Avaya Aura® Session Manager Overview and Specification

transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER

LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

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

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

Change history

Issue	Date	Summary of changes
1	August 2015	Initial release.
2	May 2016	The following changes were made to this document for Session Manager Release 7.0.1: • Added the TLS mutual authentication for SIP endpoints section. • Added the Session Manager and Avaya Aura® Device Services integration section. • Added the Hunt Group Log in/Log out button for SIP phones in a non-CC Environment section. • Added the Add/remove skill button section.

Warranty

Avaya provides a 90-day limited warranty on Session Manager. For more information about the terms of the limited warranty, see the sales agreement or other applicable documentation.

You can view the standard warranty information about Session Manager support on the Avaya Support website at https://support.avaya.com. You can find the warranty information and license terms at the bottom of the page under:

• **Help & Policies > Policies & Legal > Warranty & Product Lifecycle**

- **Help & Policies > Policies & Legal > License Terms**

Chapter 2: Overview

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

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

Specifically, Session Manager provides:

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

Supported servers

Session Manager supports the following servers:

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

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

Branch Session Manager supports the following servers:

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

These supported servers are only for Appliance Virtualization Platform configurations.

HP and Dell will discontinue the HP DL360 G7 and Dell R610 servers in the near future. For more information, see the respective vendor websites.

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

Features

Application Sequencing

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

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

Session Manager also supports application sequencing for third-party PBX endpoint. Typical applications include blocking calls based on user preferences, redirecting calls to users in the Avaya

Aura® enterprise, and augmenting caller identification information for incoming and outgoing calls. You can enable Application Sequencing without needing to upgrade or modify the code on existing third-party PBX equipment. For more information about Application Sequencing, see *Administering Avaya Aura® Session Manager*.

Call Detail Recording on Session Manager

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

The call record contains information regarding:

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

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

> ✱ **Note:**
>
> Survivable Remote Session Manager (Branch Session Manager) does not support CDR.

CDR records on Session Manager are created on connected calls.

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

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

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

Centralized applications

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

and deployment of adjuncts much simpler than methods where each PBX connects to its own adjunct.

Centralized SIP trunking

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

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

SIP Endpoint Concentrator Connection Policy

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

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

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

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

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

> ✱ **Note:**
>
> SIP Link Monitoring is not available for SIP entities of type **Endpoint Concentrator**.

Inter-gateway Alternate Routing for SIP endpoints

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

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

The IGAR triggers include:

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

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

Use cases:

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

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

Limit Number of Concurrent Calls for SIP endpoints

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

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

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

LNCC allows:

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

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

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

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

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

Normalization of disparate networks

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

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

Online/Offline Call Journal (Call History)

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

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

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

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

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

SIP phones:

- Download call logs during login only.

- Maintain call logs locally while logged in.

Personal Profile Manager

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

- retrieve configuration information such as dial plans, buttons, and contact lists.

- add or update contacts.

- save device-specific data.

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

Policy-based routing

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

- **Least-cost routing**, also called time-of-day routing, uses the lowest cost route from a list of service providers on a time-of-day or time-of-week basis.

- **Alternate routing** routes calls around network failures on a global basis and uses global PSTN fallback when the internal network is unavailable.

- **Load balancing** distributes calls. For a given SIP entity, you can administer Session Manager to select a host from multiple IP addresses based on administered priorities and weights.

- **Call admission control** reroutes calls when the bandwidth allocation for WAN link is exceeded.

System Manager Web Services

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

- Domains

- Locations

- Adaptations

- SIP Entities

- Entity Links

- Time Ranges

- Routing Policies
- Dial Patterns
- Regular Expression data

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

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

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

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

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

Chapter 3: New in this release

The following sections describe the new features and enhancements for Avaya Aura® Session Manager Release 7.0.1.

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.

With Release 7.0.1,Session Manager has a Hunt Group Log in/Log out button, with which you can:

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

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

Session Manager and Avaya Aura® Device Services integration

Avaya Aura® Device Services overview

Avaya Aura® Device Services (AADS) provides a set of services to Avaya Aura® Communicator 3.0. AADS is co-resident with Session Manager 7.0.1. and is delivered as a separate OVA.

Session Manager and Avaya Aura® Device Services integration

The following services are provided when using AADS with Avaya Aura® Communicator 3.0:

- **Contact:** To use the Contact service, a user must be a provisioned user on LDAP Server. Using the contact service, you can:

  - Manage the contact detail from any device.

  - Perform an enterprise search of existing sources of contacts, such as, exchange local contacts, and enterprise directory that is also known as the Directory service.

  - Set and retrieve information, such as, preferred names, picture, and preferences. Using the Picture service, you can create and override, delete, and update the picture of a user. This also provides a centralized, firewall-friendly interface to include these picture urls in the contact information or search results.

- **Notification:** The Notification service provides a common infrastructure that allows a client or endpoint to subscribe to receive events from a number of service resources using a single connection.

- **Dynamic Configuration:** The Dynamic Configuration service provides discovery of configuration settings to UC Clients. You can customize these settings on a global, group, individual, or platform basis. The Dynamic Configuration service uses the automatic configuration feature of Avaya Communicator 3.0 to facilitate the configuration details to the UC clients. This helps the user to avoid manual configuration of their client. To log in to the client, the user needs to enter their credentials, such as, email address or Windows user id, along with their enterprise credentials.

  The Dynamic Configuration service is supported on the following Avaya Communicator Release 3.0 devices:

  - Avaya Communicator for Android

  - Avaya Communicator for iOS

  - Avaya Communicator for Mac

  - Avaya Communicator for Windows

- **Web Deployment:** The Web Deployment service publishes and deploys the UC client updates to the devices of the end users. The Web Deployment service is supported on the following devices of the Avaya Communicator Release 3.0:

  - Avaya Communicator for Mac

  - Avaya Communicator for Windows

Cassandra clustering and data replication overview

With Session Manager Release 7.0.1, if the **Enable Data Storage Cluster** field on the Session Manager Administration page is selected, Session Managers are added to the Cassandra database cluster. Each Cassandra is running in a cluster of 1 node and there are N clusters, where N is the number of Session Managers.

January 2016   Avaya Aura® Session Manager Overview and Specification   17
Comments on this document? infodev@avaya.com

The Cassandra nodes are configured to have a single cluster of Cassandra nodes. If the **Enable Data Storage Cluster** field is not selected, all the Cassandra nodes run in standalone mode.

Cassandra clustering is done only when Avaya Aura® Device Services (AADS) servers are configured and paired with Session Manager.

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

For administering Cassandra data distribution:

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

Add/remove skill button

Add/remove skill button

From Release 7.0.1, Personal Profile Manager (PPM) supports download of an assigned add/remove skill button on 96x1 SIP phone when the phone registers to Session Manager.

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

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

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

TLS mutual authentication for SIP endpoints

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

From Release 7.0.1, 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 cannot 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 Pre 7.0.1 Session Manager, it results to 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.

Capacity limits for Session Manager Footprints

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

 Note:

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

Session Manager Device Footprints	Up to 2.5K Devices	2.5K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices (R1 footprint)	10K to 23.5K Devices (R2 footprint) * see note
CPU Minimum	2300MHz, Hyper-threaded				
vCPUs	3	5	8	12	20
CPU MHz Reservation	3450	5750	9200	13800	23000
Memory Reservation	4GB	5GB	8GB	10GB	18GB

Table continues…

Session Manager Device Footprints	Up to 2.5K Devices	2.5K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices (R1 footprint)	10K to 23.5K Devices (R2 footprint) * see note
SIP Devices (Normal/Failure)	2.5K/3K	4.5K/5K	7K/8K	10K/12K	23.3K/ 25K
CC Agents (Normal/ Failure)	2K/2.5K	3.75K/4166	5.8K/6666	8333/10K	18K/21K
Presence Users (Normal/Failure)	2.5K/3K	4.5K/5K	7K/8K	10K/12K	18K/21K
Sessions (Sec/Hour/ Max)	25/90K/ 22.4K	45/162K/37.4K	70/256K/59.8K	100/360K/90K	150/540K/ 170K

✳ Note:

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

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

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

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

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

Chapter 4: 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 7.0 supports, see https://support.avaya.com/CompatibilityMatrix/Index.aspx on the Avaya Support website.

Support for third-Party SIP applications and devices

Session Manager can support direct SIP connections to SIP standard applications and devices. Support is based on the Avaya interoperability statement.

Avaya Aura® Platform Applications Interoperability Statement

While Avaya strongly recommends all third party integrations and vendors go through DevConnect Compliance Testing to ensure a higher level of comfort in the interoperability between DevConnect member products and Avaya solutions, we recognize that is not always the case.

If a third party product/integration is not tested under DevConnect, and a customer support ticket is raised to Avaya services via an authorized Avaya support channel, Avaya will troubleshoot the issue to the Avaya demarcation point with the third party vendor to the best of our ability. If no issue is found on the Avaya side, we will close the ticket and report to the customer that the issue needs to be worked with the third party vendor.

Chapter 5: Licensing requirements

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

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

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

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

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

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

✱ **Note:**

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

Backward compatibility and upgrade for licensing

There are two types of licensing:

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

For Licensing, the recommended upgrade order is:

1. Upgrade System Manager to Release 7.0.
2. Install Session Manager 7.0 license file on System Manager Release 7.0 WebLM.
3. Upgrade Session Manager to Release 7.0.

Table 1: Use Cases

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

Chapter 6: Performance and capacity specifications

Capacity and scalability specification

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

> ⚠️ **Important:**
>
> Assigning a SIP profile to an H.323 endpoint reduces the total SIP capacity by that many endpoints. See Alternative H.323 Endpoint administration considerations and impacts on page 28.

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

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

Table continues…

Entities	Numbers (supported limits)	Notes
		In both cases, the inter-Session Manager entity links need to be counted towards the limit.
SIP Entity Links / Session Manager	10,000	
Adaptations	25,000	Assuming one Adaptation for each SIP Entity. At the most, there can be one Adaptation for each SIP Entity and some SIP Entities may not require any Adaptation. SIP Adaptations are applied only on the non-Session Manager entities.
Adaptation Entries	250,000	Full system limit. Includes both ingress and egress entries.
Regular Expressions	100	
Routing Policies	25,000	Assuming one routing policy for each SIP Entity.
Time Ranges	1,000	
Locations	25,000	Takes into account the use of locations to control bandwidth.
Location IP Address Patterns	50,000	Used to identify if a given SIP endpoint is associated with the location. Based on the assumption that on an average two patterns are used to define a location.
Local Host Name Resolution Entries	25,000	Based on an average of one for each SIP Entity.
SIP Users	250,000	Total number of users.
Handles/User	3	
Total number of SIP handles	750,000	Average number of handles/user is 3 (total handles = 250,000 X 3)
Total SIP devices	350,000	Total number of devices.
Registered Devices/User	10	A SIP user/station can have more than one registered SIP device per user, such as an Avaya one-X® Communicator in Shared Control. Session Manager capacities are based on the number of active SIP devices. The number of registered devices per user is important to know to adequately distribute users and devices across Session Manager instances.
Average Buddy List/Contacts for each User	25	Assuming an average of 25 per user (maximum number of 250/ user).
Simultaneously Registered Devices/Session Manager	43,000	On the Common R2 servers. 21,500 Primary Registered Devices

Table continues…

Entities	Numbers (supported limits)	Notes
		21,500 Secondary Registered Devices Assuming 125,00 users but 150,000 SIP devices, each with a primary and secondary Session Manager registration for failure recovery distributed across Session Managers in the configuration. A total of 150,000 primary and 150,000 secondary registrations distributed across an N+1 sparing model configuration of 7 Session Managers would be approximately 21,500 primary and 21,500 secondary registrations per Session Manager.
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	18,000 (normal conditions) 21,000 (failure conditions)	Call Center (CC) Agent SIP devices consume more resources per Session Manager. 18,000 is the maximum for CC Agent SIP devices, assuming all devices are CC agents. When configuring for systems that may support fewer CC Agents, assume that five CC Agent devices are the equivalent of six regular SIP devices.
Presence users	18,000 (normal conditions) 21,000 (temporarily during failure conditions)	
Digit Conversion Patterns (ingress)	45,000	
Digit Conversion Patterns (egress)	45,000	
Users/ Session Manager on VMware		See *Deploying Avaya Aura® Session Manager* on the Avaya support website.
Branch Session Manager instances	250	

Table continues…

Entities	Numbers (supported limits)	Notes
Per Branch Session Manager performance • Devices/survivable embedded • Devices/survivable	• 700 • 2,000	
Busy Hour Sessions/ Session Manager	540,000	The type of call determines the number of SIP sessions. An SRE call is a single session, so Busy-Hour Session is equivalent to BHCC. Conversely, a SIP station-to-SIP station call creates three sessions, and the BHCC is calculated accordingly.
Session creations/second/ Session Manager	150	
Session creations /second/ Branch Session Manager	10	
Session creations/ second / survivable embedded Session Manager	3	
Simultaneous sessions/ Session Manager	160,000	

Alternative H.323 Endpoint administration considerations and impacts

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

• System Manager to create an H.323 endpoint without a SIP profile.

• The Communication Manager SAT.

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

Alternative method for administering H.323 endpoints

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

The alternative method:

• Simplifies Session Manager routing configuration.

• Provides Dual Registration (H.323 and SIP endpoints on the same extension) with no further System Manager configuration.

• Provides an easy migration to a SIP endpoint by changing the endpoint type and removing the H.323 station.

Use Case

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

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

Impact on capacities

🛈 **Important:**

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

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

Dial plan specification

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

- A global enterprise-wide numbering plan used for centralized routing that is administered on a centralized management console.

- One or more local, geographically significant dial plans administer on Communication Manager, or other vendor PBX. Local dial plans specify the actual digits dialed within the constraints of the numbering plan.

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

The numbering plan describes the overall numbering scheme that the enterprise uses for centralized routing. Session Manager uses two different numbering plans for analysis and routing:
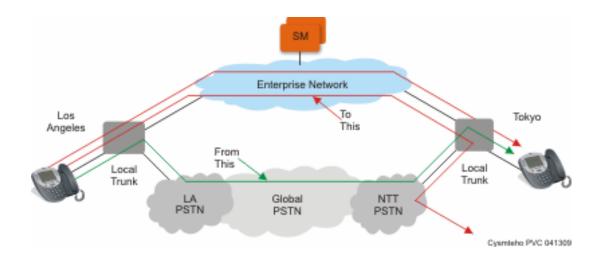
- E.164 Public Numbering Plan

- Enterprise Canonical (Private Numbering Plan)

Tail end hop off

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

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

The following figure illustrates how TEHO works:

Call Admission Control specification

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

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

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

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

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

Redundancy and high availability

An enterprise supports up to 28 Session Manager instances. You can implement the Session Manager instances in the same data center or in data centers that are separated geographically around the world. These instances do not need to exist on the same subnet.
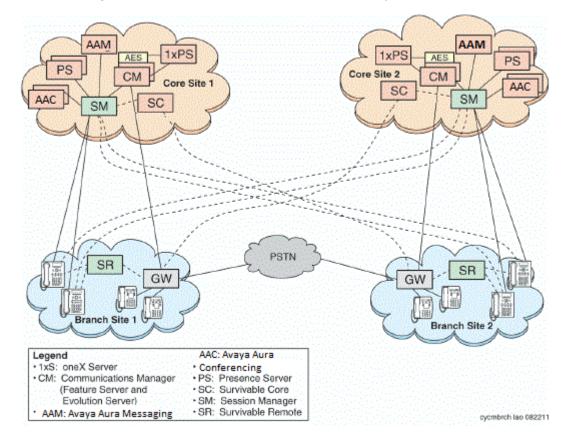
Session Manager redundancy supports networks with round trip delays of less than one second.

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

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

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

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

> **⊛ Note:**
>
> The Session Manager Release 7.0 does not support High Availability for call journaling because the primary Session Manager stores the call logs.

Survivable Core

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

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

Survivable Remote

Survivable Remote sites include a Survivable Remote Session Manager and Survivable Remote Communication Manager that is either a Feature Server or an Evolution Server, depending on the main Communication Manager to which it is connected. SIP phones simultaneously register to the main Session Manager, a backup main Session Manager, and the Survivable Remote Session Manager. During a WAN outage that removes the communication path between phones and the associated Session Manager, the phones failover to the Survivable Remote Session Manager and the Survivable Remote Communication Manager.

Chapter 7: 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 8: Resources

Documentation

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

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

Title	Description	Audience
Overview		
Avaya Aura® Session Manager Overview and Specification	Describes the key features of Session Manager.	IT management System administrators
Avaya Aura® Virtualized Environment Solution Description	Describes the Avaya Virtualized Environment, design considerations, topology, and resources requirements.	Sales engineers Implementation engineers Support personnel
Avaya Aura® Session Manager Security Design	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Avaya Aura® Session Manager 7.0.1 Release Notes	Contains enhancements, fixes, and workarounds for the Session Manager 7.0.1 release.	System administrators Services and support personnel
Implementation		
Deploying Avaya Aura® applications from System Manager	Describes how to deploy the Avaya Aura® virtual applications using the System Manager Solution Deployment Manager.	Services and support personnel
Deploying Avaya Aura® Session Manager	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Describes how to install and configure Branch Session Manager in a virtualized environment.	Services and support personnel
Routing Web Service API Programming Reference	Describes how to use the System Manager Routing Web Service API for Session Manager.	Services and support personnel

Table continues…

Comments on this document? infodev@avaya.com

Title	Description	Audience
Upgrading and Migrating Avaya Aura® applications to Release 7.0.1 from System Manager	Describes how to upgrade and migrate the Avaya Aura® virtual applications using System Manager Solution Deployment Manager.	Services and support personnel
Using		
Using the Solution Deployment Manager client	Deploy and install patches for Avaya Aura applications.	System administrators
Administration		
Administering Avaya Aura® Session Manager	Describes the procedures to administer Session Manager using System Manager.	System administrators
Administering Avaya Aura® Communication Manager Server Options	Describes the procedures to administer Communication Manager as a feature server or an evolution server. Provides information related to Session Manager administration.	System administrators
Avaya Aura® Session Manager Case Studies	Provides common administration scenarios.	System administrators
Installation and upgrades		
Installing the Dell™ PowerEdge™ R610 Server	Describes the installation procedures for the Dell™ PowerEdge™ R610 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R620 Server	Describes the installation procedures for the Dell™ PowerEdge™ R620 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R630 Server	Describes the installation procedures for the Dell™ PowerEdge™ R630 server.	Services and support personnel
Installing the HP ProLiant DL360 G7 Server	Describes the installation procedures for the HP ProLiant DL360 G7 server.	Services and support personnel
Installing the HP ProLiant DL380p G8 Server	Describes the installation procedures for the HP ProLiant DL380p G8 server.	Services and support personnel
Installing the HP ProLiant DL360 G9 Server	Describes the installation procedures for the HP ProLiant DL360 G9 server.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade Session Manager to the latest software release.	Services and support personnel
Migrating and Installing Avaya Appliance Virtualization Platform	Describes the migration and installation procedures for Appliance Virtualization Platform.	Services and support personnel
Using the Solution Deployment Manager client	Describes the patch deployment and installation procedure for Avaya Aura® applications.	Services and support personnel
Maintaining and Troubleshooting		
Maintaining Avaya Aura® Session Manager	Contains the procedures for maintaining Session Manager.	Services and support personnel

Table continues…

Title	Description	Audience
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

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.

2. At the top of the screen, enter your username and password and click **Login**.

3. Put your cursor over **Support by Product**.

4. Click **Documents**.

5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.

6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.

7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.

8. Click **Enter**.

Training

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

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

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

Table continues…

Course code	Course title
5U00081V	Session Manager Administration
5U00082I	Session Manager and System Manager Administration
5U00082R	Session Manager and System Manager Administration
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support
5U00095V	System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00097I	Avaya Aura® Session and System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00105W	Avaya Aura® Session Manager Overview
ATC01840OEN	Survivable Remote Session Manager Administration
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
2011V	What is new in Avaya Aura® System Manager 7.0 and Avaya Aura® Session Manager 7.0

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:

  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.

  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:

  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.

  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

> **Note:**
>
> Videos are not available for all products.

Support

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

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

Index

W

web services
System Manager ....