



Avaya Aura[®] Session Manager Overview and Specification

Release 8.1.x
Issue 7
April 2021

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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](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, 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). End User 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 as indicated in the order, Documentation, or as authorized by Avaya in writing. "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). End User 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") as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

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

Copyright

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

written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS

MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](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	6
Purpose.....	6
Change history.....	6
Chapter 2: Session Manager overview	8
Supported servers.....	9
Supported virtualized environments.....	9
Features.....	10
Application Sequencing.....	10
SIP Resiliency.....	10
Call Detail Recording on Session Manager.....	11
Centralized applications.....	12
Centralized SIP trunking.....	12
SIP Endpoint Concentrator Connection Policy.....	12
Inter-gateway Alternate Routing for SIP endpoints.....	13
Limit Number of Concurrent Calls for SIP endpoints.....	13
Normalization of disparate networks.....	14
Online/Offline Call Journal (Call History).....	14
Personal Profile Manager.....	15
Policy-based routing.....	15
System Manager Web Services	16
Hunt Group Log in/Log out button for SIP phones in a non-CC Environment	16
Session Manager and Avaya Aura® Device Services integration.....	17
Add/remove skill button.....	18
TLS mutual authentication for SIP endpoints	18
Regular Expression Adaptations.....	19
Push notifications.....	19
Chapter 3: What's new in Session Manager	21
New in this release.....	21
New in Session Manager Release 8.1.3.1.....	21
New in Session Manager Release 8.1.3.....	21
New in Session Manager Release 8.1.2.....	22
New in Session Manager Release 8.1.1.....	23
New in Session Manager Release 8.1.....	24
Session Manager feature matrix.....	25
Chapter 4: Capacity limits	27
Supported footprints of Session Manager.....	27
Supported footprints of Branch Session Manager.....	29
Chapter 5: Interoperability	31
Product compatibility.....	31

Accessing the Compatibility Matrix.....	31
Supported Avaya endpoints.....	31
Chapter 6: Licensing Requirements.....	32
Licensing requirements.....	32
Chapter 7: Performance and capacity specifications.....	34
Capacity and scalability specification.....	34
Alternative Endpoint administration considerations and impacts.....	38
Dial plan specification.....	38
Tail end hop off.....	39
Call Admission Control specification.....	39
Redundancy and high availability.....	40
Survivable Core.....	41
Survivable Remote.....	41
Chapter 8: Security.....	43
Security specification.....	43
Port assignments.....	43
Chapter 9: Resources.....	44
Session Manager documentation.....	44
Finding documents on the Avaya Support website.....	45
Accessing the port matrix document.....	46
Avaya Documentation Center navigation.....	46
Training.....	47
Viewing Avaya Mentor videos.....	48
Support.....	48
Using the Avaya InSite Knowledge Base.....	48
Glossary.....	50

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
7	April 2021	Updated the section Capacity and scalability specification on page 34.
6	March 2021	Updated the section Supported footprints of Session Manager on page 27.
5	February 2021	Added the section New in Session Manager Release 8.1.3.1 on page 21. Updated the following sections: <ul style="list-style-type: none">• Session Manager overview on page 8• Supported footprints of Session Manager on page 27
4	October 2020	For Release 8.1.3, added Push notifications on page 19. For Release 8.1.3, updated the following sections: <ul style="list-style-type: none">• What's new in Session Manager on page 21.• Session Manager feature matrix on page 25• Supported footprints of Session Manager on page 27

Table continues...

Issue	Date	Summary of changes
3	March 2020	Updated the following sections: <ul style="list-style-type: none">• New in Session Manager Release 8.1.2 on page 22.• Supported footprints of Session Manager on page 27.
2	October 2019	Updated the section What's new in Session Manager on page 21.
1	June 2019	Initial Release.

Chapter 2: Session Manager 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 and centrally managed SIP-based communications network.

Session Manager supports the following features:

- 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 scalability 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.
- Support for call reconstruction to allow Call Preservation for SIP calls, which provides mid-call features to be invoked after a failover.
- Support to carry Presence Information Data Format Location Object (PIDF-LO) as a Multipurpose Internet Mail Extensions (MIME) body/attachment in a SIP message. Session Manager can also pass the PIDF-LO information in the SIP message.

Supported servers

Session Manager supports the following servers:

- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630
- HP ProLiant DL360p G8
- HP ProLiant DL360 G9
- Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640
- Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640

Branch Session Manager supports the following servers:

- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630
- HP ProLiant DL360p G8
- HP ProLiant DL360 G9
- S8300E
- Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640
- Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640
- Release 8.0 and later does not support S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.
- Release 7.0 and later does not support S8510, S8800, and 1006R CallPilot servers.

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
- Kernel-based Virtual Machine
- Hyper-V
- Amazon Web Services
- Microsoft Azure
- Google Cloud

- IBM Bluemix

For information about Bluemix, see IBM product documentation website.

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

SIP Resiliency

When the SIP signaling path for a call between user agents is disconnected due to SIP element failure or the network unavailability, the user agents cannot exchange the signaling messages. The SIP signaling path can also be disconnected when one or more SIP elements such as proxy or location server are not working, if the user switches the network from WiFi to 4G and from 4G to Wifi, or the failure of Session Manager.

Using SIP Resiliency feature, Session Manager reconstructs the call between endpoints when the SIP signaling path for a call or a conference call is disconnected. Avaya recommends using same domain names for signaling groups to support call reconstruction.

Session Manager reconstructs the impacted SIP dialog by initiating a new dialog towards SIP user agents to replace the dialog of broken end to end call. In case of Session Manager failure, alternate Session Manager reconstructs the call.

Communication Manager supports SIP Resiliency feature by replacing SIP dialogs for each dialog of a SIP session. When Communication Manager receives INVITE request containing a Replaces header message, Communication Manager attempts to replace the SIP dialog specified in the Replaces header. The Communication Manager also maintains the integrity of a call so that the features such as hold or transfer during the call are available for the parties of the call.

For the best performance of call reconstruction, ensure that the administration settings on the signaling groups, trunk groups, network regions, and codec settings are uniform between primary Session Manager, alternate Session Manager, and Communication Manager that are configured for call reconstruction. Also, ensure that all the incoming SIP trunks must be connected to Communication Manager through Session Manager.

The call reconstruction might fail if the call topology consists of old as well as new instances of Session Manager and Communication Manager.

SIP device must also support the new call reconstruction method for SIP Resiliency feature to work.

You can enable SIP Resiliency only if all the Session Managers in the configuration are 8.0 or later.

For more information on Communication Manager settings for SIP Resiliency, see *Avaya Aura® Communication Manager Screen Reference*.

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*.

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.

From Release 8.1, call logs are stored redundantly on the primary and secondary Session Managers. The primary and secondary Session Managers store 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 programmer's 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

With Avaya Aura® Device Services, you can roll out multiple clients and seamlessly transition between devices. Avaya Aura® Device Services acts as a single point of administration for endpoints. It can also provide file server capabilities, such as firmware and settings files. Avaya Aura® Device Services can handle traditional IP phones, such as the 96xx Series Phones, and the complex configuration of SIP endpoints, such as Avaya Workplace Client¹.

SIP endpoints, such as Avaya Workplace Client, integrate telephony, video, chat, email, and presence. To log in to and use all these services, the device must be configured with multiple FQDNs or IP addresses, login IDs, and passwords. Once logged in, you require the appropriately formatted contact address to initiate communication and Avaya Aura® Device Services can provide this.

Avaya Workplace Client also provides BYOD capabilities, which allow users to use their own devices. Each device has different capabilities, so the appropriate settings must be pushed to each device. Using the Dynamic Configuration service, Avaya Aura® Device Services provides dynamically created setting files that include system-wide parameters, user-specific parameters, and device-specific parameters.

As an administrator, you must maintain software-based soft clients on a limited set of versions to ensure consistent feature sets and security. With hard phones, such as 96xx Series Phones, you can initiate a firmware download by forcing the phone to reboot. With a soft phone, such as Avaya Workplace Client, you cannot manually force the software to update unless it is configured through Avaya Aura® Device Services.

Cassandra clustering and data replication overview

From the Session Manager Release 8.0, Cassandra clustering is enabled permanently to provide redundant storage of SIP device data on instances of Session Manager. This is applicable for all systems, with and without Avaya Aura® Device Services.

When Avaya Aura® Device Services is in use, Cassandra data distribution uses the administration on the User Data Storage page to identify the Session Manager instances that are within the same datacenter. Every Session Manager instance that is paired with Avaya Aura® Device Services must be a part of a datacenter. Session Manager instances that are not paired with Avaya Aura®

¹ This document also uses the term “client” when referring to Avaya Workplace Client.

Device Services can optionally be a part of datacenter. Session Manager instances should be assigned to datacenter based on the system topology. The best redundancy is obtained when two or more Session Managers are assigned to each data center.

For administering Cassandra data distribution with Avaya Aura® Device Services:

1. Create a data center.
2. Assign co-located Session Managers to the data center.
3. Add the Avaya Aura® Device Services instance to the inventory.
4. 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.

Regular Expression Adaptations

Using Regular Expression Adaptations, you can build your own adaptations to define criteria and instructions for message modification that use regular expressions.

You can also define rules based on multiple conditions in the content of SIP messages. You can define conditions on R-URI, Response-Line, standard and custom SIP Headers, and attachment bodies.

Each regular expression adaptation has up to two lists of one or more adaptation rules, where one list is for ingress adaptation and the other for egress adaptations.

You can define the order of adaptation rules. Each adaptation rule consists of one condition, zero or more variables, and a list of one or more ordered actions.

If the condition is not assigned to the adaptation rule, the rule executes unconditionally.

The action can be to add, modify, or delete the header, request, response line, or the attachment of an identified message.

When Session Manager processes a message, Session Manager applies ingress and/or egress adaptation rules in the administered order. The egress adaptation rules are executed in the order the rules are administered. The adaptation rule checks whether the message matches the defined condition. If the condition matches, the values of administered variables are determined and set, and administered actions are executed to adapt the message.

Ingress rules are based on regular expression adaptations associated with the SIP entity sending the message and Egress rules are based on regular expression adaptations associated with the destination SIP entity of the message.

Push notifications

The push notification mechanism enables clients to receive incoming call alerts and other notifications from the Apple Push Notification service (APNs). The push notification service sends

notifications automatically. Therefore, an application can receive notifications even when it is suspended or in Sleep mode.

The Avaya Aura® Session Manager can send push notifications about the following telephony-related events:

- Incoming calls.
- Incoming calls on an Avaya Aura® Communication Manager bridged line appearance.
- Incoming calls on an Avaya Aura® Communication Manager enhanced pickup group.
- Incoming calls on an Avaya Aura® Communication Manager team button.
- Message waiting notifications.

Push notification provider

The Avaya Aura® Session Manager interacts with the APNs through a push notification provider. You must register your Session Manager with the push notification provider before activating push notifications. The default provider is the Avaya Push Notification provider, which must be used to support push notifications for Avaya Workplace Client. If you want to use push notifications for third-party SDK-based applications, you must use a third-party push notification provider.

For the Avaya Push Notification provider, you must create and configure an account at accounts.avayacloud.com. This account is used to store the data required to authorize your Session Manager system. This account requirement does not apply if you are working with a third-party provider.

Chapter 3: What's new in Session Manager

This chapter provides an overview of the new and enhanced features of Session Manager Release 8.1.x.

For more information about these features and administration, see *Administering Avaya Aura® Session Manager*.

New in this release

New in Session Manager Release 8.1.3.1

Session Manager Release 8.1.3.1 supports the following new features and enhancements:

Support for Apple Push Notification activation maintenance

With Release 8.1.3.1, Session Manager will provide real-time activation status of push notifications that a user subscribes. A newly introduced Push Notification Activations status page will display activation status, last notification time, and status information per user or device. From a maintenance point of view, you can deactivate push notification subscriptions from the status page.

New in Session Manager Release 8.1.3

Session Manager Release 8.1.3 supports the following new features and enhancements:

Support for Branch Visiting User survivability

With Release 8.1.3, Session Manager supports Branch Visiting User survivability feature, that automatically assigns a visiting user to the Branch Session Manager of the visiting location. With this feature, you do not need to manually administer or change the Branch Session Manager with the local Branch Session Manager for the visiting users that are in the SIP controller list.

To configure the feature, you can enable the **Enable Branch Visiting User** field on the Global Settings page.

*** Note:**

Branch Visiting User is only supported on Branch Session Managers survivability servers. IP Office survivable branches (formerly known as B5800) do not support the Branch Visiting User feature.

Support for Apple Push Notification Services

With Release 8.1.3, Session Manager provides telephony push notifications events through Apple Push Notification service (APNs) to Client SDK based iOS applications, such as Avaya Workplace Client for iOS. Session Manager provides push notification events for incoming calls, chat and voice messaging status updates. Avaya Workplace Client for iOS should be on Release 3.14 or later to receive push notification services.

Currently the Avaya Aura® Web Gateway supports push notification events towards iOS application and you can choose to utilize push notification service on either the Avaya Aura® Web Gateway or on Session Manager. You can select a group of users and update their client configuration through Avaya Aura® Device Services to point to either AAWG or Session Manager as their Push Notification provider.

To configure the feature, you can enable the **Enable Mobile Push Notification** field on the Global Settings page. For administering the push notification provider and application, use the **Session Manager > Network Configuration > Push Notification** page.

Support for VMware ESXi 7.0

With Release 8.1.3, Avaya Aura® applications support the VMware® vSphere ESXi 7.0 and VMware® vCenter Server 7.0 in the VMware virtualized environment.

*** Note:**

Only the Encrypted Core Session Manager (8.1E OVA) is supported on VMware ESXi 7.0.

Enhancements to the System Manager alert messages at login

With Release 8.1.3, for the Emergency Location Management Solution, System Manager displays the Session Manager emergency Dial Pattern routes notification warning message in an Alert Messages pop-up window, if the Routing Locations, Routing Policies, and Dial Patterns are not configured on Session Manager according to the emergency calling guideline.

New in Session Manager Release 8.1.2

Session Manager Release 8.1.2 supports the following new features and enhancements:

Data Encryption

With Release 8.1.2, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized environments. Once you deploy the application with data encryption, you cannot disable data encryption after deployment and vice-versa.

Administrable Endpoint Adaptation

With Release 8.1.2, Session Manager supports administrable endpoint adaptation, allowing an administrator to apply sequences of adaptations to groups of endpoints (based on device type)

and/or users (based on membership in an origination dial-pattern set). This feature is an extension of the adaptation capability made available to SIP entities in Session Manager Release 8.0.1.

Support for Log Retention

With Release 8.1.2, Session Manager supports **Log Retention** to specify the number of days for which logs will be retained. Default value for number of days to retain log files are 30 days. You can set the number of days between 1 — 180.

Support for Centralized Call History Retention (days)

With Release 8.1.2, Session Manager supports **Centralized Call History Retention (days)** to specify the number of days for which centralized call history will be retained. Default number of days is 90. You can set the number of days between 1 — 180.

Support for encrypted backup and restore

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

New in Session Manager Release 8.1.1

Session Manager Release 8.1.1 supports the following new features and enhancements:

Enhanced support for Matching Pattern

Session Manager extends the support for Matching Pattern. With Release 8.1.1, Matching Pattern ranges can be entered in the form of [start of range]:[end of range]. For example, 600000:600009.

Support for Regex Debugger

With Release 8.1.1, Session Manager supports a new tool called Regular Expression debugger which allows checking, validating and backtracking regular expressions.

Support for SIP headers and Attachment fields for Call Routing Test

With Release 8.1.1, you can use zero or more **SIP headers** to insert into the SIP INVITE request created by the call routing test.

With Release 8.1.1, you can use Content-type and content of an attachment to insert into the SIP INVITE request created by the call routing test.

Support for new Log Action for Regular-expression adaptations

With Release 8.1.1, a new Log action can be added to the regular-expression adaptations. This action will not modify a SIP message, but will instead log an event indicating that conditions were met for the action to execute.

VMware console for applications

With Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab for the application that reside on Appliance Virtualization Platform Release 7.1.2 and later.

Based on the role of the user, you can assign the permissions for accessing the console.

New in Session Manager Release 8.1

Session Manager Release 8.1 supports the following new features and enhancements:

Support for Session Manager Profile 6

With Release 8.1, Session Manager supports a new Profile 6. The Profile 6 supports 66.7K SIP devices. Using the Session Manager Profile 6, an Avaya Aura® deployment can support up to 1 million SIP devices.

Support for 5000 SIP branches

Earlier to Release 8.1, you can configure only 500 Branch Session Manager instances. From Release 8.1, you can configure 5000 Branch Session Manager instances with a single System Manager system in an Avaya Aura® deployment.

Appliance Virtualization Platform Hypervisor

With Release 8.1, Appliance Virtualization Platform is based on the customized OEM version of VMware® ESXi 6.5.

Syslog server configuration for Session Manager

With Session Manager Release 8.1, you can configure one or more syslog server for the Session Manager logging and SIP tracer for single Session Manager.

Enhancement for SIP tracing

With Session Manager Release 8.1, you can:

- View tracer configuration for the single Session Manager security module.
- Modify the tracer configuration for the single Session Manager security module, if required.
- Send traces to Syslog Server that is configured for Session Manager.

Support for managing Syslog receiver certificates for Remote Syslog receiver

With Release 8.1, you can:

- Add trusted certificates for Remote Syslog receiver by selecting the *SYSLOG* store type on System Manager.
- Create identity certificate to use with Remote Syslog receiver by selecting the *syslog* service name on System Manager.

Enhancement for origination dial pattern sets

With Session Manager Release 8.1, you can create origination dial pattern for origination dial pattern sets.

Enhancement for SIP Entity Reference Report

With Session Manager Release 8.1, you can view the outbound proxy, application, and failover group that correspond to the SIP entity.

Support for bulk upgrade of Branch Session Manager instances

With Release 8.1, you can perform bulk upgrade of Branch Session Manager instances by using the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet on the **Solution Deployment Manager > Upgrade Management > Download > Bulk Import Spreadsheet** page.

Supported browsers

Following are the minimum supported versions of the supported browsers:

- Internet Explorer 11
- Mozilla Firefox 65, 66, and 67

Support for Red Hat Enterprise Linux operating system 7.6

With Release 8.1, you can deploy and upgrade Avaya Aura® applications on the Red Hat Enterprise Linux operating system 7.6.

Session Manager feature matrix

The following table lists the feature matrix of Session Manager.

*** Note:**

The features listed in the following table are not a comprehensive feature list. It only covers the new features.

Feature name	Release 7.0.x	Release 7.1.x	Release 8.0.x	Release 8.1.x
OVA signing		Y	Y	Y
IPv6 support		Y	Y	Y
Enhanced Access Security Gateway (EASG)		Y	Y	Y
Compliance with DISA security STIGs		Y	Y	Y
Extended Security Hardening		Y	Y	Y
Conference factory URI		Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y
Customer Root Access			Y	Y
Preserve security hardening modes on upgrade			Y	Y
SIP Resiliency			Y	Y
Extended host name validation			Y	Y
Cassandra clustering		Y	Y	Y
Support for Software-only deployment			Y	Y
Support for 16 digit dial plan			Y	Y
Support for Hyper-V in Software-Only environment			Y	Y

Table continues...

What's new in Session Manager

Feature name	Release 7.0.x	Release 7.1.x	Release 8.0.x	Release 8.1.x
Support for Regular Expression based adaptation module			Y	Y
Support for Call Journaling Server High Availability			Y	Y
Cassandra security hardening			Y	Y
Support for multiple customer accounts			Y	Y
Support for role-based access control			Y	Y
Support for Avaya Solutions Platform 120 Appliance			Y	Y
Support for Avaya Solutions Platform 130 Appliance			Y	Y
Syslog server configuration				Y
Data Encryption				Y
Branch Visiting User				Y
Push notification				Y
Support for VMware ESXi 7.0				Y

Chapter 4: Capacity limits

Supported footprints of Session Manager

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.

Session Manager Device Footprints	Up to 2K Devices	2K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices	10K to 23.3K Devices	23.3K to 66.7K Devices
CPU Minimum	2200MHz, Hyper-threaded					
vCPUs	3	5	8	12	20	53
CPU MHz Reservation	3300	5500	8800	13200	22000	58300
* Note: Reservations are applicable to VMware only.						
Memory Reservation	4916 MB	7376 MB	9832 MB	12288 MB	22120 MB	67584 MB
AWS Machine (OVA)	c4.xlarge	c4.2xlarge	c4.2xlarge	c4.4xlarge	c4.8xlarge	c5.18xlarge
AWS Machine (ISO Image)	<ul style="list-style-type: none"> • c4.xlarge • c5.xlarge • c5a.xlarge 	<ul style="list-style-type: none"> • c4.2xlarge • c5.2xlarge • c5a.2xlarge 	<ul style="list-style-type: none"> • c4.2xlarge • c5.2xlarge • c5a.2xlarge 	<ul style="list-style-type: none"> • c4.4xlarge • c5.4xlarge • c5a.4xlarge 	<ul style="list-style-type: none"> • c4.8xlarge • c5a.8xlarge 	<ul style="list-style-type: none"> • c5.18xlarge • c5a.16xlarge
SIP Devices ¹ (Normal/Failure) ²	2K/2.4K	4.5K/5K	7K/8K	10K/12K	23.3K/ 25K	66.7K/72K

Table continues...

Capacity limits

Session Manager Device Footprints	Up to 2K Devices	2K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices	10K to 23.3K Devices	23.3K to 66.7K Devices
CC Agents (Normal/Failure)	1.6K/2K	3.75K/4166	5.8K/6666	8333/10K	18K/21K	21.6K/25.2K
Presence Users (Normal/Failure)	2K/2.4K	4.5K/5K	7K/8K	10K/12K	18K/21K	21.6K/25.2K
Sessions (Sec/Hour/Max)	20/72K/17.9K	45/162K/37.4K	70/256K/59.8K	100/360K/90K	150/540K/170K	180/648K/510K
HDD for AWS, VMware, or KVM OVA (GB)	<ul style="list-style-type: none"> • Disk 1: 50 • Disk 2: 10 • Disk 3: 30 Total: 90	<ul style="list-style-type: none"> • Disk 1: 50 • Disk 2: 10 • Disk 3: 30 Total: 90	<ul style="list-style-type: none"> • Disk 1: 55 • Disk 2: 25 • Disk 3: 40 Total: 120	<ul style="list-style-type: none"> • Disk 1: 55 • Disk 2: 25 • Disk 3: 40 Total: 120	<ul style="list-style-type: none"> • Disk 1: 85 • Disk 2: 50 • Disk 3: 65 Total: 200	<ul style="list-style-type: none"> • Disk 1: 85 • Disk 2: 50 • Disk 3: 65 Total: 200
HDD (GB) (If the deployment is using Solutions Deployment Manager)	90	90	120	120	200	200
Encrypted Core Session Manager (8.1 E OVA) HDD for VMware (GB)	<ul style="list-style-type: none"> • Disk 1: 35 • Disk 2: 55 Total: 90	<ul style="list-style-type: none"> • Disk 1: 35 • Disk 2: 55 Total: 90	<ul style="list-style-type: none"> • Disk 1: 40 • Disk 2: 80 Total: 120	<ul style="list-style-type: none"> • Disk 1: 40 • Disk 2: 80 Total: 120	<ul style="list-style-type: none"> • Disk 1: 60 • Disk 2: 140 Total: 200	<ul style="list-style-type: none"> • Disk 1: 60 • Disk 2: 140 Total: 200
HDD for Software-Only ISO (GB) ³	90	90	120	120	200	200

Notes:

1. SIP devices: It includes all hard endpoints, soft clients, AST/NON-AST SIP endpoints and third-party endpoints.
2. Normal/Failure: Normal refers to capacity of the Session Manager in Sunny Day scenario and Failure refers to capacity of the Session Manager in Rainy Day scenario. A Session Manager in a rainy day scenario can have more number of users registered as it has registrations from the users whose Primary Session Manager is down.
3. You can deploy Session Manager software-only *ISO image* on VMware, KVM, Nutanix, Hyper-V, Amazon Web Services, Google Cloud Platform, and Microsoft Azure platforms.

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.

Avaya Aura® deployment 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 IX Workplace devices	Previous IX Workplace 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
Profile 6	66,700	13,900	-

Supported footprints of Branch Session Manager

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

Branch Session Manager Device Footprints	Up to 1K Devices	1k to 5K Devices
CPU Minimum	2200 MHz, Hyper-threaded	
vCPUs	2	4
CPU MHz Reservation	2200	4400
Memory	3072 MB	4500 MB
Memory Reservation	3072 MB	4500 MB
CC Agents Max	583	4167

Table continues...

Capacity limits

Branch Session Manager Device Footprints	Up to 1K Devices	1k to 5K Devices
Sessions (Sec/Hour/Max)	3/10.8K/4.8K	30/108K/35K
HDD (GB)	35G	35G

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

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). You can either use standalone WebLM or WebLM that is embedded in System Manager.

You can download the license file from PLDS and install the license. Avaya or an authorized Business Partner can also 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 instance counts. 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

The types of licensing are:

- 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 the Release 8.1.
2. Install Session Manager 8.1 license file on System Manager Release 8.1.

3. Upgrade Session Manager to Release 8.1.

Chapter 7: Performance and capacity specifications

Capacity and scalability specification

Various N+M redundant Session Manager configurations can support up to 300K SIP users and 1 million SIP devices. The customer is responsible for adequately distributing devices across primary and secondary servers to accommodate the configuration. For example, the typical Session Manager Profile 5 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 a non-SIP endpoint reduces the total SIP capacity by that many endpoints. For details on alternate endpoint administration see *Alternative Endpoint administration considerations and impacts*.

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	
Origination Dial Pattern Sets	1,000	100,000 Origination Dial Patterns per Origination Dial Pattern Set
SIP Domains	1,000	
SIP Entities	25,000	

Table continues...

Entities	Numbers (supported limits)	Notes
SIP Entity Links/System Manager	75,000	<ol style="list-style-type: none"> Assuming 3 links for each SIP entity, such as, UDP, TCP, and TLS links. Assuming that each SIP Entity is linked to two Session Managers (for redundancy) with only one transport protocol used. Here, 50,000 links are needed. <p>In both cases, the inter-Session Manager entity links need to be counted towards the limit.</p>
SIP Entity Links/Session Manager	10,000	
Adaptations	25,000	Assuming one Adaptation for each SIP Entity. There can be multiple 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 ingress and egress entries.
Conditions	25,000	
Regular Expression Adaptations	25,000	Maximum of 25k regex adaptations
Regular Expressions	1,000	
Routing Policies	25,000	Assuming one routing policy for each SIP Entity.
Time Ranges	1,000	
Locations	25,000	Considers 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	300,000	Total number of users.
Handles/User	3	
Total number of SIP handles	1,050,000	Average number of handles/user is 3 (total handles = 350,000 X 3)
Total SIP devices	1,000,000	Total number of devices.

Table continues...

Entities	Numbers (supported limits)	Notes
Registered Devices/User	10	A SIP user/station can have multiple registered SIP devices 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 per user).
Active (Primary) SIP Devices/Session Manager	23,300 (normal conditions) 25,000 (temporarily under failure conditions)	If a user has multiple registered SIP devices, be careful when distributing users across Session Managers to avoid exceeding the SIP device 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	21,600 (normal conditions) 25,200 (failure conditions)	Call Center (CC) Agent SIP devices consume more resources per Session Manager. 21,600 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	21,600 (normal conditions) 25,200 (temporarily during failure conditions)	
Digit Conversion Patterns (ingress)	45,000	
Digit Conversion Patterns (egress)	45,000	
Users/Session Manager on VMware		See <i>Deploying Avaya Aura[®] Session Manager and Avaya Aura[®] Branch Session Manager in Virtualized Environment</i> on the Avaya support website.
Branch Session Manager instances	5,000	

Table continues...

Entities	Numbers (supported limits)	Notes
Devices per Branch Session Manager on S8300D (Survivable Embedded)	700	<p>The introduction of Spectre and Meltdown fixes with the Avaya Aura® Release 7.1.3 impacts 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.</p> <p>Since the Spectre and Meltdown fixes are enabled by default, consider configuration changes to upgrade to Release 7.1.3.</p> <p>Consider the following options if the higher capacity is required from the S8300D:</p> <ul style="list-style-type: none"> • Disable Spectre and Meltdown fixes on S8300D. This allows the S8300D to deliver the same level of capacity as in the Avaya Aura® Release 7.1.2 and before. • Upgrade the embedded server to the latest S8300E model if disabling fixes on the S8300D is not viable. <p>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.</p>
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	648,000	The type of call determines the number of SIP sessions. An SRE call is a single session, so a 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	180	
Session creations/second/ Branch Session Manager	10	
Session creations/second / survivable embedded Session Manager	3	

Alternative Endpoint administration considerations and impacts

The current method for administering non-SIP endpoints is to use either of the following:

- System Manager to create a non-SIP 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 endpoints

An alternative method for administering non-SIP, such as H.323 and analog, is to use System Manager to create a SIP profile for an non-SIP endpoint. URE routing will automatically route calls to the correct Communication Manager.

The alternative method:

- Simplifies Session Manager routing configuration.
- Allows non-SIP endpoints to have multiple SIP handles.
- 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.

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:

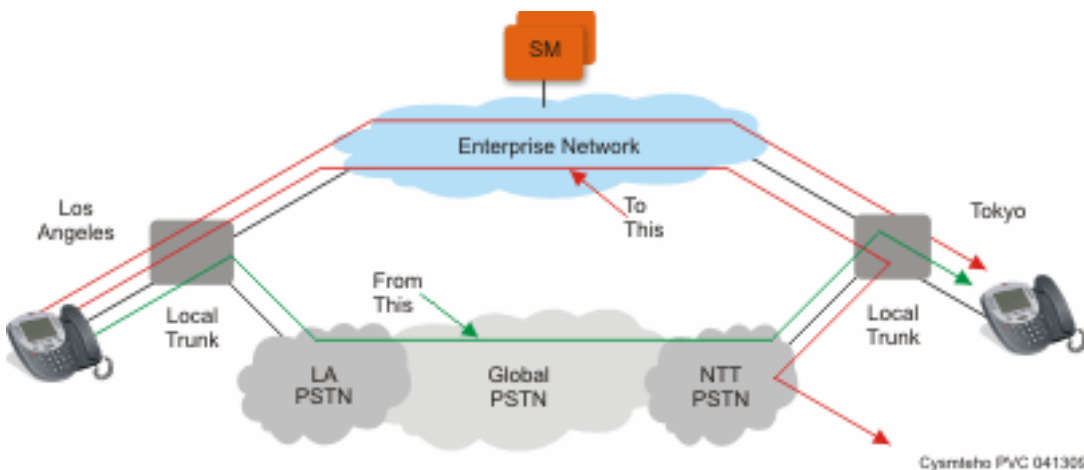
- E.164 Public Numbering Plan
- Enterprise Canonical (Private Numbering Plan)

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.

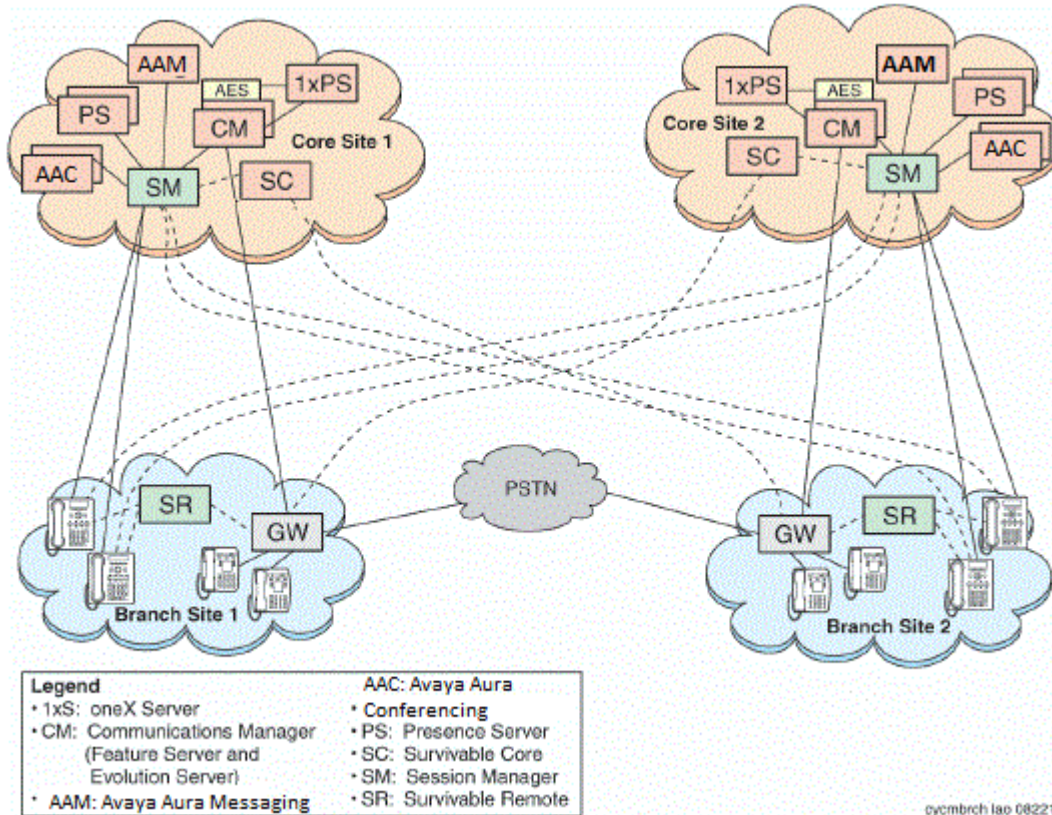
Session Manager redundancy supports networks with round trip delays of less than one second.

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

Session Manager documentation

The following table lists the documents related to Session Manager. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Description	Audience
Overview		
<i>Avaya Aura® Session Manager Overview and Specification</i>	Describes the key features of Session Manager.	System administrators
<i>Avaya Aura® Session Manager Security Design</i>	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Implementation		
<i>Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment</i>	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Services and support personnel
<i>Deploying Avaya Aura® Session Manager in Infrastructure as a Service Environment</i>	Describes how to deploy the Session Manager in the Infrastructure as a Service (IaaS) environment.	Services and support personnel
<i>Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Software-Only Environment</i>	Describes how to deploy the Session Manager in the Software-Only environment.	Services and support personnel
<i>Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtual Appliance</i>	Describes how to deploy the Session Manager in Virtual Appliance.	Services and support personnel
<i>Routing Web Service API Programming Reference</i>	Describes how to use the System Manager Routing Web Service API for Session Manager.	Services and support personnel
<i>Avaya Aura® Session Manager Element Manager Web Service API Programming Reference</i>	Describes how to get programmatic access to Session Manager Dashboard and User Registration status data.	Services and support personnel

Table continues...

Title	Description	Audience
Administration		
<i>Administering Avaya Aura® Session Manager</i>	Describes the procedures to administer Session Manager using System Manager.	System administrators
<i>Avaya Aura® Session Manager Case Studies</i>	Provides common administration scenarios.	System administrators
<i>Avaya Aura® Session Manager Data Privacy Guidelines</i>	Describes how to administer Session Manager to fulfill Data Privacy requirements.	System administrators, Network administrators, services, and support personnel
Installation and upgrades		
<i>Upgrading Avaya Aura® Session Manager</i>	Describes the procedures to upgrade Session Manager to the latest software release.	Services and support personnel
Maintaining and Troubleshooting		
<i>Maintaining Avaya Aura® Session Manager</i>	Contains the procedures for maintaining Session Manager.	Services and support personnel
<i>Troubleshooting Avaya Aura® Session Manager</i>	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. Go to <https://support.avaya.com>.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

The **Choose Release** field is not available if there is only one release for the product.

6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

7. Click **Enter**.

Accessing the port matrix document

Procedure

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



Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at <https://documentation.avaya.com>.


Important:

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

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
 - Click **Filters** to select a product and then type key words in **Search**.
 - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** () to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** ().

Navigate to the **Manage Content > My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
- Add topics from various documents to a collection.
- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon ().

Navigate to the **Manage Content > Watchlist** menu, and do the following:

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

 **Note:**

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

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
20980W	What's New with Avaya Aura® Release 8.1
71200V	Integrating Avaya Aura® Core Components
72200V	Supporting Avaya Aura® Core Components
20130V	Administering Avaya Aura® System Manager Release 8.1

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

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

 **Note:**

Videos are not available for all products.

Support

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

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

A

accessing port matrix	46
adaptations	19
add/remove skill button	18
alternate routing	15
applications	
sequencing	10
aux-work button	16
Avaya Aura Device Services	
overview	17
Avaya support website	48

C

call reconstruction	10
Cassandra clustering	
overview	17
CDR	11
centralized	
dial plan	38
routing	38
SIP trunking	12
collection	
delete	46
edit name	46
generating PDF	46
sharing content	46
Communication Manager	
IGAR	13
LNCC	13
connection policy	
SIP endpoint concentrator	12
content	
publishing PDF output	46
searching	46
sharing	46
sort by last updated	46
watching for updates	46

D

data replication	17
dial plan	38
documentation	
Session Manager	44
documentation center	46
finding content	46
navigation	46
documentation portal	46
finding content	46
navigation	46
document changes	6

F

feature matrix	
Session Manager	25
finding content on documentation center	46
finding port matrix	46

G

global routing	38
----------------------	--------------------

H

hunt group Log in/Log out button	16
--	--------------------

I

InSite Knowledge Base	48
inter-gateway alternate routing for SIP endpoints	13
iOS	
push notifications	19

L

least-cost routing	15
Limit Number of Concurrent Calls	13
load balancing	15 , 38

M

mutual authentication	18
My Docs	46

N

new in release	
Session Manager	21–24
Non-SIP endpoint considerations	38
normalized network	14

O

overview	
Avaya Aura Device Services	17
Session Manager	8

P

policy-based routing	38
port assignments	43
port matrix	46

PPM [15](#)
 push notifications [19](#)

R

Regular Expression Adaptations [19](#)
 routing
 alternate [38](#)
 global [38](#)
 policy-based [38](#)

S

searching for content [46](#)
 security specification [43](#)
 sequenced applications [10](#)
 Session Manager
 feature matrix [25](#)
 new in release [21–24](#)
 overview [8](#)
 what’s new [21](#)
 sharing content [46](#)
 sip phones [16](#)
 SIP Resiliency [10](#)
 SIP trunking [12](#)
 sort documents by last updated [46](#)
 support [48](#)
 Survivable Remote [41](#)
 System Manager
 web services [16](#)

T

tail end hop off [39](#)
 TLS certificate [18](#)
 TLS mutual authentication [18](#)

V

videos [48](#)

W

watch list [46](#)
 web services
 System Manager [16](#)
 what’s new
 Session Manager [21](#)