greater than 7.

This feature might not work or might show an unknown channel type on the CTI application when:

- The Direct Media feature is enabled.
- Communication Manager is not able to identify the channel from the incoming SIP request.

Support for Service Observe and Barge-in features using feature access code through ASAI

Communication Manager Release 7.1.1 enables Avaya Oceana™ Solution to:

- Perform Service Observe and Barge-in operations on a voice channel.
- Add a Service Observer to a call by using Feature Access Codes.
- Toggle between listen-only and barge-in modes through CTI. To toggle between modes, Avaya Oceana™ Solution must drop a Service Observer while in a mode and add the Service Observer back while in another mode.

Support to drop or disconnect Service Observer from call using CTI application over ASAI

Prior to Communication Manager Release 7.1.1, a Service Observer was dropped or disconnected from a call only when the Service Observer goes on-hook. With Communication Manager Release 7.1.1, you can drop or disconnect a Service Observer from a call using a CTI application over ASAI.

New in Release 7.1

Red Hat Enterprise Linux Support

Communication Manager Release 7.1 supports Red Hat Linux® 7.2 with Kernel version 3.10.0-327.10.1.el7.AV3.x86_64.

OVA signing

Communication Manager release 7.1 supports the Open Virtualization Archive (OVA) security feature. OVAs are digitally signed with Avaya certificates that ensure application integrity.

Communication Manager server separation

In earlier releases, Communication Manager duplex configurations required a cable for connecting two Communication Manager instances. With Communication Manager 7.1, you can physically separate the Communication Manager instances.

Discontinued Support for RFA/AFS Generated Identity Certificates

For Communication Manager Releases 5.0 to 7.0.x, the Remote Feature Activation/Authentication File Server tools have been building a unique Identity Certificate for Communication Manager as part of the license installation process. These tools were being signed by the Avaya Product Root CA with an outdated security signature of SHA1 and RSA 1024 key length. To improve the security process, from Communication Manager 7.1, customers must use the SMI pages to import the third-party hosted certificates.

Support for deployment on Amazon Web Services

You can deploy simplex and duplex Communication Manager on Amazon Web Services.

Amazon Web Services (AWS) is a cloud services platform that enables the enterprises to securely run the applications on the virtual cloud. The key components of AWS are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

Supporting the Avaya applications on the AWS Infrastructure as a service (IaaS) platform provides the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure. The customers can move from CAPEX to operational expense (OPEX).
- Reduces the maintenance cost of running the data centers.
- Provides the common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.

Network preemption

Communication Manager supports network preemption. For network preemption to work, Communication Manager must be configured to use Session Manager as the bandwidth manager. To configure Session Manager as the bandwidth manager, see *Avaya Aura® Communication Manager Feature Description and Implementation*. The security administrator can assign bandwidth budgets for audio and video, to each network link on Session Manager. When server or network resources are running too low to allow additional calls, call preemption occurs. For more information, see *Administering Avaya Aura® Session Manager*.

Support for ESXi 6.5 and vSphere 6.5

Communication Manager adds support for ESXi 6.5 and vSphere 6.5 in the Virtualized Environment.

ESXi versions 5.0 and 5.1 are no longer supported. Also, ESXi 6.5 is not supported with HP ProLiant DL360 G7.

Updated browser support

Communication Manager Release 7.1 and later supports the following web browsers:

- Mozilla Firefox browser: version 45.0 and later
- Microsoft Internet Explorer browser: version 11

Note:

If you use unsupported browsers, some features might not work, or an application might not open.

Minimum support version for TLS

Communication Manager Enables the administrator to specify the minimum supported TLS version to restrict the use of the older TLS versions in the system.

Support for Enhanced Access Security Gateway

Communication Manager supports Enhanced Access Security Gateway (EASG). EASG is a certificate based challenge-response authentication and authorization solution. Avaya uses EASG to securely access customer systems and provides support and troubleshooting.

EASG provides a secure method for Avaya services personnel to access the Communication Manager remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck. EASG must be enabled for Avaya Services to perform the required maintenance tasks.

You can enable or disable EASG through Communication Manager.

EASG only supports Avaya services logins, such as init, inads, and craft.

Discontinuance of ASG and ASG-enabled logins

EASG in Communication Manager 7.1.x replaces Avaya's older ASG feature. In the older ASG, Communication Manager allowed the creation of ASG-enabled user logins through the SMI Administrator Accounts web page. Such logins are no longer supported in Communication Manager 7.1.x. When upgrading to Communication Manager 7.1.1 from older releases, Communication Manager does not support ASG-enabled logins.

For more information about EASG, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Compliance with DISA security STIGs

Communication Manager Release 7.1 is now compliant with the security requirements stated in Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs).

Command History

Use this feature to define the number of months for which Communication Manager must maintain the command history and to compress the command history file after running the rotation action.

Define the number of months the system requires to maintain command history. Choose a duration between 3 months to 24 months.

In addition to the above, you can now compress the command history file after running the rotation action on the SMI page.

CAC sharing between Communication Manager and Session Manager

Communication Manager can establish VoIP media for H.323 stations and trunks, for inter Port Network, gateway or Avaya Aura® Media Server IP connections and for non-Session Manager routed SIP trunks. These IP media connections are not visible to Session Manager. In Communication Manager 7.1, Session Manager can be configured as a central authority for bandwidth management. With this setting, Communication Manager requires bandwidth for voice and multimedia IP connections from Session Manager. You can set the bandwidth limits applicable for various locations through System Manager. For more information about setting bandwidth limits, see *Administering Avaya Aura® Session Manager*.

Discontinued support of tethereal symbolic link to tshark

Communication Manager Release 7.1 and later does not support the symbolic link of tethereal command to the **tshark** command. Users must now use the **tshark** command to analyze the network traffic.

Discontinued support for Telnet

Communication Manager Release 7.1 does not support Telnet.

IPv6 support

Communication Manager Release 7.1 supports dual stack. Therefore, Communication Manager can be simultaneously connected with endpoints and entities that use IPv4 and IPv6 addresses.

Discontinued support of default server identity certificate

From Communication Manager Release 7.1, the Communication Manager server no longer supports the use of the default server identity certificate, which is signed by Avaya Product Root CA, and is automatically loaded into the Communication Manager application Identity Certificate stores by Authentication File Server at the time of installation.

Starting with Communication Manager Release 7.1, you must import identity certificates for the Web Services application and the Communication User Services application.

To create Communication Manager Identity Certificates, do one of the following:

- Import certificates that are created and signed by a third party host. For example, Verisign.
- Create and sign the Identity Certificate for Communication Manager by using the Trust Management PKI feature of Avaya Aura® System Manager.
- Generate a Certificate Signing Request (CSR) by using the Communication Manager SMI interface. Send the CSR to a signing authority.

In each of the options, the Communication Manager SMI interface directs the download of the Identity Certificate to store into one or more of the Communication Manager application trust stores. These application trust certificates are exchanged during the TLS client or server handshake to securely confirm the identity of the Communication Manager application.

Supported footprints

Supported footprints of Communication Manager on VMware

- **Table 1: On Appliance Virtualization Platform**

Product name	Footprint (Max users)	Release	CPU (GHz) — Haswell or equivalent	Number of vCPUs	RAM (GB)	HDD (GB)	NICs (* with OOBM)
Communication Manager Simplex small	1000	7.1	S8300D or S8300E	2	3.5	64	1 or 2*
Communication Manager Simplex medium	2400	7.1	2.4	2	4	64	1 or 2*
Communication Manager Simplex large	41000	7.1	2.4	2	4.5	64	1 or 2*
Communication Manager Duplex	30000	7.1	2.4	3	5	64	2 or 3*
Communication Manager Hi Duplex	41000	7.1	2.6	3	5	64	2 or 3*

- **Table 2: On Virtualized Environment**

Product name	Footprint (Max users)	Release	CPU (GHz) — Haswell or equivalent	Number of vCPUs	RAM (GB)	HDD (GB)	NICs
Communication Manager Simplex	41000	7.1	2.4	2	4.5	64	2
Communication Manager Duplex	30000	7.1	2.4	3	5	64	3
Communication Manager Hi Duplex	41000	7.1	2.6	3	5	64	3

Supported footprints of Communication Manager on KVM

Product name	Footprint (Max users)	Release	CPU (GHz) — Haswell or equivalent	Number of vCPUs	RAM (GB)	HDD (GB)	NICs
Communication Manager Simplex	41000	7.1	2.4	2	4.5	64	2
Communication Manager Duplex	30000	7.1	2.4	3	5	64	3
Communication Manager Hi Duplex	41000	7.1	2.6	3	5	64	3

Note:

NICs must be in bridge mode.

Supported footprints for Communication Manager on AWS

Product name	Footprint (Max users)	AWS instance type	AWS vCPU	AWS RAM (GB)	HDD (GB)	NICs
Communication Manager Simplex	41000	m4.large	2	8	64	2
Communication Manager Duplex	41000	c4.xlarge	4	7.5	64	3

Chapter 3: Interoperability

Supported platforms

Avaya Aura® Communication Manager supports the following platforms:

Sl. No.	Platform	Reference
1	VMware	See *Deploying Avaya Aura® Communication Manager*.
2	Amazon Web Services	See *Deploying Avaya Aura® Communication Manager on Amazon Web Services*.
3	Kernel-based Virtual Machine	See *Deploying Avaya Aura® Communication Manager on Kernel-based Virtual Machine*. Kernel-based Virtual Machine platform is supported from Avaya Aura® Communication Manager Release 7.1.1.

Supported hardware

Avaya Aura® Communication Manager supports the following servers:

Sl. No.	Supported server	Reference
1	Avaya S8300E	See *Installing and Upgrading the Avaya S8300 Server*.
2	Avaya S8300D	See *Installing and Upgrading the Avaya S8300 Server*.
3	HP-ProLiant-DL360–G7–1U	See *Installing the HP ProLiant DL360 G7 Server*.
4	HP ProLiant DL360 G9	See *Installing the HP ProLiant DL360 G9 Server*.
5	Dell PowerEdge R610 1U	See *Installing the Dell PowerEdge R610 Server*.
6	Dell PowerEdge R620 1U Server	See *Installing the Dell PowerEdge R620 Server*.
7	Dell PowerEdge R630 Server	See *Installing the Dell PowerEdge R630 Server*.

Supported endpoints

Avaya Aura® Communication Manager supports the following communication devices:

- Analog devices
  - Avaya analog telephones
- Digital devices
  - Avaya digital deskphones and telephones
  - Avaya Callmaster telephone
  - Avaya DECT Handsets
- IP-based devices
  - Avaya IP deskphones
  - Avaya one-X® IP Telephones
  - Avaya IP wireless telephones
  - Avaya IP conference phones
  - 96x1 H.323 and 96x1 SIP Deskphones
  - Avaya Attendant Console

For a complete list of supported devices, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Supported servers

You can deploy Communication Manager using the following OVA types:

- **Simplex:** If you want to have only one Communication Manager server in your environment, then you can use simplex OVA.
- **Duplex:** If you want to have a standby Communication Manager server, then you can use duplex OVA. The standby server becomes active when the main server goes down. To deploy the Duplex OVA, install the Duplex OVA on two different hosts. Ensure that the hosts reside on two different clusters.

The following table provides the information about servers compatible with each OVA.

OVA type	Server configuration	Supported server
Simplex	• Main • Survivable Core • Survivable Remote	• S8300D • S8300E • Dell™ PowerEdge™ R610 • Dell™ PowerEdge™ R620 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G7 • HP ProLiant DL360p G8 • HP ProLiant DL360 G9
Duplex	• Main • Survivable Core	• Dell™ PowerEdge™ R610 • Dell™ PowerEdge™ R620 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G7 • HP ProLiant DL360p G8 • HP ProLiant DL360 G9

For information about capacities, see *Avaya Aura® Communication Manager System Capacities Table*.

For information about hardware specifications, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Operating system compatibility

The following table provides information about the operating system versions compatible with the various releases of Communication Manager:

Communication Manager release	Linux version	Kernel version
7.1.x	7.2	3.10.0-327.10.1.el7.AV3.x86_64
7.0.x	6.5	2.6.32-504.8.1.el6.AV3

Note:

Communication Manager uses a modified version of Linux® operating system.

Product compatibility

For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Third-party product requirements

Supported browsers

Communication Manager supports the following web browsers:

- Mozilla Firefox 45 and later
- Microsoft Internet Explorer 11

To view the supported browsers for AWS, see https://aws.amazon.com/console/faqs/#browser_support on the AWS website.

Chapter 4: Performance specification

Capacity and scalability specification

For information about system capacities, see *Avaya Aura® Communication Manager System Capacities Table*.

Traffic specification

In Communication Manager, the processor occupancy or the server occupancy consists of:

- Static occupancy
- Call processing occupancy
- System management occupancy

Due to the fluctuating nature of system management functions, a fixed portion of the total processing capacity is assigned to system management. For all Communication Manager servers, 27% of the total processing capacity of the system is allocated to system management. If the total processor occupancy exceeds approximately 92%, all system management operations are delayed, and subsequent call attempts are rejected.

Considerations:

To ensure that the proposed solution design manages the anticipated traffic load, the Avaya Sales Factory team determines the Communication Manager CPU occupancy. Some of the considerations for calculating the traffic usage are:

- Busy Hour Call Completion (BHCC) for inbound calls.
- Call vectoring, especially for announcements that Communication Manager plays for calls in queue.
- The number of simultaneous active SIP trunks. The active SIP trunks that support calls that are in a queue have a greater impact on the Communication Manager CPU occupancy than the number of active SIP trunks that support calls being handled by agents.
- The Communication Manager release, CPU clock speed, and server duplication mode.
- Computer Telephony Integration (CTI) operations, such as monitoring, adjunct routing, and third-party call control.

- Intelligent Customer Routing (ICR) and Best Service Routing (BSR) operations.

For more information about traffic engineering and specifications, see *Avaya Aura® Communication Manager Solution Design Considerations and Guidelines*.

Chapter 5: Security specification

Communication Manager security, privacy, and safety

Communication Manager provides security features for detecting probable breaches, taking measures to protect the system, notification and tracking activities. It also provides real-time media encryption for environments where enhanced voice privacy over a LAN/WAN is required.

Communication Manager supports:

- Industry Standard Secure Real Time Protocol (SRTP) for authentication and media encryption for both audio and voice media streams. Additionally, SRTCP encryption is supported.
- Real Time Media and Signaling Encryption
- Access Security Gateway
- Malicious Call Tracking
- Toll Fraud protection
- Emergency Calling Services (E911)

You can isolate Communication Manager telephony servers from the rest of the enterprise network to safeguard them from viruses, worms, DoS (Denial of Service) and other attacks. It uses the minimum number of services and access ports to reduce susceptibility to malicious attacks and employs encryption between servers, gateways and endpoints to secure the voice stream and signaling channels.

See *Avaya Aura® Communication Manager Security Design* for further information.

Supported media encryption algorithms

The use of AEA and AES is discouraged as these are older Avaya-proprietary-encryption techniques.

Avaya security recommends to use the following types of encryption techniques:

- srtp-aescm128-hmac80
- srtp-aescm128-hmac32
- srtp-aescm256-hmac80

- srtp-aescm256-hmac32
- none (non encrypted call connection).

In all these encryption algorithms, the system dynamically creates encryption keys for each connection. The system creates the encryption keys within the gatekeeper and transmits the keys to the endpoints and the processing boards over secure links. Additionally, the system produces separate keys for the incoming and outgoing streams of each call. For conference calls, the system assigns a unique pair of keys for encrypting the payload of each endpoint, one for the incoming stream and one for the outgoing stream.

Because all the authentication keys are dynamically created and assigned, the system stores these keys only in RAM. These keys are not accessible by administrators or users. RTP keys are not escrowed.

SRTCP provided the ability to encrypt the control channel associated with the SRTP media stream. These two channels normally reside on adjacent UDP ports.

Key exchange details

Key agreement is performed using Diffie-Hellman techniques.

TLS connections can now be used between Communication Manager and the H.248 or H.323 endpoint gateways.

Chapter 6: Licensing Requirements

Licensing requirements

To use the Communication Manager software, you require a valid Communication Manager license file. Without a valid license file, Communication Manager enters the License Error mode, with a 30-day grace period. If the grace period expires before a valid license file is installed, Communication Manager enters the License Restricted mode. In this mode, you cannot save any administrative changes to Communication Manager.

Communication Manager uses the Avaya PLDS or Product Licensing and Delivery System to manage license entitlements and generate license files. The license file contains information regarding the product, major release, license features, and capacities. Avaya PLDS provides the ability to move licenses between Communication Manager servers if the support offer and the move policy are followed.

Communication Manager uses the Service Pack and Dot Release Guardian technology to protect and control the authorized use of service packs and dot releases. Using this technology, Communication Manager inserts the Support End Date (SED) in the license file and compares it with the publication date of the service pack or the dot release, thus, preventing the use of a service pack or a dot release that has a publication date after the SED.

Virtual appliance licensing on VMware

Each Communication Manager software that is deployed on the VMware platform uses a single instance of WebLM license server to host the license file. The WebLM instance located within System Manager is the first and the preferred WebLM instance.

In a network of multiple Communication Manager systems, each Communication Manager server or Communication Manager software-duplication pair requires a separate license file. Using the Centralized Licensing feature, install the Communication Manager or Communication Manager software-duplication pair license files on System Manager WebLM. You can also install the Communication Manager license files on the standalone WebLM virtual appliance (per Communication Manager/Communication Manager software-duplication pair).

Centralized Licensing

The Centralized Licensing feature is available for most Avaya products. Using the Centralized Licensing feature, you can install up to 600 license files for Communication Manager on a single System Manager WebLM server. After installing a license file for a Communication Manager main server either simplex or duplex pair, you must link the Communication Manager main server to the license file in WebLM.

The Centralized Licensing feature provides the following advantages:

- Eliminates the need to install and configure multiple WebLM servers, one for each Communication Manager main server.
- Eliminates the need to log in to each WebLM server to manage licenses for each Communication Manager main server.
- Reduces the VMware licensing cost for installing and configuring multiple WebLM OVAs on VMware.
- Provides a centralized view of license usage for Communication Manager.

Note:

- The standalone or non-System Manager WebLM server does not support the Centralized Licensing feature.
- The Centralized Licensing feature is optional. Use the Centralized Licensing feature when you have more than one Communication Manager server.

For System Manager and Communication Manager centralized licensing backward compatibility, see http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Chapter 7: Resources

Documentation

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

Title	Description	Audience
Design		
Avaya Aura® Communication Manager Security Design, 03-601973	Describes security-related issues and security features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Solution Design Considerations and Guidelines, 03-603978	Describes the Avaya Aura® solution, IP and SIP telephony product deployment, and network requirements for integrating IP and SIP telephony products with an IP network.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager System Capacities Table, 03-300511	Describes the system capacities for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Maintenance and Troubleshooting		
Avaya Aura® Communication Manager Reports, 555-233-505	Describes the reports for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers, 03-300430	Provides procedures to monitor, test, and maintain an Avaya server or Media Gateway.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers, 03-300431	Provides information to monitor, test, and maintain hardware components of an Avaya servers or Gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel

Table continues…

Title	Description	Audience
Avaya Aura® Communication Manager Server Alarms, 03-602798	Provides procedures to monitor, test, and maintain an Avaya servers.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Denial Events, 03-602793	Describes the denial events listed on the Events Report form.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Toll Fraud and Security Handbook, 555-025-600	Describes the security risks and measures that can help prevent external telecommunications fraud involving Avaya products.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		
Administering Avaya Aura® Communication Manager, 03-300509	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Describes the network connectivity for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Avaya Aura® System Manager	Describes procedures for managing the features that are part of Solution Deployment Manager for Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Implementation and Upgrading		
Deploying Avaya Aura® Communication Manager	Describes the implementation instructions while deploying Communication Manager on VMware.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® applications from System Manager	Describes the implementation instructions while deploying and configuring Solution Deployment Manager for Communication Manager.	Implementation Engineers, Support Personnel, Solution Architects
Upgrading and Migrating Avaya Aura® applications from System Manager	Describes the implementation instructions while deploying and configuring Solution Deployment Manager for Communication Manager.	Implementation Engineers, Support Personnel, Solution Architects
Understanding		

Table continues…

Title	Description	Audience
Avaya Aura® Communication Manager Feature Description and Implementation, 555-245-205	Describes the features that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Screen Reference, 03-602878	Describes the screens that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Call Center Elite Overview and Specification	Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Sales Engineers, Solution Architects, Support Personnel
What's New in Avaya Aura® Release 7.1, 03-601818	Describes the new features for the current release of Avaya Aura®.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Special Application Features	Describes the special features that are requested by specific customers for their specific requirement.	Sales Engineers, Solution Architects, Avaya Business Partners, Support Personnel

Finding documents on the Avaya Support website

Procedure

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

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

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**.

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

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

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

Busy Hour Call Completions	A measure of dynamic traffic calls that can be completed in an average busy hour.
Call Admission Control	A method of limiting voice traffic over a particular link in a network.
Codec	A coder and decoder (Codec) is a device that encodes or decodes a signal.
Communication Manager	A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.
S8300	A Communication Manager server supporting medium-sized customers.
Session Manager	An enterprise SIP proxy registrar and router that is the core component within the Avaya Aura® solution.
System Manager	A common management framework for Avaya Aura® that provides centralized management functions for provisioning and administration to reduce management complexity. System Manager can also function as a self-signed Root Certificate Authority (CA) or as an intermediate CA. System Manager enables the Simple Certificate Enrollment Protocol (SCEP) application to sign certificates for Avaya deskphones.

Index

R

S

T

V

W