Avaya Aura® Session Manager Overview and Specification

Release 7.1.3
Issue 5
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.

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

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document describes tested Avaya Aura® Session Manager characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.

This document is for anyone who wants to gain a high-level understanding of the Avaya Aura® Session Manager features, functions, capacities, and limitations.

Change history

Issue	Date	Summary of changes
Issue 5	May 2018	• Added support for VMware vSphere ESXi 6.7. • Introduced ability to selectively enable or disable security hardening. • Added support for User-to-User information in CDR.
Issue 4	December 2017	• Introduced Extended Security Hardening. • Updated the document for user registration export enhancement. • Added a support for collecting CPU statistical data.
Issue 3	August 2017	• Introduced emergency calling application sequence. • Introduced a new tab for regular expression pattern rules under implicit user administration.

Table continues…

Issue	Date	Summary of changes
		• Introduced ability to reboot SIP phone through System Manager web services API. • Introduced backup and restore of pluggable adaptation module parameters. • Added KVM support.

Chapter 2: Overview

Avaya Aura® Session Manager is a SIP routing tool that integrates all SIP devices across the entire enterprise network.

Session Manager simplifies the existing communication infrastructure by combining existing PBXs and other communications systems, regardless of the vendor, into a cohesive, centrally managed, SIP-based communications network.

Specifically, Session Manager provides:

- Integration with third-party equipment and endpoints to normalize disparate networks.
- Centralized routing of calls using an enterprise-wide numbering plan.
- Centralized management through System Manager, including configuration of user profiles and deployment of enterprise-wide centralized applications.
- Interconnection with Communication Manager and Avaya Communication Server 1000 to provide multiple feature support for SIP and non-SIP endpoints.
- Interconnection with IP Office through SIP to provide feature support for SIP endpoints.
- Third-party E911 emergency call service for enterprise users.
- Centralized Presence Services for scale and reduced network complexity with a variety of endpoints and communication servers.
- Support for converged voice and video bandwidth management.
- Application sequencing capability to incrementally deploy applications without needing to upgrade the PBX.
- Geographic redundancy.
- Mobility of SIP telephones and enterprise mobility for SIP users.

Supported servers

Session Manager supports the following servers:

- Dell™ PowerEdge™ R610
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630

- HP ProLiant DL360 G7
- HP ProLiant DL360p G8
- HP ProLiant DL360 G9

Branch Session Manager supports the following servers:

- Dell™ PowerEdge™ R610
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G7
- HP ProLiant DL360p G8
- HP ProLiant DL360 G9
- S8300D
- S8300E

These supported servers are only for Appliance Virtualization Platform configurations.

Avaya no longer supports the S8510 and S8800 servers. Any S8510 or S8800 server can be migrated to a supported server using the server replacement procedure.

Note:

Switching cables within a network is must for a Session Manager instance prior to release 7.0.

Supported virtualized environments

Session Manager supports the following virtualized environments:

- VMware® vCenter
- VMware® vSphere
- Avaya Aura® Appliance Virtualization Platform from System Manager Solution Deployment Manager or the Solution Deployment Manager client
- Amazon Web Services
- Kernel-based Virtual Machine

Features

Application Sequencing

With Application Sequencing, you can define and manage a set of applications for call sequencing based on the communication profile of the user. Each application in a sequence processes all requests to deny, modify, or forward initial SIP requests. Some examples of sequenced applications are:

- Billing Service
- Voice Monitoring
- Communication Manager Feature Server
- Call Blocker
- Personal assistant
- Meeting Coordinator

Call Detail Recording on Session Manager

The Call Detail Recording (CDR) feature records information on calls. When you enable CDR, the CDR records are saved in a special directory on the local hard drive of the server.

The call record contains information regarding:

- The time of the call
- The duration of the call
- The dialed number
- The calling party
- The terminating SIP entity
- The originating SIP entity
- The bandwidth indicator

For each Session Manager, you can administer CDR as either disabled or enabled. CDR records are created if you enable the CDR in at least one of two Session Manager entities.

Note:

Survivable Remote Session Manager (Branch Session Manager) does not support CDR.

CDR records on Session Manager are created on connected calls.

In route-through scenarios, where one Session Manager routes directly to another Session Manager, CDR is generated only on the originating Session Manager if so administered, not on the terminating Session Manager.

For sequenced applications (implicit or administered for a user), only one CDR record is generated for a given call.

If the secondary Session Manager of a user receives a call, the call is routed to the primary Session Manager of the user as per user registration. In that case, the CDR is still generated on the secondary Session Manager and not on the primary Session Manager.

Centralized applications

Session Manager provides connectivity for centralized Avaya applications such as Avaya Aura® Messaging, Avaya Voice Portal, Avaya Aura® Conferencing, and Avaya Meeting Exchange™. Each PBX, gateway, or location connects to the centralized application through Session Manager rather than individually. Session Manager also connects to SIP-enabled adjuncts, making the management and deployment of adjuncts much simpler than methods where each PBX connects to its own adjunct.

Centralized SIP trunking

Centralized SIP trunking routes all network traffic, including branch site traffic, through the enterprise core site. Session Manager provides redundant connections to a SIP service provider using the Gateway or Session Border Controller (SBC).

Customers can use centralized SIP trunking to save on operational costs. However, the setup should have more than one hub-site to avoid the risk of a single point of failure.

SIP Endpoint Concentrator Connection Policy

To inter-operate with virtualized desktop solutions such as a Citrix server hosting 1xC, the Endpoint Concentrator (endpt conc) connection policy provides for up to 1000 connections from a single IP address.

You can assign the Endpoint Concentrator connection policy to a SIP entity link. The Session Manager (ASSET) allows up to 1000 connections on that SIP entity link.

The Endpoint Concentrator policy is an untrusted policy based on the current **Default** (endpoint) policy. The requests arriving over the SIP entity link with the **endpt conc** connection policy are challenged similar to any other endpoint.

When the customer administers a SIP entity as an **Endpoint Concentrator** on the SIP entity page, all subsequently added SIP entity links towards that entity will have the **endpt conc** connection policy by default.

The **endpt conc** policy cannot be used for remote office (REMO) configurations. With a REMO configuration, the Session Border Controller servers use a single connection in the SIP entity link towards Session Manager to multiplex multiple calls. For such configurations, the connection policy must allocate large amounts of memory and buffers for a single connection.

Note:

SIP Link Monitoring is not available for SIP entities of type **Endpoint Concentrator**.

Inter-gateway Alternate Routing for SIP endpoints

Inter-gateway Alternate Routing (IGAR) provides voice connectivity using a public service provider (PSTN) if not enough bandwidth is available on the private network. If the Corporate Data Network cannot handle the call, the bearer connection is routed over the Public Voice Network.

You can use IGAR when calling to or from a SIP endpoint that is registered to a Session Manager server.

The IGAR triggers include:

- The inter-branch bandwidth limit is reached.
- IGAR is always on for branches with low-bandwidth connectivity.

The source and destination of the call must be associated with the same Communication Manager. Video calls are automatically downgraded to audio if IGAR is triggered.

Use cases:

- Case #1: Vijay in Bangalore and Michael in London both have SIP endpoints and are served by Communication Manager. At peak hours, bandwidth between Bangalore and London is insufficient to carry audio calls with proper quality. With IGAR, Communication Manager automatically sends the audio media over the PSTN, ensuring excellent audio for the call.
- Case #2:

  An enterprise has a small branch gateway in Reykjavik with all SIP endpoints registered to an Avaya Aura® data center in Stockholm. The low-cost data connection to Iceland has insufficient bandwidth to carry more than a few audio calls. With IGAR, every call to or from Reykjavik is carried over a low-cost PSTN connection using the “always on” option.

Limit Number of Concurrent Calls for SIP endpoints

The Limit Number of Concurrent Calls (LNCC) feature causes a multi-call appearance endpoint to behave as a single line appearance endpoint. When the LNCC feature is enabled and the user is active/busy on one call appearance, subsequent incoming calls receive a busy signal or follow normal busy treatment such as coverage and are tagged as missed calls.

LNCC works on all H.323 and DCP endpoints and any SIP endpoint that supports call appearances.

A user controls this feature using a feature button or feature access code (FAC). Normal operation allows two incoming calls. The user must enable LNCC to allow only one call.

LNCC allows:

- outgoing calls, incoming priority calls, and emergency callback for SIP stations.
- outgoing calls, incoming priority calls, emergency callback, and crisis alert for H.323 and DCP stations.

LNCC works with the Dual Registration and Multiple Device Access features. The user applies LNCC at the user level, and all devices associated with the user inherit the LNCC feature. For example:

- Most of the time, Steve wants to be active on only one call at a time, so he activates LNCC.
- Andy calls Steve, and they talk for 15 minutes.
- During their conversation, Cindy calls Steve. Because LNCC is active, Cindy's call goes straight to coverage.
- Cindy does not leave a message, but Steve's endpoint still records her call as a missed call. Steve calls Cindy after he finishes his conversation with Andy.

The LNCC feature administration field appears on the station screen and is saved as part of the station record by the **`save translations`** command. Subsequent resets restore the LNCC settings to the state when the **`save translations`** was performed. A user activates and deactivates the feature by using the limit-call feature button or by using two Feature Access Codes: **Limit Number of Concurrent Calls Activation/Deactivation**. The limit-call button indicates whether the LNCC feature is active or not.

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

Normalization of disparate networks

Session Manager normalizes and adapts disparate SIP protocols to meet the strict SIP standards of the network. With normalization of disparate networks, third-party PBXs work with each other and with Avaya equipment enabling customers to realize true vendor interoperability.

For example, Cisco and other PBXs can connect with Session Manager and operate with each other and with Avaya equipment. Session Manager converts the headers in SIP messages that display calling and called-party information in the format required by each switch in a call.

Online/Offline Call Journal (Call History)

The call log of a device includes incoming calls when the device is not logged in. In addition, if a call cannot be delivered to an endpoint due to the Limit the Number of Concurrent Calls (LNCC) feature, the calls is also logged.

- For H.323 endpoints, Communication Manager stores logged out missed calls and downloads the Call History logs when the endpoint logs in. The maximum number of H.323 Call History logs is 10.

- For SIP endpoints, the primary Session Manager stores all call logs and downloads the logs to the endpoint during login. The endpoint maintains the logs locally while logged in.

Call logs are only stored on the primary Session Manager of the user. There is no redundancy for storing call logs. The primary Session Manager stores the call logs in the User Data Storage database.

You enable Call History logging on the Session Manager Communication Profile for the user by enabling **Enable Centralized Call History**. The default is **off**. The maximum number of call logs per Communication Profile is 100.

SIP phones:

- Download call logs during login only.
- Maintain call logs locally while logged in.

Personal Profile Manager

The Personal Profile Manager (PPM) maintains and manages the personal information of the end user in the system. SIP endpoints communicate with PPM to:

- retrieve configuration information such as dial plans, buttons, and contact lists.
- add or update contacts.
- save device-specific data.

The PPM provides an interface for endpoints to attach to the network to download profile data and store data back in the network for easy access across multiple user devices.

Policy-based routing

Customers can use Session Manager to define the routing policy. The routing policy controls when calls are made, how the call load is balanced, and how calls are routed during network failures.

- **Least-cost routing**, also called time-of-day routing, uses the lowest cost route from a list of service providers on a time-of-day or time-of-week basis.
- **Alternate routing** routes calls around network failures on a global basis and uses global PSTN fallback when the internal network is unavailable.
- **Load balancing** distributes calls. For a given SIP entity, you can administer Session Manager to select a host from multiple IP addresses based on administered priorities and weights.
- **Call admission control** reroutes calls when the bandwidth allocation for WAN link is exceeded.

System Manager Web Services

The System Manager Web Services interface for routing and dial plan management provides remote programmatic access for querying, creating, and deleting all Session Manager routing domain data. The routing data that the service accesses and modifies is the same routing data supported by the routing bulk import and administration GUI. The primary routing domain data types are:

- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expression data

The System Manager Web Services API enforces the same level of data integrity as the GUI and import interfaces. The API components enforce the same validation logic the GUI and Import interfaces use.

Use the System Manager Web Services interface for provisioning only. Do not use the Web Service API for real-time application access or SIP application integration. The System Manager Web Service API is appropriate for automating normal administrative tasks and has the same administration data propagation delay to Session Managers as the Routing GUI and bulk import interfaces. The System Manager Web Services API also allows re-booting of SIP phone.

The System Manager Web Services API uses RESTful current best practices. The service provides for XML payloads by default but can optionally support JSON payloads.

Users can select any desired REST client implementation technology. Users must have Web Service development level skills for REST client development.

The System Manager Web Services interface documentation includes a programmers guide, detailed schema definition, and examples and samples.

Hunt Group Log in/Log out button for SIP phones in a non-CC Environment

When the Unified Communications (UC) users in customer configurations are members of a department hunt group, they need to log in and out of the hunt group and see a visual indication of their status.

Session Manager has a Hunt Group Log in/Log out button, with which you can:

- Log in and out from receiving calls distributed in a hunt group.
- Activate or deactivate the feature with a single button click by using the Hunt Group Log in/Log out toggle-button.
- See the status of feature activation. A visible indicator is available to show the status, whether the feature is turned on or off.

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

Session Manager and Avaya Aura® Device Services integration

Avaya Aura® Device Services overview

Avaya Aura® Device Services is co-resident with Session Manager, but it is delivered as a separate OVA. You can deploy Avaya Aura® Device Services through Amazon Web Services (AWS), VMware, or Solution Deployment Manager.

Avaya Aura® Device Servicesprovides the following services to the Avaya Equinox® clients:

- **Contact:** To use the contact service, a user must be provisioned on the user on LDAP Server. Using the contact service, you can:
  - Add, update, and delete a contact.
  - Perform an enterprise search for contacts.

    Avaya Aura® Device Services supports directory searches of up to 300 contacts. The number of contacts displayed in the search results varies for each client.
  - Set and retrieve information, such as, preferred names or pictures. Using the Picture service, you can create, override, delete, and update the user pictures. You can also include these picture URLs in the contact information or search results.
  - Search and retrieve information about Avaya Scopia® users and terminals.

    You can use Avaya Aura® Device Services to search for Avaya Scopia® users and terminals only when Avaya Equinox Management address is configured on Avaya Aura® Device Services.
- **Notification:** The Notification service provides a common infrastructure that allows a client or endpoint to subscribe to receive events from a number of service resources using a single connection.
- **Dynamic Configuration:** The Dynamic Configuration service provides discovery of configuration settings to UC Clients. You can customize these settings on a global, group, individual, or platform basis. The Dynamic Configuration service uses the automatic configuration feature of Avaya Equinox® to facilitate the configuration details to the UC clients. This helps the user to avoid manual configuration of their client. To log in to the client, the user needs to provide their email address or Windows user ID, along with their enterprise credentials.

- **Web Deployment:** The Web Deployment service publishes and deploys UC client updates to end user devices. The Web Deployment service is supported on the Avaya Equinox® desktop clients.

Cassandra clustering and data replication overview

If the **Enable Data Storage Cluster** field on the Session Manager Administration page is selected, all Session Managers are added to the Cassandra database cluster.

If the **Enable Data Storage Cluster** field is not selected, all the Cassandra nodes run in standalone mode.

Cassandra clustering should be done only when Avaya Aura® Device Services servers are configured and paired with Session Manager.

Cassandra data distribution uses the administration on the User Data Storage page to identify the Session Manager instances that are within the same datacenter.

For administering Cassandra data distribution:

1. Enable data storage clustering.
2. Create a data center.
3. Assign co-located Session Managers to the data center.
4. Add the Avaya Aura® Device Services instance to the inventory.
5. Pair a Session Manager instance with an Avaya Aura® Device Services node.

Add/remove skill button

Add/remove skill button

Personal Profile Manager (PPM) supports download of an assigned add/remove skill button on 96x1 SIP phone when the phone registers to Session Manager.

Agents or supervisors can use add/remove skills button to add or remove an assigned skill.

Communication Manager prompts the agent while adding or removing a skill and displays the updated set of skills.

For more information about Add/remove skill button, see *Avaya Aura® Call Center Elite Feature Reference*.

TLS mutual authentication for SIP endpoints

Session Manager provides validation of the endpoint Transport Layer Security (TLS) certificate. This authentication is applicable to SIP and HTTP traffic.

Session Manager provides the ability for administrators, while authenticating SIP devices, to choose the following:

- No Mutual Authentication
- Optional Mutual Authentication
- Mandatory Mutual Authentication

The **TLS Endpoint Certificate Validation** field has three options:

- **None**: No mutual authentication occurs. There is no certificate validation and SIP endpoint can establish the connection.
- **Optional**: Communication occurs if the endpoint presents a valid certificate or otherwise.
- **Required**: Communication occurs only if the endpoint presents a valid certificate trusted by Session Manager.

The default setting for the upgrades, as well as new installations, is optional mutual authentication. You can decide to change the setting to no or mandatory mutual authentication. If you select mandatory mutual authentication for the **TLS Endpoint Certificate Validation** field, Session Manager rejects the connection request if:

- a client does not provide a certificate or,
- the client certificate is invalid or not trusted by Session Manager.

Note:

If you select the **Required** option for Session Manager 7.0 or earlier, it results in the **Optional** option to support backward compatibility.

Implementation of the new TLS validation policy supports network configuration of Session Manager 7.0 and later with the earlier versions of Session Manager or Branch Session Manager.

Chapter 3: New in this release

The following sections describe the new features and enhancements for Avaya Aura® Session Manager Release 7.1.3.

Ability to enable or disable AIDE

With Session Manager Release 7.1.3, you can selectively enable or disable Advanced Intrusion Detection Environment (AIDE). By default, AIDE is disabled.

For more information, see *Administering Avaya Aura® Session Manager*.

Added a support for ESXi 6.7

Starting with the Release 7.1.3, Avaya Aura® Session Manager supports VMware vSphere ESXi 6.7.

Support for User-to-User information in Session Manager CDR

From Release 7.1.3, Session Manager is enhanced to capture the contents User-to-User header, which contains the UCID value. The XML based CDRs are enhanced to support this function. When Session Manager receives INVITE request with User-to-User header, Session Manager copies the content of User-to-User in to the *uu-info* element of the CDR XML file.

Security hardening

With Session Manager Release 7.1.2, you can enable or disable the following profiles for Session Manager:

- Standard
- Hardened
- Custom

For more information, see *Administering Avaya Aura® Session Manager*.

User registrations export enhancement

With Session Manager Release 7.1.2, a new **Start Export Job** button is added on the User Registration Export page for exporting more than 100,000 user registrations.

The system schedules the job to run immediately. After the job is complete, you can download the exported file with the registration data.

For more information, see *Administering Avaya Aura® Session Manager*.

Support for collecting CPU statistical data

With Session Manager Release 7.1.2, the **CPU** tab is restored on the System Performance page to collect the CPU statistical data. Earlier the **CPU** tab was available on the Session Manager Release 7.0 system. User can generate CPU Usage report which includes the following details:

- User
- System
- Idle
- IO Wait

For more information, see *Administering Avaya Aura® Session Manager*.

Emergency Calling Application Sequence

In the release 7.1.1, administrators can enable application for emergency calls. Administrators can assign emergency calling application sequences to a user.

For more information, see *Administering Avaya Aura® Session Manager*.

Regular Expression Pattern Rule

In the release 7.1.1, a new tab for regular expression pattern rules is introduced on the Implicit User Rule Editor page. This tab enables the administration of application sequences for emergency calling using regular expression based pattern rules.

For more information, see *Administering Avaya Aura® Session Manager*.

Ability to reboot SIP phone through Avaya Aura® System Manager API

The System Manager Web services interface allows remote rebooting of SIP phone.

The System ManagerWeb services interface provides programmatic access to the Session Manager dashboard and user registration data for querying, creating, and deleting all Session Manager routing domain data.

The System Manager Web Services API enforces the same level of data integrity as the GUI and import interfaces. The API components enforce the same validation logic the GUI and Import interfaces use.

The System Manager Web Services API is available on the Avaya DevConnect Web site at https://www.devconnectprogram.com/site/global/home/p_home.gsp.

KVM Support

From release 7.1.1, Avaya Aura® Session Manager supports Kernel-based Virtual Machine (KVM). You can now deploy Avaya Aura® Session Manager on Kernel-based Virtual Machine (KVM). Kernel-based Virtual Machine (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.

Backup and restore of pluggable adaptation modules

From the release 7.1.1, Session Manager supports backup and restore of pluggable adaptation module parameters. Pluggable adaptation module parameters are preserved during the upgrade of Session Manager.

IPv6 support

From Release 7.1, Session Manager supports IPv6 addresses in addition to IPv4 addresses. Session Manager supports a dual stack architecture. Therefore, Session Manager can be simultaneously connected with endpoints and SIP entities that use IPv4 and IPv6 addresses. When one party in a call uses IPv4 addressing and the other party uses IPv6 addressing:

- Session Manager provides signaling interworking
- Communication Manager provides media interworking

A large variety of address type combinations are possible in SIP signaling. For example, messages can have:

- Only IPv4 addresses
- Only IPv6 addresses
- A mixture of IPv6 and IPv4 addresses

In addition, the address family used in media stream negotiations is independent of the SIP signaling address family. Session Manager functions as the registrar and interconnecting agent to connect SIP entities of different types. Therefore, Session Manager must handle signaling interworking to ensure that a network comprising mixed address family elements works properly. Before forwarding a SIP message to the next SIP entity or endpoint, Session Manager uses the Address Family Interworking Function (AFIF) to adapt the SIP messages to meet the needs of the next hop. For example, consider that an incoming message has IPv4 addresses and the destination SIP entity supports only IPv6 addresses. Session Manager uses AFIF and replaces the IPv4 addresses with IPv6 addresses in the request. Similarly, after receiving a response, Session Manager uses AFIF to reverse the adaptation and converts the IPv6 messages to IPv4 messages.

Session Manager uses the address family of the SIP entity or endpoint and the type of the link to determine their address type and then uses AFIF.

Complex Station Access Code

In Session Manager, administrators can set up a **Station Admin Password** to ensure secure log in and administration of the SIP phone. Before Release 7.1, Session Manager accepted only numeric values up to 32 digits in the **Station Admin Password** field.

From Session Manager Release 7.1, the administrator can define the Complex Station Access Code validation rules using the Station Access Code Policy screen on the Device and Location Configuration page. The administrator can establish parameters to define the access codes, such as minimum length, allowed characters, and inclusion of minimum character sets.

The administrator can set a numeric Station Admin Password and Complex Station Access Code simultaneously. Therefore, the system can support End of Sale (EOS), End of Life (EOL), and earlier endpoints along with new endpoints. Session Manager uses Complex Station Access Code

for SIP 96x1 and Avaya J100 Series IP Phones. For desk phones earlier than 96x1, the system continues to use the numeric Station Admin password.

Complex Station Access Code is encrypted using encryption algorithm ensuring code security.

Station Access Code policy constraints

- The administrator must define the minimum required length from 6 to 25 characters.
- The administrator must define one of the following:
  - Minimum character set. Administrator can choose any combination from the following character sets:
    - Upper case
    - Lower case
    - Numerics
    - Special characters
  - Minimum required characters for each character set.

  For example, set the **Minimum character set** field to 0 and **Upper case** and **Special character** set to 1. In this case, any password containing one upper case and special character is a valid Station Access Code.

  If you set the **Minimum character set** field to 2, the password must contain at least two characters from the numeric, upper, or special character sets.
- The administrator must ensure that the minimum required length is equal to or greater than the number of characters required for each character set.

Note:

If a password does not meet the password strength policy, the Device and Location Settings group administrator rejects the password.

Ability to disable TLS versions

Session Manager supports TLS versions 1.0, 1.1, and 1.2. TLS version 1.0 is the least secure, while version 1.2 is the most secure. Based on the capability of the SIP entity, the system negotiates and establishes the highest common TLS version. For example, if the SIP entity supports TLS version 1.0, then after capability negotiation Session Manager establishes a connection with TLS version 1.0. Negotiating a lower TLS version might not be acceptable to customer configurations that have known vulnerabilities.

With Session Manager Release 7.1.3, a system administrator can define the minimum allowed TLS version for the global SIP entity and for each SIP entity. In some scenarios, the SIP entity does not support a TLS version equal to or above the minimum allowed TLS version. In this case, the SIP entity cannot establish a connection with Session Manager.

Session Manager Release 7.1.3 adds two global policies that govern the minimum allowed TLS versions for the SIP Entities and SIP endpoints respectively. For more information, see *Administering Avaya Aura® Session Manager*.

When negotiating TLS versions, Session Manager starts with the latest TLS version. However, the system allows the version downgrade only up to the global policy defining the minimum allowed TLS version. For example, a customer does not want to allow TLS connections with the SIP Entities earlier than version 1.1. The administrator can accordingly set the global policy of minimum allowed TLS version for SIP Entities to 1.1. This ensures that Session Manager allows TLS connections with the SIP Entities at a minimum of TLS version 1.1 or later.

To ensure that upgrades are non-interruptive, the value of this setting after upgrade is set to 1.0. You must manually change the minimum allowed TLS version when required. For new installations, the version is set to version 1.2 by default.

OVA signing

OVA signing is a new security feature in Session Manager Release 7.1.3. OVAs are digitally signed to ensure file integrity.

Enhanced Access Security Gateway

Session Manager supports Enhanced Access Security Gateway (EASG), an authentication interface that secures the system administration and logins on the system. EASG provides a secure method for Avaya services personnel to access the Avaya Aura® applications 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 uses a challenge and response protocol to confirm the validity of a user. This process reduces the opportunity for unauthorized access.

From the Session Manager Dashboard screen, you can enable or disable EASG for all supported users. To enable or disable EASG for individual users, you must use the command line interface. Enabling EASG globally through System Manager does not override the EASG disabled setting for individual users.

Certificate Revocation Lists

Digital Certificates identify communication entities in a Public Key Infrastructure (PKI). Certificate Authorities (CAs) issue certificates with a validity period. During validation, communicating entities ensure the certificate has not expired and also check the revocation status of the certificate. At times, the issuing CA might want to revoke the certificate before it expires. For example, when an employee leaves the company, the CA must revoke the certificates issued to that employee to avoid misuse. Session Manager 7.1 uses the Certification Revocation List (CRL) method for checking certificate revocation.

CRLs contain a list of serial numbers for certificates that are revoked. Entities with a revoked certificate must no longer be trusted. To revoke a certificate:

- The Certificate Authority (CA) administrator can log on to a CA and revoke the certificate.
- The CA publishes the CRL to an HTTP or LDAP repository referenced in the CRL Distribution Point (CDP) extension of a certificate.

Session Manager performs the required certificate revocation checks based on the global Certificate Revocation Check policy that is configured on System Manager.

If Certificate Revocation Checking is enabled, every certificate exchanged while establishing a TLS connection is verified against a CRL. Before using a CRL, Session Manager verifies the validity of CA's digital signature in a CRL.

System Manager provides the ability to periodically download CRLs in advance to make them available before a TLS connection is attempted. If a CRL is not previously downloaded, the system might attempt to download the CRL when trying to establish a TLS connection. In that case, the system attempts to download the CRLs from the URI specified in the certificate's CRL Distribution Point (CDP) extension. Multiple CDP locations may be included in the CDP extension. If multiple CDP locations are specified, an attempt is made to download a CRL from the first location, followed by the next location, and so on, until the system either downloads a CRL or times out.

CRL revocation checking options

The following CRL revocation checking options are available:

- Mandatory: The certificate is considered valid if all CRLs in a certificate chain can be fetched and no certificate is present on any CRL.
- Best effort: The certificate is considered valid if none of the CRLs in a certificate chain that have been fetched indicate that the certificate has been revoked, or if CRL cannot be fetched.
- Off: No CRL revocation checking is performed.

Assured Services SIP

Session Manager supports the Assured Services SIP feature by using a combination of different features. Administrators can enable or disable the Assured Services SIP feature using a Session Manager global setting and configuring the supported network domain. By default, the feature is disabled.

Multilevel Precedence and Preemption

Session Manager allocates bandwidth to calls based on the priority of the calls. Session Manager determines the priority of the call from the Resource-Priority header in the Invite request. If Session Manager does not have adequate bandwidth to allocate to a high-priority call from the specific domain that is configured for precedence, Session Manager preempts one or more lower-priority calls. Preempting lower-priority calls frees up the associated bandwidth, allowing Session Manager to ensure that adequate bandwidth is available to successfully establish high-priority calls.

Assured Services Admission Control

Assured Services Admission Control assigns bandwidth limits for audio and video to network entities and links. Assured Services Admission Control also monitors the bandwidth usage and ensures that the bandwidth used by network entities and links does not exceed the specified limits.

Assured Services for SIP IP gateway

The Assured Services SIP IP gateway supports the insertion of necessary routes between Enterprise Session Controllers and Local Session Controllers which are connected with soft switches and SBCs. Session Controllers insert a primary route, which passes through a designated set of SBCs, when processing calls to the primary soft switch. The insertion of the primary route ensures that the routes of all calls are established through the set of SBCs. If the primary route components or the network fails, Session Controllers detect the failure using the SIP OPTIONS method. Session Controllers establish all subsequent calls using the alternate route to the secondary soft switch that passes through a secondary set of SBCs.

Ping-pong based health check mechanism

From Release 7.1, Session Manager provides the client and server side support of the ping-pong based health check mechanism for SIP entities. Previously, Session Manager only provided the server side support for endpoint connections. The administrator can enable and disable ping-pong based health monitoring at the SIP Entity level with the SIP entities. Session Manager as a client generates a ping or a double Carriage Return and Line Feed (CRLF). The response to a ping is a pong or a single CRLF response. If the Session Manager does not receive a pong response, it will mark the SIP Entity as down. Session Manager waits up to 10 seconds to receive a pong in response to a ping it sent out.

By default, the ping-pong based health monitoring is disabled. When ping-pong based health monitoring is enabled, the administrator can set the ping interval between 1 and 900 seconds. The

default value of the ping interval is 120 seconds. After the ping-pong based health monitoring is enabled, Session Manager can send a periodic ping at the administered level.

Chapter 4: Capacity limits

Capacity limits for Session Manager Footprints

The following table summarizes single Session Manager capacities for all Session Manager footprints.

Note:

The capacities listed here are only for Session Manager. For information about capacity limits for AADS, see the AADS documentation.

Important:

In Session Manager 7.1 the concurrently registered device capacity of Session Manager Profile 1 is reduced from 2500 devices to 2000 devices. Session Manager systems administered with more than 2000 devices before upgrading to 7.1 must understand the usage. If the system requires more than 2000 concurrent registrations the system must re-administer to reduce the number of devices. This might require adding an additional Session Manager server, or increasing the footprint by using a higher Profile on the existing server.

Session Manager Device Footprints	Up to 2K Devices	2K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices (R1 footprint)	10K to 23.5K Devices (R2 footprint) * see note
CPU Minimum	2300MHz, Hyper-threaded				
vCPUs	3	5	8	12	20
CPU MHz Reservation	3450	5750	9200	13800	23000
Memory Reservation	4GB	5GB	8GB	10GB	18GB
Shared NICs	Four virtual NICs @ 1000 Mbps, used for: • Management (eth0) • Services Port (eth1) • ASSET (eth2) • NIC bonding (eth3)				
SIP Devices (Normal/Failure)	2K/2.4K	4.5K/5K	7K/8K	10K/12K	23.3K/ 25K

Table continues…

Session Manager Device Footprints	Up to 2K Devices	2K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices (R1 footprint)	10K to 23.5K Devices (R2 footprint) * see note
CC Agents (Normal/ Failure)	1.6K/2K	3.75K/4166	5.8K/6666	8333/10K	18K/21K
Presence Users (Normal/Failure)	2K/2.4K	4.5K/5K	7K/8K	10K/12K	18K/21K
Sessions (Sec/ Hour/Max)	20/72K/ 17.9K	45/162K/37.4K	70/256K/59.8K	100/360K/90K	150/540K/ 170K
HDD (GB)	90	90	125	125	175
HDD (GB) (If the deployment is using Solutions Deployment Manager)	90	90	150	150	225

Note:

Session Manager Footprint 5 is only supported on Avaya Common Server Release 2, Release 3 and onward and not supported on Release 1.

Session Manager instances are intended to operate as redundant, homogeneous servers to provide high reliability if a Session Manager failure or a network component failure occurs. Each Session Manager should have similar system resources and a balanced number of devices.

Session Manager instances must be similarly sized in both processing power and available memory to accommodate distributions of devices during failover. Small and large footprints are not intended to be mixed in a solution. However, closely sized footprints, such as one size with the next size down in the table above, can be mixed temporarily as capacities increase. You must ensure that the number of devices failing over to a smaller footprint does not exceed the device capacities of that footprint.

You can implement a system that consists of a mixture of Session Manager instances hosted on VMware platforms as well as Session Manager instances hosted on the existing non-VMware platforms. You must configure the VMware-based Session Manager to be similar to the non-VMware-based Session Manager across the enterprise. Similar configurations ensure the best use of system resources and handling failover scenarios. Be careful when configuring the system where a large non-VMware Session Manager can failover to Session Manager running in VMware environment. You must ensure that the target Session Manager can handle the total capacities.

A single 350K SIP device solution supports a geo-redundant Session Manager configuration of up to 28 Session Manager instances that are interconnected and aware of each other. Configurations that exceed this limit are not expected to have problems, but these configurations are not guaranteed to be supported.

The following table summarizes the number of soft clients supported per Session Manager when the softclients are using Avaya Aura® Device Services.

Session Manager profile	Total SIP devices	Number of Equinox devices	Previous Equinox devices
Profile 1	2,000	1,200	750
Profile 2	4,500	2,700	1350
Profile 3	7,000	4,200	2100
Profile 4	10,000	6,000	3000
Profile 5	23,300	13,900	5240

Capacity limits for Branch Session Manager Footprints

The following table summarizes single Branch Session Manager capacities for all Branch Session Manager footprints.

Branch Session Manager **Device Footprints**	**Up to 1K Devices (also for CSR1 upgrades up to 2k)**	**1k to 5K Devices**
vCPUs	2	4
CPU Reservation	2300 MHz	4600 MHz
Memory	2 GB	3.5 GB
Memory Reservation	2 GB	3.5 GB
CC Agents Max	583	4167
Sessions (Sec/Hour/Max)	3/10.8K/4.8K	30/108K/35K

Branch Session Manager instances are intended to operate as redundant, homogeneous servers to provide high reliability if a Branch Session Manager failure or a network component failure occurs. Each Branch Session Manager should have similar system resources and a balanced number of devices.

Branch Session Manager instances must be similarly sized in both processing power and available memory to accommodate distributions of devices during failover. Small and large footprints are not intended to be mixed in a solution. However, closely sized footprints, such as one size with the next size down in the table above, can be mixed temporarily as capacities increase. You must ensure that the number of devices failing over to a smaller footprint does not exceed the device capacities of that footprint.

You can implement a system that consists of a mixture of Branch Session Manager instances hosted on VMware platforms as well as Branch Session Manager instances hosted on the existing non-VMware platforms. You must configure the VMware-based Branch Session Manager to be similar to the non-VMware-based Branch Session Manager across the enterprise. Similar configurations ensure the best use of system resources and handling failover scenarios. Be careful when configuring the system where a large non-VMware Branch Session Manager can failover to Branch Session Manager running in VMware environment. You must ensure that the target Branch Session Manager can handle the total capacities.

A single 350K SIP device solution supports a geo-redundant Branch Session Manager configuration of up to 28 Branch Session Manager instances that are interconnected and aware of each other. Configurations that exceed this limit are not expected to have problems, but these configurations are not guaranteed to be supported.

Chapter 5: Interoperability

Product compatibility

For the latest and most accurate compatibility information, see https://support.avaya.com/CompatibilityMatrix/Index.aspx on the Avaya Support website.

Accessing the Compatibility Matrix

The Compatibility Matrix provides compatibility information of the Avaya products that are supported with the various releases of Session Manager.

Note:

The screen refreshes each time you make a selection.

Procedure

1. Access the Compatibility Matrix page at https://support.avaya.com/CompatibilityMatrix/Index.aspx.
2. Scroll to the bottom of the page and select **Avaya Aura® Session Manager** from the **Product** drop-down menu.
3. When the page refreshes, scroll to the bottom of the page and select the appropriate release from the **Release** drop-down menu.
4. Scroll to the bottom of the page and do one of the following:
   - Select a product from the product drop-down menu to view only the compatibility for a particular product with Session Manager.
   - Click the red **(ViewAll)** link under the **Avaya Products Compatible with Avaya Aura® Session Manager**.

Supported Avaya endpoints

For information about the Avaya endpoints that Session Manager supports, see https://support.avaya.com/CompatibilityMatrix/Index.aspx on the Avaya Support website.

Chapter 6: Licensing requirements

For licensing, Branch Session Manager and core Session Manager require:

- Product Licensing and Delivery System (PLDS) for license entitlement management, license activation, and license file delivery.
- Web License Manager (WebLM) in the System Manager for license management, including the use of the standalone WebLM server.

You can download the license file from PLDS and install the license as well as the authentication file. Alternately, Avaya or an authorized Business Partner can download and install the license file.

Software licenses for upgrades to major releases of Session Manager are chargeable. Software licenses for upgrades to the next minor upgrade release are not chargeable.

The Session Manager license file contains the total number of authorized Session Manager licenses available for the enterprise. With Session Manager you can monitor the Session Manager licenses used in the system, based on the number of concurrent sessions. Session Manager raises an alarm when the number of licenses used exceeds the number of authorized Session Manager licenses available for the system. The system does not block the calls or disable the feature. You can:

- Purchase additional Session Manager licenses from Avaya.
- Analyze the Session Manager license usage and reschedule the planned usage of the system.

Note:

Licensing provides a 30-day grace period for all license errors, including no license file present on initial installation, before applying any license enforcement.

Backward compatibility and upgrade for licensing

There are two types of licensing:

- Session Manager connection licensing. This licensing is deprecated from Release 7.0 onwards.
- Session Manager instance licensing. This licensing is introduced in Release 7.0 onwards.

For Licensing, the recommended upgrade order is:

1. Upgrade System Manager to Release 7.1.
2. Install Session Manager 7.1 license file on System Manager Release 7.1.
3. Upgrade Session Manager to Release 7.1.

Table 1: Use Cases

Use Case Number	Combination	License File	Details
1	System Manager 6.0 - Session Manager 7.0	Session Manager License File 6.0	This configuration is not supported. You will get connection licensing because of System Manager 6.0.
2	System Manager 6.0 - Session Manager 7.0	Session Manager License File 7.0	This configuration is not supported. Upgrade order is not followed. You will get license error alarming on connection licensing because Session Manager 7.0 license file does not include connection licenses, but System Manager 6.0 performs connection licensing.
3	System Manager 7.0 - Session Manager 6.0	Session Manager License File 6.0	This is a mid-upgrade scenario. Session Manager Element Manager performs connection licensing.
4	System Manager 7.0 - Session Manager 6.0	Session Manager License File 7.0	This is a mid-upgrade scenario. Session Manager Element Manager performs the instance licensing on Session Manager 6.0 servers.
5	System Manager 7.0 - Session Manager 7.0	Session Manager License File 6.0	This configuration is not supported. Connection licensing is not supported in 7.0. You will get a Session Manager version mismatch error and Session Manager will be in license error mode with 30 day grace period.
6	System Manager 7.1 - Session Manager 7.1	Session Manager License File 7.1	Pre-upgrade scenario: instance licensing done.
7	System Manager 7.1 - Session Manager 7.0	Session Manager License File 7.0	This is a mid-upgrade scenario. Session Manager Element Manager performs the instance licensing on Session Manager 7.0 servers.

Chapter 7: Performance and capacity specifications

Capacity and scalability specification

Up to 250K SIP users or 350K connection re-use SIP devices can be supported by any N+M sparing Session Manager configuration consisting of Session Manager R2 Footprint servers and connection re-use devices. The customer is responsible for adequately distributing devices across primary and secondary servers to accommodate the configuration. For example, the typical Session Manager solution with N+1 sparing supports 350K SIP devices across 15 Session Manager instances allowing a single Session Manager failure. Similarly, a dual data center (N+N) supports 350K SIP devices across 28 Session Manager instances (14 in each data center).

Important:

Assigning a SIP profile to an H.323 endpoint reduces the total SIP capacity by that many endpoints. See Alternative H.323 Endpoint administration considerations and impacts on page 39.

The following table contains the type of SIP entity, maximum number of entities supported per Session Manager, and clarifying notes.

Entities	Numbers (supported limits)	Notes
Core Avaya Aura® Session Manager instances	28	
Dial Patterns * Locations/ Pattern * Routing Policies	300,000	
SIP Domains	1,000	
SIP Entities	25,000	
SIP Entity Links/ System Manager	75,000	1. Assuming 3 links for each SIP entity, such as, UDP, TCP, and TLS links. 2. Assuming that each SIP Entity is linked to two Session Managers (for redundancy) with only one transport protocol used. In this case, there would need to be 50,000 links.

Table continues…

Entities	Numbers (supported limits)	Notes
		In both cases, the inter-Session Manager entity links need to be counted towards the limit.
SIP Entity Links / Session Manager	10,000	
Adaptations	25,000	Assuming one Adaptation for each SIP Entity. At the most, there can be one Adaptation for each SIP Entity and some SIP Entities may not require any Adaptation. SIP Adaptations are applied only on the non-Session Manager entities.
Adaptation Entries	250,000	Full system limit. Includes both ingress and egress entries.
Regular Expressions	100	
Routing Policies	25,000	Assuming one routing policy for each SIP Entity.
Time Ranges	1,000	
Locations	25,000	Takes into account the use of locations to control bandwidth.
Location IP Address Patterns	50,000	Used to identify if a given SIP endpoint is associated with the location. Based on the assumption that on an average two patterns are used to define a location.
Local Host Name Resolution Entries	25,000	Based on an average of one for each SIP Entity.
SIP Users	250,000	Total number of users.
Handles/User	3	
Total number of SIP handles	750,000	Average number of handles/user is 3 (total handles = 250,000 X 3)
Total SIP devices	350,000	Total number of devices.
Registered Devices/User	10	A SIP user/station can have more than one registered SIP device per user, such as an Avaya one-X® Communicator in Shared Control. Session Manager capacities are based on the number of active SIP devices. The number of registered devices per user is important to know to adequately distribute users and devices across Session Manager instances.
Average Buddy List/Contacts for each User	25	Assuming an average of 25 per user (maximum number of 250/ user).
Active (Primary) SIP Devices/ Session Manager	23,300 (normal conditions)	If a user has multiple registered SIP devices, be careful when distributing users across Session Managers to avoid exceeding the SIP device

Table continues…

Entities	Numbers (supported limits)	Notes
	25,000 (temporarily under failure conditions)	capacities of an individual Session Manager. For example, 15,000 users each have two registered SIP devices, but 30,000 devices exceed the capacity of a single Session Manager. Instead, assign only 10,750 users to the individual Session Manager to not exceed the 23,300 device capacity limit.
CC Agents/ Session Manager	18,000 (normal conditions) 21,000 (failure conditions)	Call Center (CC) Agent SIP devices consume more resources per Session Manager. 18,000 is the maximum for CC Agent SIP devices, assuming all devices are CC agents. When configuring for systems that may support fewer CC Agents, assume that five CC Agent devices are the equivalent of six regular SIP devices.
Presence users	18,000 (normal conditions) 21,000 (temporarily during failure conditions)	
Digit Conversion Patterns (ingress)	45,000	
Digit Conversion Patterns (egress)	45,000	
Users/ Session Manager on VMware		See *Deploying Avaya Aura® Session Manager* on the Avaya support website.
Branch Session Manager instances	500	
Devices per Branch Session Manager on S8300D (Survivable Embedded)	700	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 and Branch Session Manager 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 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

Table continues…

Entities	Numbers (supported limits)	Notes
		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.
Devices per Branch Session Manager on S8300E (Survivable Embedded)/VE	1,000	
Devices per Branch Session Manager on Appliance Server/VE	5,000	
Busy Hour Sessions/ Session Manager	540,000	The type of call determines the number of SIP sessions. An SRE call is a single session, so Busy-Hour Session is equivalent to BHCC. Conversely, a SIP station-to-SIP station call creates three sessions, and the BHCC is calculated accordingly.
Session creations/second/ Session Manager	150	
Session creations /second/ Branch Session Manager	10	
Session creations/ second / survivable embedded Session Manager	3	

Alternative H.323 Endpoint administration considerations and impacts

The current method for administering H.323 endpoints is to use either of the following:

- System Manager to create an H.323 endpoint without a SIP profile.
- The Communication Manager SAT.

You must configure Session Manager to route calls to the correct Communication Manager.

Alternative method for administering H.323 endpoints

An alternative method for administering H.323 endpoints is to use System Manager to create a SIP profile for an H.323 endpoint. URE routing will automatically route calls to the correct Communication Manager.

The alternative method:

- Simplifies Session Manager routing configuration.
- Provides Dual Registration (H.323 and SIP endpoints on the same extension) with no further System Manager configuration.
- Provides an easy migration to a SIP endpoint by changing the endpoint type and removing the H.323 station.

Use Case

A customer has H.323 endpoints with DID numbers scattered randomly among different Communication Manager servers. This arrangement makes it cumbersome to configure Session Manager routing to send calls for H.323 endpoints to correct Communication Manager.

The Customer uses the new technique to take advantage of URE routing in place of manually administering Session Manager routing policies.

Impact on capacities

Important:

This method assigns a SIP profile to an H.323 endpoint. Using this method reduces the total SIP endpoint capacity by the number of H.323 endpoints assigned a SIP profile.

For example, if you configure 200 H.323 stations using the alternative method, you reduce the maximum number of SIP devices by 200.

Dial plan specification

With Session Manager, call routing is controlled by two interdependent schemes:

- A global enterprise-wide numbering plan used for centralized routing that is administered on a centralized management console.
- One or more local, geographically significant dial plans administer on Communication Manager, or other vendor PBX. Local dial plans specify the actual digits dialed within the constraints of the numbering plan.

Session manager adjusts routing information (digits and domains) to accommodate the numbering plan or dial plans as required.

The numbering plan describes the overall numbering scheme that the enterprise uses for centralized routing. Session Manager uses two different numbering plans for analysis and routing:

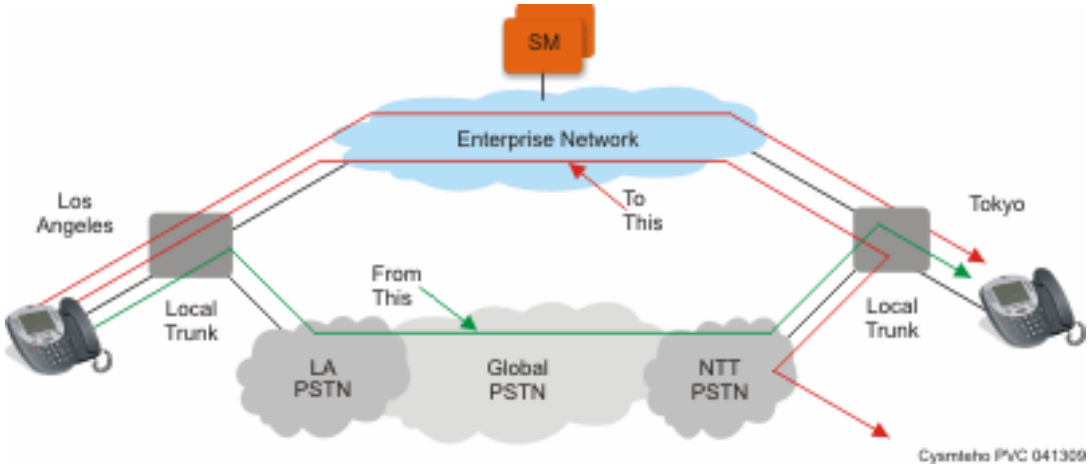
- E.164 Public Numbering Plan
- Enterprise Canonical (Private Numbering Plan)

Tail end hop off

Session Manager can route outgoing calls to local trunks at each location so that all users across the network enterprise can save toll charges for calls that go off the network. This configuration is called tail end hop off (TEHO).

For example, a call from Tokyo to Los Angeles can be routed through a company intranet and then sent to the PSTN from the Los Angeles PBX, which is similar to a *local* call from Los Angeles. And calls bound for Tokyo are routed through the Tokyo PBX.

The following figure illustrates how TEHO works:



Call Admission Control specification

Session Manager supports converged voice and video bandwidth management with Avaya Aura® System Manager centralized administration and control. You can administer bandwidth allocations between voice and multimedia traffic, and allow voice to use bandwidth from unused video allocations when network conditions require the bandwidth. Session Manager intercepts each SIP request for service, examines the SIP message for the requested bandwidth, and allocates the actual bandwidth requested and accepted. However, Session Manager denies as well as downspeeds calls if the bandwidth allocation is exceeded. In addition, Session Manager can automatically downspeed video calls to the bandwidth available and enable video calls to complete at lower bandwidths.

Session Manager provides advanced control of video and multimedia bandwidth allocation. Administrators can configure:

- The maximum allowed bandwidth for a multimedia call with separate controls for inter-location (where resources are scarce) and intra-location (where more bandwidth is generally available so higher quality can be allowed) on a per-location basis.

- The minimum level to downspeed video bandwidth by location to ensure a level of video quality.

Administrators can view the current bandwidth usage and the number of calls for accurate management.

Redundancy and high availability

An enterprise supports up to 28 Session Manager instances. You can implement the Session Manager instances in the same data center or in data centers that are separated geographically around the world. These instances do not need to exist on the same subnet.

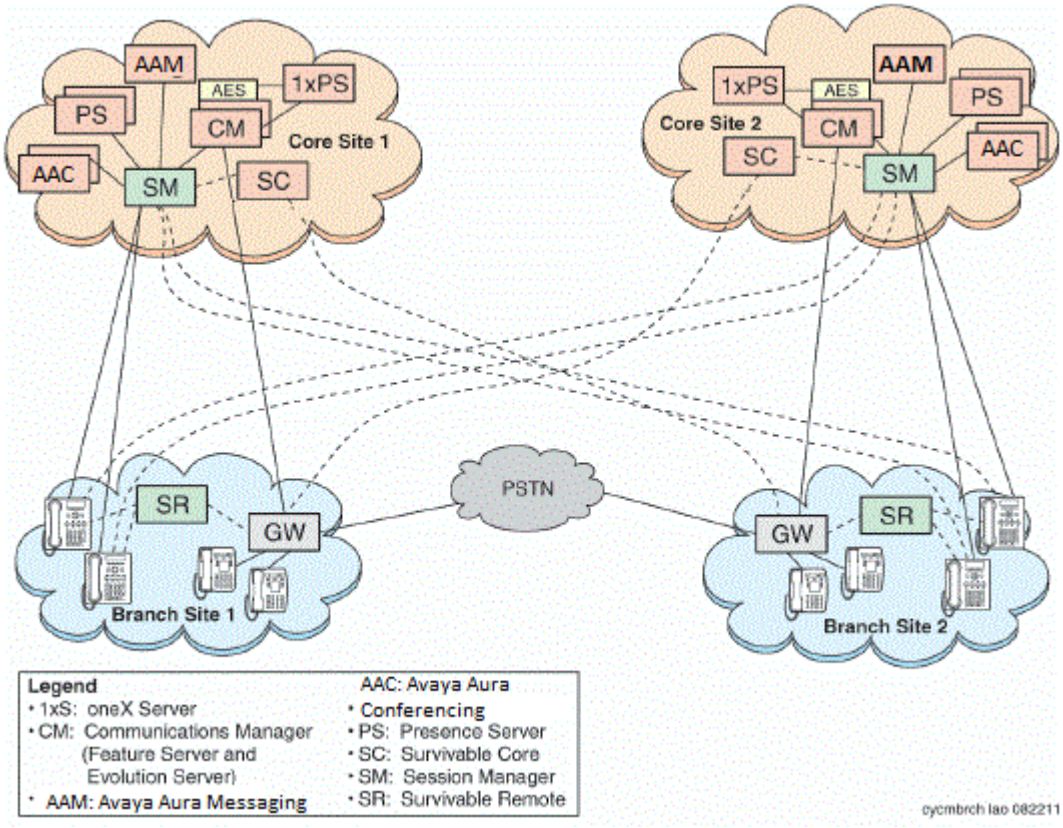
Session Manager redundancy supports networks with round trip delays of less than one second.

Session Manager uses the active-active approach where two instances are active simultaneously and either of the instances can process any request. This feature is important for distributing traffic across the network.

Configuring more than one Session Manager in a network has the following benefits:

- A failure of one of the Session Manager instances does not interrupt service.
- You can use one System Manager to administer all the Session Manager instances.
- The centralized dial plan is in effect for Avaya and third-party PBXs. The centralized dial plan connects the PBXs, using SIP either directly or using a SIP gateway, to one of the Session Manager instances.
- When SIP endpoints register simultaneously with two Session Manager instances at the core and with one Branch Session Manager, the SIP endpoints continue to be operational if any one of the associated Session Manager instances fails.

The following illustration shows solution-level survivability in the enterprise:



Note:

Session Manager does not support High Availability for call journaling because the primary Session Manager stores the call logs.

Survivable Core

Survivable Core (SC) provides geo-redundant Communication Manager Feature Server redundancy. It supports multiple Data Centers for a failed or unreachable main Communication Manager. Session Manager works with the Survivable Core as follows:

- After the main Communication Manager goes down, Session Manager starts sending SIP messages to the Survivable Core.
- When the main Communication Manager recovers, Session Manager again starts sending SIP messages to the main Communication Manager instead of the Survivable Core.

Survivable Remote

Survivable Remote sites include a Survivable Remote Session Manager and Survivable Remote Communication Manager that is either a Feature Server or an Evolution Server, depending on the

main Communication Manager to which it is connected. SIP phones simultaneously register to the main Session Manager, a backup main Session Manager, and the Survivable Remote Session Manager. During a WAN outage that removes the communication path between phones and the associated Session Manager, the phones failover to the Survivable Remote Session Manager and the Survivable Remote Communication Manager.

Chapter 8: Security

Security specification

All SIP sessions flow through Session Manager, which is the SIP routing element. Session Manager protects the Unified Communications (UC) applications and servers from Network and Transport Denial of Service (DoS) attacks, SIP DoS attacks, and other network attacks. Session Manager also enforces access control policy for UC applications. As a SIP Registrar, Session Manager authenticates and authorizes user access to protect customers from toll fraud and other malicious attacks.

Session Manager runs on the Linux® operating system. The operating system is hardened to provide only those functions necessary for securing critical call processing applications.

Using Session Manager, an administrator can select TLS to secure the SIP signaling to ensure the privacy of the application credentials of the user, as well as to secure the keys used for securing the media stream with SRTP.

Session Manager ensures that security defenses, encryption, authentication, and certificate use are embedded at all levels across the enterprise network to maintain secure continuous communications between all endpoints without compromising performance.

For more information about Session Manager security, see *Avaya Aura® Session Manager Security Design*.

Port assignments

For complete port matrix information, see the Port Matrix Documents section at http://support.avaya.com/security.

Chapter 9: Resources

Documentation

The following documents are available at http://support.avaya.com.

For the latest information, see the Session Manager Release Notes.

Title	Description	Audience
Overview		
Avaya Aura® Session Manager Overview and Specification	Describes the key features of Session Manager.	IT management System administrators
Avaya Aura® Virtualized Environment Solution Description	Describes the Avaya Virtualized Environment, design considerations, topology, and resources requirements.	Sales engineers Implementation engineers Support personnel
Avaya Aura® Session Manager Security Design	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Avaya Aura® Session Manager 7.1 Release Notes	Contains enhancements, fixes, and workarounds for the Session Manager 7.1 release.	System administrators Services and support personnel
Implementation		
Deploying Avaya Aura® applications from System Manager	Describes how to deploy the Avaya Aura® virtual applications using the System Manager Solution Deployment Manager.	Services and support personnel
Deploying Avaya Aura® Session Manager	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Describes how to install and configure Branch Session Manager in a virtualized environment.	Services and support personnel

Table continues…

Title	Description	Audience
Routing Web Service API Programming Reference	Describes how to use the System Manager Routing Web Service API for Session Manager.	Services and support personnel
Upgrading and Migrating Avaya Aura® applications from System Manager	Describes how to upgrade and migrate the Avaya Aura® virtual applications using System Manager Solution Deployment Manager.	Services and support personnel
Using		
Using the Solution Deployment Manager client	Deploy and install patches for Avaya Aura applications.	System administrators
Administration		
Administering Avaya Aura® Session Manager	Describes the procedures to administer Session Manager using System Manager.	System administrators
Administering Avaya Aura® Communication Manager Server Options	Describes the procedures to administer Communication Manager as a feature server or an evolution server. Provides information related to Session Manager administration.	System administrators
Avaya Aura® Session Manager Case Studies	Provides common administration scenarios.	System administrators
Installation and upgrades		
Installing the Dell™ PowerEdge™ R610 Server	Describes the installation procedures for the Dell™ PowerEdge™ R610 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R620 Server	Describes the installation procedures for the Dell™ PowerEdge™ R620 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R630 Server	Describes the installation procedures for the Dell™ PowerEdge™ R630 server.	Services and support personnel
Installing the HP ProLiant DL360 G7 Server	Describes the installation procedures for the HP ProLiant DL360 G7 server.	Services and support personnel
Installing the HP ProLiant DL380p G8 Server	Describes the installation procedures for the HP ProLiant DL380p G8 server.	Services and support personnel
Installing the HP ProLiant DL360 G9 Server	Describes the installation procedures for the HP ProLiant DL360 G9 server.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade Session Manager to the latest software release.	Services and support personnel
Migrating and Installing Avaya Aura® Appliance Virtualization Platform	Describes the migration and installation procedures for Appliance Virtualization Platform.	Services and support personnel
Using the Solution Deployment Manager client	Describes the patch deployment and installation procedure for Avaya Aura® applications.	Services and support personnel

Table continues…

Title	Description	Audience
Maintaining and Troubleshooting		
Maintaining Avaya Aura® Session Manager	Contains the procedures for maintaining Session Manager.	Services and support personnel
Troubleshooting Avaya Aura® Session Manager	Contains the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and 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**.

Training

The following table contains courses that are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go**.

New training courses are added periodically. Enter **Session Manager** in the **Search** field to display the inclusive list of courses related to Session Manager.

Course code	Course title
1A00236E	Knowledge Access: Avaya Aura® Session and System Manager Fundamentals
4U00040E	Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation
5U00081V	Session Manager Administration
5U00082I	Session Manager and System Manager Administration

Table continues…

Course code	Course title
5U00082R	Session Manager and System Manager Administration
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support
5U00095V	System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00097I	Avaya Aura® Session and System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00105W	Avaya Aura® Session Manager Overview
ATC01840OEN	Survivable Remote Session Manager Administration
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
2011V	What is new in Avaya Aura® System Manager 7.0 and Avaya Aura® Session Manager 7.0

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

Call Admission Control	Prevent the over subscription of VoIP and protects the flow of voice traffic to ensure that there is enough bandwidth for authorized call flows.
Centralized Applications	A set of core Avaya SIP applications such as Modular Messaging, Media Exchange and Voice Portal.
Centralized SIP Trunking	A consolidation of trunks to a common core location as opposed to the network edges.
DNS Server	A server that maintains a database of mappings of DNS domain names to various types of data, such as IP addresses.
Internet Protocol Security (IPsec)	A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. It is a dual-mode, end-to-end, security scheme operating at the Internet Layer of the Internet Protocol Suite or OSI model Layer 3.
Local Host Name Resolution	Host name resolution is the process of resolving a host name to an IP address.
Network Address Translation (NAT)	The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network.
Secure Access Link (SAL)	Avaya equipment designed to enable remote access to Aura equipment for troubleshooting and diagnostic purposes.
Sequenced Applications	A collection of SIP applications that engage automatically based on the user's profile. These applications are added to a call path during the logical progression of the call (incoming or outgoing).
Session Border Controller (SBC)	A device used in some Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications.
Tail End Hop Off (TEHO)	In a private network, a call which is carried over flat rate facilities (Inter-machine Trunks or IMT) to the closest switch node to the destination of the call, and then connected into the public network as a local call.

Time of day routing	A configuration which determines how calls are routed during specific times of day across the network.
Toll Avoidance / By-pass	A configuration which allows calls to be routed to and from the service provider without incurring any cost.
Trunk	Connection between two switches, can be multiplexed to provide higher bandwidths such as DS-1 and DS-3.

Index

R

S

T

U

V

W