Avaya Aura® Session Manager Overview and Specification

Release 10.2.x
Issue 9
March 2026

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction 6
- Purpose 6
- Changes to platform support 6
- Change history 6

Chapter 2: Session Manager overview 8
- Session Manager feature matrix 8
- Features 11
  - Add/remove skill button 11
  - Application Sequencing 11
  - Avaya Aura® support for third party clients 12
  - Branch Visiting User survivability 12
  - Call Detail Recording on Session Manager 12
  - Centralized applications 13
  - Centralized SIP trunking 13
  - Edge friendly branch survivability 13
  - Hunt Group Log in/Log out button for SIP phones in a non-CC Environment 14
  - HTTP proxy 14
  - Inter-gateway Alternate Routing for SIP endpoints 15
  - Limit Number of Concurrent Calls for SIP endpoints 15
  - Normalization of disparate networks 16
  - Online/Offline Call Journal (Call History) 16
  - Personal Profile Manager 17
  - Policy-based routing 17
  - Policy-based Assignment of Users to Session Managers Overview 17
  - Push notifications 18
  - Regular Expression Adaptations 19
  - Session Manager and Avaya Aura® Device Services integration 20
  - SIP Endpoint Concentrator Connection Policy 21
  - SIP Resiliency 21
  - Stir/Shaken message normalization and adaptation module 22
  - System Manager Web Services 22
  - TLS mutual authentication for SIP endpoints 23
- Supported servers 24

Chapter 3: What's new in Session Manager 25
- New in this release 25
  - New in Session Manager Release 10.2.1.1 25
  - New in Session Manager Release 10.2.1 25
  - New in Session Manager Release 10.2 26

Chapter 4: Capacity limits 29

Supported footprints of Session Manager on VMware 29
Supported footprints of Branch Session Manager on VMware 31
Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10) 32
Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) 33
Chapter 5: Interoperability 34
Product compatibility 34
Accessing the Compatibility Matrix 34
Supported Avaya endpoints 34
Chapter 6: Licensing Requirements 35
Licensing requirements 35
Chapter 7: Performance and capacity specifications 36
Capacity and scalability specification 36
Alternative Endpoint administration considerations and impacts 40
Dial plan specification 41
Tail end hop off 41
Call Admission Control specification 42
Redundancy and high availability 42
Survivable Core Server 43
Survivable Remote 43
Chapter 8: Security 45
Security specification 45
Port assignments 45
Chapter 9: Resources 46
Session Manager documentation 46
Finding documents on the Avaya Support website 47
Accessing the port matrix document 47
Avaya Documentation Center navigation 48
Training 49
Viewing Avaya Mentor videos 49
Support 50
Using the Avaya InSite Knowledge Base 50
Glossary 52

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.

Changes to platform support

As of January 1, 2026, Avaya has refined its infrastructure support strategy for Avaya Aura® and Surround Applications. This update specifically impacts Software-Only and Infrastructure as a Service (IaaS) deployment models. To ensure your environment remains compliant and supported, review the following changes to supported platforms:

Discontinued Platforms:

- Hypervisor: Microsoft Hyper-V
- Cloud Platforms: Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud

Supported platforms for Software Only and Infrastructure as a Service (IaaS) deployment models:

- Cloud Platform: AWS
- On-premises platforms: KVM, Nutanix, VMware

Change history

Issue	Date	Summary of changes
9	March 2026	Added the section: Changes to platform support on page 6

Table continues…

Issue	Date	Summary of changes
8	February 2026	Updated the following section: • Supported servers on page 24
7	August 2025	Updated the following section: • Cassandra clustering and data replication overview on page 20
6	June 2025	Updated the following section: • Licensing requirements on page 35
5	April 2025	Added the following sections for R10.2.1.1: • New in Session Manager Release 10.2.1.1 on page 25 • HTTP proxy on page 14 Updated the following sections for R10.2.1.1: • Session Manager feature matrix on page 8
4	March 2025	Updated the product name from “Avaya Cloud Office” to “Avaya Cloud Office Hybrid”
3	December 2024	Added the following sections for R10.2.1: • New in Session Manager Release 10.2.1 on page 25 • Avaya Aura support for third party clients on page 12 • Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 32 • Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 33 Updated the following sections for R10.2.1: • Session Manager feature matrix on page 8 • System Manager Web Services on page 22 • Supported servers on page 24 • Supported footprints of Session Manager on VMware on page 29 • Supported footprints of Branch Session Manager on VMware on page 31 • Capacity and scalability specification on page 36
2	February 2024	Updated the following section: Capacity and scalability specification on page 36
1	December 2023	Release 10.2

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.

Session Manager feature matrix

The following table lists the feature matrix of Session Manager from Release 7.1.x to Release 10.2.x. The features listed in the table covers the key features only.

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x	Release 10.2.x
OVA signing	Y	Y	Y	Y	Y
IPv6 support	Y	Y	Y	Y	Y
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y	Y
Compliance with DISA security STIGs	Y	Y	Y	Y (R 10.1.0.2 onwards)	Y
Extended Security Hardening	Y	Y	Y	Y	Y
Conference factory URI	Y	Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y	Y
Customer Root Access		Y	Y	Y	Y
Preserve security hardening modes on upgrade		Y	Y	Y	Y
SIP Resiliency		Y	Y	Y	Y
Extended host name validation		Y	Y	Y	Y
Cassandra clustering	Y	Y	Y	Y	Y
Support for Software-only deployment		Y	Y	Y	Y
Support for 16 digit dial plan		Y	Y	Y	Y
Support for Hyper-V in Software-Only environment		Y	Y	Y	Y
Support for Regular Expression based adaptation module		Y	Y	Y	Y
Support for Call Journaling Server High Availability		Y	Y	Y	Y
Cassandra security hardening		Y	Y	Y	Y
Support for multiple customer accounts		Y	Y	Y	Y
Support for role-based access control		Y	Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x	Release 10.2.x
Support for Avaya Solutions Platform 120 Appliance		Y	Y		
Support for Avaya Solutions Platform 130 Appliance		Y	Y	Y	Y
Syslog server configuration			Y	Y	Y
Data Encryption			Y	Y	Y
Branch Visiting User			Y	Y	Y
Apple Push notification			Y	Y	Y
Support for VMware ESXi 7.0			Y	Y	Y
Policy-based Assignment of Users to Session Manager				Y	Y
Registration of SIP Clients to four Session Managers				Y	Y
Support for TLS 1.3				Y	Y
Android Push notification				Y	Y
Support for Red Hat Enterprise Linux (RHEL) 8.4				Y	Y
Support for Red Hat Enterprise Linux (RHEL) 8.10					Y (R 10.2.1 onwards)
Avaya Solutions Platform S8300 for Branch Session Manager				Y	Y
Support for VMware ESXi 8.0					Y
Support for Edge friendly branch survivability					Y
Support of Stir/ Shaken message normalization and adaptation module					Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x	Release 10.2.x
Support of Avaya Aura® X for Zoom Workplace				Y	Y
Support of Avaya Cloud Office Hybrid					Y
Support for Avaya Solutions Platform S8300 Release 5.x				Y	Y
Support for Avaya Solutions Platform S8300 Release 6.0.x			Y	Y	Y
Support for Avaya Solutions Platform 130 Release 5.x			Y	Y	Y
Support for Avaya Solutions Platform 130 Release 6.0.x			Y	Y	Y
Support for HTTP Proxy					Y R10.2.1.1 onwards

Features

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 Experience Platform® On-Prem (AXP On-Prem, formerly Avaya Aura® Call Center Elite) Feature Reference*.

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

Avaya Aura® support for third party clients

Avaya Aura® supports Avaya Aura® X for Zoom Workplace (ZOOM) and Avaya Cloud Office Hybrid feature. Users can use the Avaya Aura® features from Zoom Workplace or Avaya Cloud Office Hybrid through a license subscription. Avaya Aura®System Manager tracks the license count for ZOOM and Avaya Cloud Office Hybrid features. The license count determines the number of users who can use the ZOOM or Avaya Cloud Office Hybrid features. System Manager audits the license count every nine minutes and generates a license error alarm if the user count exceeds the permissible count. System Manager displays the license error until the user count returns to the permissible count.

For more information about how to register a Zoom Workplace client with Avaya Aura®, see Configuring the Zoom-Avaya Aura integration.

For more information about enabling Avaya Aura® X for Zoom Workplace or Avaya Cloud Office Hybrid feature, see *Administering Avaya Aura® Session Manager*.

Branch Visiting User survivability

The Branch Visiting User survivability feature is a resiliency feature that automatically assigns a Branch Session Manager to a user at a visiting location and provides local survivability during a WAN outage. With this feature, you do not need to manually administer a Branch Session Manager or change the existing Branch Session Manager with the local Branch Session Manager for the visiting user.

The calling and device features available to a visiting user depend on the user's administered Communication Manager with respect to the Survivable Remote Server (SRS) of the visiting branch and the state of the branch network when the user arrives.

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.

Edge friendly branch survivability

In an Edge friendly branch survivability configuration, the survivable components, SRS and Branch Session Manager, in the G4xx media gateways connect to the core Communication

Manager and Session Manager on cloud. The connection between the media gateways and cloud is over the Internet or through SD-WAN. Thus, providing you a comprehensive Total Cost of Ownership (TCO) advantages.

An Avaya Session Border Controller (SBC) is required at the core edge for connectivity to the branch. Third-party SBC is not supported in an edge friendly branch survivability configuration.

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*.

HTTP proxy

From release 10.2.1.1, you can configure HTTP proxies from the HTTP Proxy Configuration page for the following features:

- CRL download
- Push Notification

HTTP Proxies can be configured using IPv4 addresses or FQDNs. If multiple HTTP Proxies are administered, Session Manager selects a proxy based on the proxy's accessibility and the order that it appears on the HTTP Proxy Configuration page.

Note:

Avaya recommends using HTTP Proxy Configuration page instead of the Global Settings page to configure the HTTP proxies. Configuration values from the HTTP Proxy Configuration page override the HTTP Proxy values on the Global Settings page.

For more information about the HTTP Proxy administration, see *Administering Avaya Aura® System Manager*.

For more information about the HTTP Proxy related commands, see *Troubleshooting Avaya Aura® Session Manager*.

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.

Policy-based Assignment of Users to Session Managers Overview

The policy-based assignment feature provides dynamic assignment of Session Managers based on a defined policy. A policy-based model indicates that the system selects the Session Manager servers based on a defined policy. The dynamic assignment occurs when the user logs in to their device. If a user logs in through multiple devices, the system applies the policy for each device login. Therefore, all devices of a user are assigned to the same set of Session Managers at a time.

When a user is assigned a Session Manager(s) dynamically, the system stores these assignments details in the Cassandra database. All Session Managers can access this data from Cassandra

database. If the Session Manager server restarts, the system continues to perform the dynamic assignment of Session Managers.

The following policies can be applied to a user’s communication profile:

- Fixed
- Fixed-region
- Location-region

To administer the policy-based assignment feature, select the **Enable Policy Based Assignment of Session Managers** option on the **Elements** > **Session Manager** > **Global Settings** page.

Note:

Before you enable the Policy-based Assignment of Users to Session Managers feature and pair Session Managers to Avaya Aura® Device Services, ensure that Avaya Aura® Device Services is on Release 8.1.4.

Fixed policy

This policy provides a fixed set of Session Managers to be assigned to a user. This policy is in line with the current practice of manual Session Manager assignment to a user and is maintained for backward compatibility. You can now assign up to 4 Session Managers to a user's profile with this policy. The additional two Session Managers allow both local and geo-redundancy simultaneously for added reliability.

Fixed-region policy

This policy dynamically assigns Session Managers to a user based on fixed administered regions. These regions are administered with the required Session Managers that eliminates the need to administer specific Session Managers to a user. The user is assigned to the Session Manager group or regions, and the policy selects the least loaded Session Managers within the regions and assigns it to the user.

Whenever a region assignment in a user’s communication profile is changed, the updates to the user’s Session Manager profile occurs immediately. If Session Manager assignment within the region is changed, then the system reflects the changes for the user’s Session Manager profile within 24 hours. A region group requires a minimum of one Session Manager and a minimum of two Session Managers if the same region is assigned to a communication profile more than once (for example: primary and secondary region). If the region is not referenced in a **Location To Region Mapping** or in a user's Session Manager profile, you can delete regions with Session Managers assigned.

Location-region policy

This policy determines the Session Managers assigned to the user based on the location of the last device login. A user’s location is mapped to regions on the Session Manager Groups page. When a user’s communication profile is assigned with the location-region policy, the least loaded Session Managers are selected from the regions mapped to the user’s location. The location-region policy helps to spread the load evenly across given regions.

Push notifications

The push notification mechanism enables clients to receive incoming call alerts and other notifications from the Push Notification service. 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 push notification service through a push notification provider. You must register your Session Manager cluster 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 cluster. This account requirement does not apply if you are working with a third-party provider.

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.

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

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® Device Services should 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.

SIP Endpoint Concentrator Connection Policy

To inter-operate with virtualized desktop solutions such as a Citrix server hosting 1xC or an Ascom IPVM, the Endpoint Concentrator (endpt conc) connection policy provides for up to 4000 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 4000 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**.

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 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*.

Stir/Shaken message normalization and adaptation module

The StirShakenAdapter adaptation module can display the attestation or verification level that is set by the service provider on the agent phone. The StirShakenAdapter operates on inbound and outbound call (INVITE) requests and can modify the STIR/SHAKEN information present in the SIP messaging.

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 interface supports the following:

- Administration

- User registration
- Implicit users

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.

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.

Supported servers

- Avaya Solutions Platform S8300 Release 6.0 for Communication Manager and Branch Session Manager
- Avaya Solutions Platform 130 Release 6.0 Appliance: Dell PowerEdge R640 and R660xs

Chapter 3: What's new in Session Manager

This chapter provides an overview of the new and enhanced features of Session Manager Release 10.2.x.

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

New in this release

New in Session Manager Release 10.2.1.1

Avaya Aura® Session Manager Release 10.2.1.1 supports the following new feature:

HTTP proxy

You can configure HTTP proxies from the HTTP Proxy Configuration page for CRL download and Push Notification. HTTP Proxies can be configured using IPv4 addresses or FQDNs. If multiple HTTP Proxies are administered, Session Manager selects a proxy based on the proxy's accessibility and the order that it appears on the HTTP Proxy Configuration page.

Note:

Avaya recommends using HTTP Proxy Configuration page instead of the Global Settings page to configure the HTTP proxies. Configuration values from the HTTP Proxy Configuration page override the HTTP Proxy values on the Global Settings page.

For more information about the HTTP Proxy administration, see *Administering Avaya Aura® System Manager*.

For more information about the HTTP Proxy related commands, see *Troubleshooting Avaya Aura® Session Manager*.

New in Session Manager Release 10.2.1

Avaya Aura® Session Manager Release 10.2.1 supports the following new feature:

Avaya Aura® X for Zoom Workplace

Avaya Aura® supports Avaya Aura® X for Zoom Workplace (ZOOM) feature. Users can use the Avaya Aura® features from Zoom Workplace through a license subscription. Avaya Aura®System Manager tracks the license count for Avaya Aura® X for Zoom Workplace. The license count determines the number of users using the Avaya Aura® X for Zoom Workplace feature. The

System Manager generates a license error alarm if the user count exceeds the permissible count. Enable Avaya Aura® X for Zoom Workplace feature through the System Manager web console. For more information about enabling Avaya Aura® X for Zoom Workplace feature, see *Administering Avaya Aura® Session Manager*.

Avaya Cloud Office Hybrid

Avaya Aura® supports Avaya Cloud Office Hybrid from release 10.2.1. Users can use the Avaya Aura® features from Avaya Cloud Office Hybrid through a license subscription. Avaya Aura®System Manager tracks the license count for Avaya Cloud Office Hybrid. The license count determines the number of users using the Avaya Aura® features from Avaya Cloud Office Hybrid. The System Manager generates a license error alarm if the user count exceeds the permissible count. Enable Avaya Cloud Office Hybrid feature through the System Manager web console. For more information about enabling Avaya Cloud Office Hybrid feature, see *Administering Avaya Aura® Session Manager*.

Support for System Manager Web Services implicit user roles

System Manager Web Services support creating, reading, updating, and deleting of implicit user roles.

Support for Software-Only Deployment on Nutanix Environment

With Release 10.2, the Session Manager Software-Only application can be deployed on Nutanix 6.5 and later.

Red Hat Enterprise Linux (RHEL) 8.10 support

With Release 10.2.1, Session Manager supports Red Hat Enterprise Linux Release 8.10.

Kernel-based Virtual Machine (KVM) on RHEL 8.10 hypervisor support

With Release 10.2, Session Manager can be deployed on Avaya-supplied KVM on RHEL Release 8.10 hypervisor (Avaya Solutions Platform 130 R6.0).

New in Session Manager Release 10.2

Avaya Aura® Session Manager Release 10.2 supports the following new features and enhancements:

Enhancement to the patchSM command with the --snapshot option

With Release 10.2, the **`patchSM`** command is enhanced to take the snapshot while installing the Session Manager or Branch Session Manager patch in a virtualized environment.

Support of the vmsnapshot command

With Release 10.2, use the **`vmsnapshot`** command to create, remove, revert, and list the snapshot of Session Manager and Branch Session Manager deployed in a virtualized environment.

Edge friendly branch survivability

With Release 10.2, you can use the edge topology configuration for cloud deployment. Avaya Aura® 10.1 supported Edge friendly gateways to seamlessly establish connections between the on-premise G4xx media gateways and core Communication Manager hosted on the cloud. This safeguards your investments when transitioning to a cloud-based infrastructure.

With Avaya Aura® 10.2, the migration to cloud is made more easier by allowing the survivable components, SRS and Branch Session Manager, in the G4xx media gateways to connect to the core Communication Manager and Session Manager on cloud. The connection between the media gateways and cloud can be over the Internet or through SD-WAN. Thus, providing you a comprehensive Total Cost of Ownership (TCO) advantages.

With Release 10.2:

- To deploy the edge Branch Session Manager set up in a virtualized environment, a new **Edge Topology BSM** option is added in the Branch Session Manager Settings section.
- To configure the edge Branch Session Manager server, a new **`edgeSetup`** command is added.
- To enable edge topology for core Session Manager and edge Branch Session Manager on the **Elements** > **Session Manager** > **Global Settings** page, the **Enable Edge Topology** check box is added.
- To create core Session Manager and edge Branch Session Manager SIP entities on the **Elements** > **Routing** > **SIP Entities** page, the **Network Topology**, **SBC Public IP Address or FQDN**, and **SBC Private IP Address or FQDN** fields are added.
- To display the core Session Manager and edge Branch Session Manager SIP entities configuration on the Session Manager Dashboard page, a new **Topology** column is added.
- To add an edge Branch Session Manager instance on the **Elements** > **Session Manager** > **Session Manager Administration** > **Branch Session Manager Instances** page, when you select the edge Branch Session Manager SIP entity, Session Manager:
  - Renames the **Management Access Point FQDN/IP** field to **Management Access Point FQDN**.
  - Displays the **Network Topology** and **Remote Access Configuration** fields.

Enhancement to the Remote Access Configuration page

With Release 10.2, on the Remote Access Configuration page:

- A new **SIP Proxy Public FQDN (Reference A)** column is added in SIP Proxy Mapping Table.
- If **Enable Edge Topology** is enabled on the Global Settings page, the system displays the **Translate Address** column in SIP Proxy Private IP Addresses.

  If you select the **Translate Address** check box, edge Branch Session Manager performs the address translation for the specified table entry, not Session Border Controller.

Support of Stir/Shaken message normalization and adaptation module

STIR/Shaken is a suite of protocols intended to reduce caller ID spoofing on public telephone networks.

Avaya Aura® 10.2 supports STIR/Shaken and can display the attestation or verification level that is set by the service provider on the agent phone. This feature can work only over SIP trunks. You can enable or disable this feature at a system level according to your preference.

With Release 10.2, you can configure the following:

- The **Stir/Shaken Ingress Normalization** option to set the message normalization for the inbound messages on the **Elements** > **Session Manager** > **Global Settings** page.

- In the **Module Name** field, you can select the **StirShakenAdapter** adaptation module on the **Elements** > **Routing** > **Adaptations** > **Adaptations** page.

Support for Trellix AV (formerly known as McAfee) in Virtualized Deployments

Avaya Aura® Release 10.2 supports the deployment of Trellix AV software in a virtualized (OVA-based) environment. This new feature effectively detects, prevents, and eliminates malware threats, resulting in enhancing the security of your Avaya Aura® environment. The IT industry widely recognizes Trellix AV as a trusted cybersecurity solution. With the integration capabilities in Avaya Aura® Release 10.2, you can seamlessly integrate Avaya Aura® applications as managed devices as part of your existing Trellix deployment. For more information on support of Trellix for AV on Avaya Aura®, see *Application Note for Support of Trellix AV on Avaya Aura®* on the Avaya Support website at https://support.avaya.com.

Support for VMware 8.0

With Release 10.2, Avaya Aura® applications support the VMware® vSphere ESXi 8.0 and VMware® vCenter Server 8.0 in a VMware virtualized environment.

Chapter 4: Capacity limits

Supported footprints of Session Manager on VMware

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.

Note:

Avaya Aura® Session Manager supports VMware hosts with Hyperthreading enabled at the BIOS level.

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					
vCPUs	3	5	8	12	20	53
CPU MHz Reservation	3300	5500	8800	13200	22000	58300
Memory Reservation	5132MiB	7828 MiB	10552 MiB	13368 MiB	24370 MiB	74064 MiB
SIP Devices[1] (Normal/Failure) [2]	2K/2.4K	4.5K/5K	7K/8K	10K/12K	23.3K/ 25K	66.7K/72K
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/90 K	150/540K/ 170K	180/648K/ 510K
HDD for VMware OVA (GiB)[3]	100	100	135	135	210	210

Table continues…

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
HDD for Software-Only ISO (GiB)[4]	100	100	135	135	210	210

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. HDD for VMware OVA: When deployed with SDM. Other deployment methods require that disk size be resized manually.
4. You can deploy Session Manager software-only *ISO image* on VMware, KVM, 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 soft clients are using Avaya Aura® Device Services.

Session Manager profile	Total SIP devices	Number of Workplace devices	Previous Workplace devices
Profile 1	2,000	1,200	750

Table continues…

Session Manager profile	Total SIP devices	Number of Workplace devices	Previous Workplace devices
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 on VMware

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

Note:

Avaya Aura® Session Manager supports VMware hosts with Hyperthreading enabled at the BIOS level.

A gibibyte (GiB) and a gigabyte (GB) are sometimes used as synonyms, though they do not describe the same output of capacity technically. However, they are close in size. A gibibyte = 1024^3 and gigabyte = 1000^3.

The terms mebibyte and megabyte are closely related and often used as synonyms, though they don't technically refer to the same amount of capacity. However, they are close in size, One mebibyte equals 1.048576 megabytes.

Branch Session Manager Device Footprints	Up to 1K Devices	1k to 5K Devices
CPU Minimum	2200 MHz	
vCPUs	2	4
CPU MHz Reservation	2200	4400
Memory Reservation	3164 MiB	4952 MiB
CC Agents Max	583	4167
Sessions (Sec/Hour/Max)	3/10.8K/4.8K	30/108K/35K
HDD (GiB)	50	50

Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10)

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

Note:

Avaya Aura® Session Manager supports KVM hosts with Hyperthreading enabled at the BIOS level.

Session Manager Device Footprints	Up to 2K Devices	2K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices (R1 footprint)	10K to 23.5K Devices (R2 footprint)	23.5K to 72K Devices
CPU Minimum	2200 MHz					
vCPUs	3	5	8	12	20	53
CPU MHz Reservation[1]	3300	5500	8800	13200	22000	58300
Memory Reservation[1]	5132 MiB	7828 MiB	10552 MiB	13368 MiB	24370 MiB	74064 MiB
SIP Devices[2] (Normal/Failure)[3]	2K/2.4K	4.5K/5K	7K/8K	10K/12K	23.3K/ 25K	66.7K/72K
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/90 K	150/540K/ 170K	180/648K/ 510K
HDD for VMware OVA (GiB)	100	100	135	135	210	210

Note:

1. Ensure to consider reservations for deploying Avaya Aura® applications on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300.
2. SIP devices: It includes all hard endpoints, soft clients, AST/NON-AST SIP endpoints and third-party endpoints.
3. 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.

Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10)

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

Note:

Avaya Aura® Session Manager supports KVM hosts with Hyperthreading enabled at the BIOS level.

A gibibyte = 1024^3 and gigabyte = 1000^3

The terms mebibyte and megabyte are closely related and often used as synonyms, though they don't technically refer to the same amount of capacity. However, they are close in size, One mebibyte equals 1.048576 megabytes.

Branch Session Manager Device Footprints	Up to 1K Devices	1k to 5K Devices
CPU Minimum	2200 MHz	
vCPUs	2	4
CPU MHz Reservation	2200	4400
Memory Reservation	3164 MiB	4952 MiB
CC Agents Max	583	4167
Sessions (Sec/Hour/Max)	3/10.8K/4.8K	30/108K/35K
HDD (GiB)	50	50

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). Use 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 10.2.
2. Install Session Manager 10.2 license file on System Manager Release 10.2.
3. Upgrade Session Manager to Release 10.2.

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	
Total Number of Dial Patterns	300,000	
Number of Dial Patterns per Routing Policy	120,000	
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	1. Assuming 3 links for each SIP entity, such as, UDP, TCP, and TLS links. 2. Assuming that each SIP Entity is linked to two Session Managers (for redundancy) with only one transport protocol used. Here, 50,000 links are needed. In both cases, the inter-Session Manager entity links need to be counted towards the limit.
SIP Entity Links/Session Manager	10,000	
Adaptations	25,000	Assuming one Adaptation for each SIP Entity. 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 or KVM on RHEL 8.10		See *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment* 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	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 SRS and Branch Session Manager with the Spectre and Meltdown fixes enabled can only support 200 users with up to 500 BHCC traffic. Since the Spectre and Meltdown fixes are enabled by default, consider configuration changes to upgrade to Release 7.1.3. Consider the following options if the higher capacity is required from the S8300D: • Disable Spectre and Meltdown fixes on S8300D. This allows the S8300D to deliver the same level of capacity as in the Avaya Aura® Release 7.1.2 and before. • Upgrade the embedded server to the latest S8300E model if disabling fixes on the S8300D is not viable. For more information about Spectre and Meltdown fixes included in Avaya Aura® Release 7.1.3, see PSN020346u on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101048606.
Devices per Branch Session Manager on ASP S8300E (Survivable Embedded)/VE/KVM on RHEL 8.10	1,000	
Devices per Branch Session Manager on Application Services Platform/VE/KVM on RHEL 8.10	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	

Table continues…

Entities	Numbers (supported limits)	Notes
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:

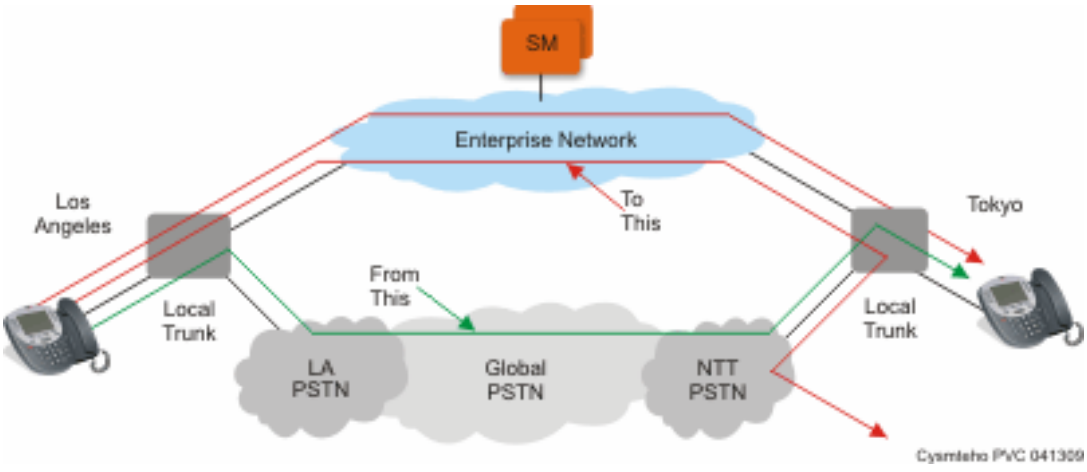
- E.164 Public Numbering Plan
- Enterprise Canonical (Private Numbering Plan)

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.

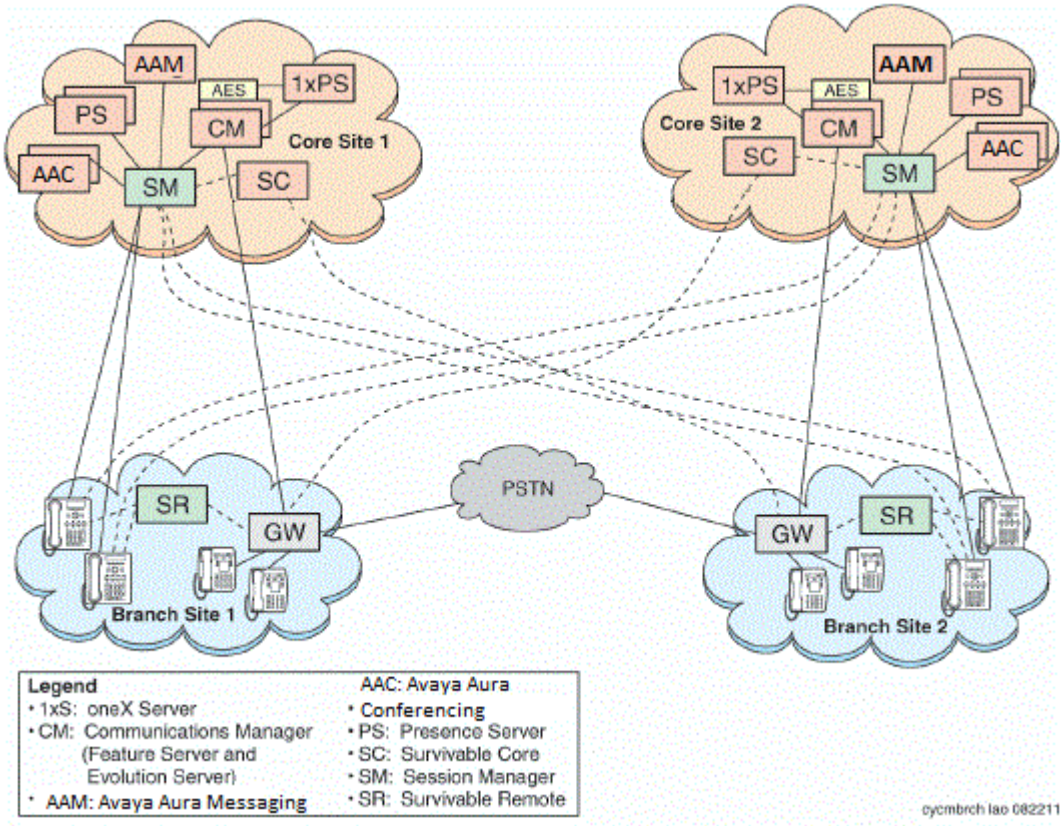
Session Manager redundancy supports networks with round trip delays of less than one second.

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 Server

A Survivable Core Server (SCS), formerly known as Enterprise Survivable Processor, 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 SCS as follows:

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

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 https://support.avaya.com.

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

Table continues…

Title	Description	Audience
Avaya Aura® Session Manager Data Privacy Guidelines	Describes how to administer Session Manager to fulfill Data Privacy requirements.	System administrators, Network administrators, services, and support personnel
Installation and upgrades		
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade Session Manager to the latest software release.	Services and support personnel
Maintaining and Troubleshooting		
Maintaining Avaya Aura® Session Manager	Contains the procedures for maintaining Session Manager.	Services and support personnel
Troubleshooting Avaya Aura® Session Manager	Contains the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.

3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.

- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.

- Send feedback for a topic.

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
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Glossary

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 47
adaptations 19
add/remove skill button 11
alternate routing 17
applications
    sequencing 11
aux-work button 14
Avaya Aura Device Services
    overview 20
Avaya InSite Knowledge Base 50
Avaya support website 50

B

branch visiting user survivability 12

C

call reconstruction 21
Cassandra clustering
    overview 20
CDR 12
centralized
    dial plan 41
    routing 41
    SIP trunking 13
change history 6
changes to platform support 6
collection
    delete 48
    edit 48
    generating PDF 48
    sharing content 48
Communication Manager
    IGAR 15
    LNCC 15
connection policy
    SIP endpoint concentrator 21
content
    publishing PDF output 48
    searching 48
    sharing 48
    sort by last updated 48
    watching for updates 48

D

data replication 20
dial plan 41
documentation
    Session Manager 46
documentation center 48
    finding content 48
    navigation 48
documentation portal 48

E

edge friendly branch survivability 13

F

feature matrix
    Session Manager 8
finding content on documentation center 48
finding port matrix 47

G

global routing 41

H

HTTP proxy 14
hunt group Log in/Log out button 14

I

inter-gateway alternate routing for SIP endpoints 15
iOS
    push notifications 18

K

KB
    Support site 50

L

least-cost routing 17
Limit Number of Concurrent Calls 15
load balancing 17, 41

M

mutual authentication 23

N

new in release

new in release *(continued)*
Session Manager 10.2 26
Session Manager 10.2.1 25
Session Manager 10.2.1.1 25
Non-SIP endpoint considerations 40
normalized network 16

O

overview
Avaya Aura Device Services 20
policy based assignment 17
Session Manager 8

P

policy based assignment overview 17
policy-based routing 41
port assignments 45
port matrix 47
PPM 17
push notifications 18

R

Regular Expression Adaptations 19
routing
alternate 41
global 41
policy-based 41

S

searching for content 48
security specification 45
sequenced applications 11
Session Manager
feature matrix 8
overview 8
what's new 25
Session Manager 10.2
new in release 26
Session Manager 10.2.1
new in release 25
Session Manager 10.2.1.1
new in release 25
sharing content 48
sip phones 14
SIP Resiliency 21
SIP trunking 13
sort documents 48
Stir/Shaken module 22
support 50
Survivable Remote 43
System Manager
web services 22

T

tail end hop off 41
TLS certificate 23
TLS mutual authentication 23

V

videos 49

W

watchlist 48
web services
System Manager 22
what's new
Session Manager 25

Z

Zoom Workplace
Session Manager licensing 12