Avaya Aura® Session Manager Overview and Specification

Release 6.3
Issue 3
October 2013

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

Avaya grants you a license within the scope of the license types described below, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Concurrent User License

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that 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”). 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 Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Virtualization

Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Avaya channel partner would like to install two of the same type of vAppliances, then two vAppliances of that type must be ordered.

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: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura® are registered trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

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

Intended audience

This document is intended for people who want to gain a high-level understanding of the product features, functions, capacities, and limitations.

Document changes since last issue

The following changes have been made to this document since the last issue:

- Updated the topic *New in this release* in the chapter *Session Manager overview*.
- Updated the topic *Supported Avaya servers* in the chapter *Interoperability*.
- Updated the topic *Capacity and scalability specification* in the chapter *Performance specifications*.

Related resources

Documentation

See the following related documents.

Title	Use this document to:	Audience
Overview		
Security Design for Avaya Aura® Session Manager	Make Session Manager secure on the network.	Network administrators, services and support personnel
Avaya Aura® Session Manager Overview and Specification	Understand the product overview and feature descriptions.	IT management
Implementation		
Deploying Avaya Aura® Session Manager	Install and complete initial administration of Session Manager	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Install and complete initial administration of Branch Session Manager.	Services and support personnel
Implementing Avaya Aura® Communication Manager	Install the appropriate Communication Manager template, including Branch Session Manager, on the server.	Services and support personnel
Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide	Install, configure, complete initial administration and troubleshoot Session Manager on VMware.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Upgrade Session Manager to a new software release.	Services and support personnel
Installing Service Packs For Avaya Aura® Session Manager	Install service packs on Session Manager.	Services and support personnel
Installing Patches For Avaya Aura® Session Manager	Install patches on Session Manager.	Services and support personnel
Installing the Avaya S8800 Server for Avaya Aura® Communication Manager	Install the S8800 server in the rack.	Services and support personnel
Installing the Avaya S8510 Server Family and Its Components	Install the S8510 server in the rack.	Services and support personnel
Installing the Dell™ PowerEdge™ R610 Server	Install the Dell™ PowerEdge™ R610 server in the rack.	Services and support personnel
Installing the Dell™ PowerEdge™ R620 Server	Install the Dell™ PowerEdge™ R620 server in the rack.	Services and support personnel
Installing the HP ProLiant DL360 G7 Server	Install the HP ProLiant DL360 G7 server in the rack.	Services and support personnel

Title	Use this document to:	Audience
Installing the HP ProLiant DL360p G8 Server	Install the HP ProLiant DL360p G8 server in the rack.	Services and support personnel
Maintenance and Troubleshooting		
Maintaining and Troubleshooting Avaya Aura® Session Manager	Troubleshoot Session Manager, resolve alarms, and replace hardware. Also contains alarm codes and event ID descriptions.	Services and support personnel
Administration		
Administering Avaya Aura® Session Manager	Administer Session Manager using System Manager.	System administrators
Administering Avaya Aura® Communication Manager Server Options	Administer Communication Manager as a feature server or evolution server. Describes the associated Session Manager administration.	System administrators
Avaya Aura® Session Manager Case Studies	Provides case studies that walk users through common administration scenarios.	System administrators

Training

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

Course code	Course title
5U00104W	Session Manager 6.2 Delta Overview
5U00105W	Avaya Aura® Session Manager Overview
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
ATC01840OEN	Survivable Remote Session Manager Administration

Avaya Mentor videos

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

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

To find videos on the Avaya support site, select the product name, and check the *videos* checkbox to see a list of available videos.

Note:

Videos are not available for all products.

To find the Avaya Mentor videos on YouTube, go to http://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 site.

Support

Visit 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.

Warranty

Avaya provides a 90-day limited warranty on Session Manager. See the sales agreement or other applicable documentation for more information about the terms of the limited warranty. In addition, see the standard warranty and details about Session Manager support during the warranty period on the Avaya Support website at https://support.avaya.com under **Help & Policies> Policies & Legal > Maintenance and Warranty Information**. See also **Help & Policies > Policies & Legal > License Terms**.

Chapter 2: Session Manager overview

Session Manager is a SIP routing and integration tool. Session Manager integrates all SIP devices across the entire enterprise network within a company and leverages the existing PBX infrastructure. Session Manager provides the following advantages:

- Business agility driven through holistic enterprise architectures for connecting users, applications, and multivendor solutions.
- New cost savings from SIP connectivity and reduced public switched telephone network (PSTN) usage through centralized, enterprise-wide routing.
- Lower total cost of ownership with a centralized, easy-to-use management interface and the efficient deployment of enterprise-wide central applications.
- Unprecedented enterprise-wide scalability with support for truly global deployments.
- Strong reliability, security, and redundancy support.

Feature description

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

Specifically, Session Manager:

- Normalizes disparate networks— integrates with third-party equipment and endpoints.
- Provides centralized routing of calls using an enterprise wide numbering plan.
- Offers centralized management through System Manager, including configuration of user profiles and efficient deployment of enterprise-wide centralized applications.
- Communicates with Session Border Controller and provides protection at the edge of the enterprise network.
- Interconnects Communication Manager and Avaya Communication Server 1000 and provides multiple feature support for SIP and non-SIP endpoints.
- Enables third-party E911 emergency call service for enterprise users.
- Centralizes Presence Services, providing scale and reduced network complexity with a variety of endpoints and communication servers.
- Supports truly converged voice and video bandwidth management.

- Provides application sequencing capability, thus enabling incremental application deployments without PBX upgrades.
- Provides outstanding geographic redundancy.

Policy-based routing

Customers can define their call routing policy with Session Manager. Using these policies, they can control 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, chooses the lowest cost route from a list of service providers on a time-of-day or time-of-week basis. This results in cost savings for the enterprise.
- 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 to a SIP entity to multiple IP addresses. You can administer Session Manager to select from multiple IP addresses for a given entity and select these hosts based on administered priorities and weights.
- Call admission control reroutes calls when the WAN link to a branch fills up.

Centralized applications

Session Manager provides connectivity for centralized Avaya applications such as Avaya Aura® Messaging, Avaya Voice Portal, 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.

SIP Proxy and Registrar functionality

Session Manager functions as the SIP Proxy and Registrar server of the enterprise network.

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.

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 and can deny, modify, or forward initial SIP requests. The following are some examples of sequenced applications:

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

Session Manager also supports third-party PBX endpoint application sequencing. Typical applications include blocking calls based on user preferences, directing calls to users when they move across the Avaya Aura® enterprise, and augmenting caller identification information for incoming and outgoing calls. You can enable Application Sequencing without upgrading or modifying the code on existing third-party PBX equipment. See *Administering Avaya Aura® Session Manager* for details.

Personal Profile Manager

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, to add or update contacts, and to save device-specific data. With PPM, endpoints can attach to the network to download profile data and store data back in the network for easy access across multiple user devices.

Centralized SIP trunking

Centralized SIP trunking routes all network traffic, including branch site traffic, through the enterprise core site. In this approach, Session Manager provides redundant connections to a SIP service provider using the Gateway or SBC. Centralized SIP trunking enables enterprises 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.

New in this release

Define number ranges in Session Manager Dial-plan:

In this release, Session Manager provides an enhanced Dial-plan administration feature. You can specify number ranges in the Session Manager Dial-plan to account for DID numbers that are not in blocks of 10, 100, or 1000.

You can enter a range that is a subset or superset of an existing range or pattern. The smaller range is called a sub-range. Sub-ranges have the following limitations within the same location and domain:

Example

If the specified range is 5000:5499, you can specify the sub-ranges as:

- 5002:5011
- 5000:5499 and 5492:5499, where the end of sub-range and range match.
- 5000 (single entry) and 5000:5009, where the beginning of sub-range and range match.

The subrange 5300:5555 is not valid because the sub-range crosses the end of the range.

To enable the Dial Plan Range feature in an enterprise system, all Session Manager installations need to be of version 6.3.4 and later.

For more information about the Dial Plan Range feature, see *Administering Avaya Aura® Session Manager Release 6.3*.

Session Manager Firewall rule administration and maintenance enhancement:

As of Session Manager Release 6.2.1, the Session Manager SIP Firewall is enabled by default for all new installations. With Session Manager 6.3.4, there are several enhancements related to the administration and management of the Firewall rules.

In this release, Session Manager SIP Firewall provides the following enhancements:

- Simplify on-going maintenance of rule sets and rule settings, including automatic upgrade of default settings.
- Create named SIP Firewall rule sets specific to the Session Manager system.

- View the status of SIP Firewalls across all Session Manager systems, including the specific rule set that is deployed to each Session Manager and Branch Session Manager in the network.
- View SIP Firewall rule match counts for all Session Manager systems in the network.

Session Manager also runs a periodic audit to ensure that SIP Firewall is in a healthy and functioning state. Based on this audit, Session Manager

- retrieves the state of the SIP Firewall (for example, empty, loading, running).
- resets the rule set to the default rule set and generates an event under the following conditions:
  - If the SIP Firewall Rule Set is found to be in the not assigned state (empty state).
  - If the SIP Firewall Rule Set has been in a loading state for more than five minutes (or for a complete maintenance cycle).

For more information about the Firewall Administration feature, see *Administering Avaya Aura® Session Manager Release 6.3*.

Flexible Footprint for Session Managers on VMware:

In this release, Session Manager offers a flexible footprint for a server configuration, based on the specific number of users supported for the customer implementation.

You can re-configure a Session Manager instance running on VMware to support one of the following user capacities:

- Up to 500 SIP users on a sunny day and up to 1000 users on a rainy day
- Up to 1000 SIP users on a sunny day and up to 2000 users on a rainy day
- Up to 2400 SIP users on a sunny day and up to 3000 users on a rainy day
- Up to 3500 SIP users on a sunny day and up to 4000 users on a rainy day
- Up to 4500 SIP users on a sunny day and up to 5000 users on a rainy day
- Up to 7000 SIP users on a sunny day and up to 8000 users on a rainy day
- Up to 10000 SIP users on a sunny day and up to 12000 users on a rainy day

For more information about reconfiguring hardware resources for different user footprints, see *Session Manager using VMware® in the Virtualized Environment Deployment Guide*.

Session Manager CDR enhancements:

Session Manager now generates Call Detail Recording (CDR) records for station to station calls, for reporting and billing. This is in addition to current trunk call CDR capabilities.

Session Manager provides the following CDR data file formats:

- The existing Session Manager 6.3 CDR flat file format

This format continues without any changes and allows customers to use their existing Session Manager CDR adjuncts without changes or updates.

- The new Session Manager 6.3.4 CDR flat file format

  This format adds new data on the existing Session Manager 6.3.2 format. The most notable additions are as follows:

  - user to user (formally called as station to station) calls
  - incomplete calls
  - Tenant ID (where applicable)

- The new Session Manager 6.3.4 XML format

  This new CDR format provides enhanced call records and enables CDR adjuncts to easily adopt any future changes in the CDR formats.

For more information about Call Detail Recording, see *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Session Manager support for Avaya SBCE Remote Worker feature:

In this release, Session Manager supports the SBCE Remote Worker capability.

Using this feature, a remote endpoint can register and securely communicate with a Session Manager in the core. In previous releases, in order to support the remote workers who were using the Avaya SBCE, you needed to enable PPM connection limiting. In this release, this restriction is removed, providing increased scale and security.

For the Remote Worker configuration, Session Manager supports the following SIP endpoints:

- 96x1
- Avaya one-X® Communicator SIP
- Avaya one-X® Mobile SIP
- Flare Experience
- ADVD
- B179 Conference Phone
- VDI Communicator

For more information about the Remote Worker feature, see *Administering Avaya Aura® Session Manager Release 6.3*.

Pluggable SIP Adaptation Modules:

In SIP network configurations involving different elements, one of the major problems is interoperability among different SIP elements. The inherent flexibility of the SIP protocol leads to different SIP dialects and inconsistent implementations. To solve this key problem, Session

Manager provides a capability, called SIP Adaptation Modules, to selectively modify signaling messages, based on the interfacing SIP entity. Session Manager provides a number of adaptation modules to meet the broader and general inconsistencies or nuances of particular SIP elements.

These modules are also referred as the *system Adaptation Modules*, because these modules are packaged within the Session Manager software releases.

With Session Manager 6.3.4, Avaya has opened this interface so that Avaya Professional Services (APS) can develop adaptation modules.

Using this capability:

- APS can build custom adaptation modules to meet specific customer needs.
- Avaya can release these adaptation modules, independent of standard Session Manager software release cycles.

Inter Tenant Communication Control:

Using the Inter Tenant Communication Control (ITCC) feature, customers can share the Avaya Aura® infrastructure across multiple user communities to reduce people, capital and operating costs. In a single Avaya Aura® infrastructure, ITCC provides segmented *virtual* systems to specific user communities. With ITCC, the system places restrictions on the communication between the segmented communities or, across *tenant* boundaries. The ITCC feature allows the user-to-user calls within the tenant boundaries. Any call targeted by a user to another user who is part of another tenant or to an external number, needs to be routed through a carrier SIP element. The system uses the user-to-Session Manager routing logic to route requests across tenant boundaries. This procedure of routing the requests also applies to other non-SIP methods that are routed based on the contents of the R-URI.

In addition to the routing requirements, the ITCC feature places restrictions on Contact Management.

In Session Manager, there are two types of contacts. An enterprise contact, also called internal contact, and a private contact, also called external contact.

- When performing a search operation, a search request returns only the contacts that belong to the same tenant partition (as that of requesting user).
- When performing the add contact operation, only contacts within the same tenant partitions are stored as internal contacts.
- A contact from a different tenant partition is stored as an external contact.

In Presences Services, the users in different tenants cannot see the presence of other tenant users and cannot send IM messages unless they are added as external contacts.

Chapter 3: Interoperability

Product compatibility

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

Supported Avaya endpoints

Session Manager 6.3 supports the following Avaya endpoints:

Endpoints	Notes
9600 Series IP Deskphones with Deskphone SIP 2.6.6, 6.0, 6.1, or 6.2. Specifically: • 9620, 9620C, 9620L, 9630, 9630G, 9640, 9640G, 9650, 9650C with Deskphone SIP 2.6.6, 2.6.10 • 9601, 9608, 9611, 9621, 9641 with Deskphone SIP 6.2.2	
96x1 Series SIP endpoints (9608SIP, 9611SIP, 9621SIP, 9641SIP, 9611SIPCC, 9608SIPCC, 9621SIPCC, 9641SIPCC) – fw 6.3	
Call Center Agent endpoints (9621 and 9641 with custom faceplates) - 6.2, and one-X Agent (6.2.2)	
ADVD	Administered as a 9640SIP phone, with 1.1.2
Flare Communicator Windows 1.0	
Flare Experience Windows 1.0 and 1.1	
Flare Communicator iPad 1.0	
Flare Experience iPad 1.0 and 1.1	
VDI Communicator 1.0	Supported as an endpoint controlled by one-X

	Communicator 6.1.7 as a SIP client in shared control mode
one-X Communicator 6.1 for Windows	For CS1000 7.5 and Session Manager. Supports all three audio modes. One-X communicator does not support Session Manager prior to Session Manager 6.0.
one-X Communicator for MacOS 1.0.4	SIP only and does not support CES. Supports all three audio modes. One-X communicator does not support Session Manager prior to Session Manager 6.0.
One-X Mobile iOS SIP Client – 6.2 (or later)	This version does not support the Multi Device Access (MDA) feature.
11xx and 12xx SIP endpoints.	Treated as 3rd party endpoints. PPM cannot download data to these endpoints.
Radvision SIP endpoints: XT1000, XT1000 Piccolo, XT1200, XT4000, XT5000	Treated as 3rd party endpoints. PPM cannot download data to these endpoints.
Konftel	Treated as 3rd party endpoints. PPM cannot download data to these endpoints.
1603SW-I SIP endpoint, such as Blaze	
Avaya 10x0 video endpoints (such as Lifesize, aliased as 96x0SIP) as follows: • 1010/20: AV_PP1_4_7_3_5.cmg • 1030/40/50: AV_RM1_4_7_3_5.cmg	
46xx endpoints	

Note:

1. UniSTIM is a non-SIP endpoint that is supported as part of the overall Avaya Aura® solution. UniSTIM endpoints do not register with Session Manager but register to a CS1000.
2. Previous endpoint releases that are supported are listed as follows:
   - one-X Communicator® version 6.0 supports Session Manager 6.0.

- one-X Communicator® version 6.1 supports Session Manager 6.0 and Session Manager 6.1.
- one-X Communicator® version 6.2 supports Session Manager 6.1 and Session Manager 6.2.
- Flare Communicator 1.0 supports Session Manager 6.1 and Session Manager 6.2
- Flare Experience 1.0 supports Session Manager 6.2 (requires Session Manager 6.2 and AAC 7.0)

3. Older SIP endpoints does not support all features in release 6.3, but can still register to Session Manager (for example, 46xx).

Deployment options

Session Manager can be deployed under the following environments in an enterprise.

Avaya supported hardware for large enterprises

A large enterprise can have upto 10 Session Manager instances supporting 1,00,00 users.

Hardware

The supported servers for Session Manager 6.3 are:

- S8800, S8510 (upgrades only), HP DL360PG8, HP DL360G7, Dell R620 and Dell R610 for Session Manager as a appliance.
- S8800, S8510, HP DL360PG8, HP DL360G7, Dell R620 and Dell R610 servers and S8300D for Survivable Remote.

For a list of components and specifications for these servers, see *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

VMware virtualized environment

Existing customers who have a VMware IT infrastructure can deploy Session Manager as a virtual application on VMware.

Session Manager on VMware is capable of supporting the following user capacities:

1. Capacity footprint 1 - 500 users under normal conditions and 1,000 users under failure conditions.
2. Capacity footprint 2 - 1,000 users under normal conditions and 2,000 users under failure conditions.
3. Capacity footprint 3 - 2,400 users under normal conditions and 3,000 users under failure conditions.
4. Capacity footprint 4- 3,500 users under normal conditions and 4,000 users under failure conditions.

5. Capacity footprint 5- 4,500 users under normal conditions and 5,000 users under failure conditions.
6. Capacity footprint 6- 7,000 users under normal conditions and 8,000 users under failure conditions.
7. Capacity footprint 7- 10,000 users under normal conditions and 12,000 users under failure conditions.

Hardware

The customer provides the servers and the VMware infrastructure including the VMware licenses. For details on Session Manager in a VMware® vSphere ™ 5.1 virtualization environment, see the *Session Manager using VMware® in the Virtualized Environment Deployment Guide* available on the support site.

System Platform for midsize enterprise

Avaya Aura® solution, that includes Session Manager as an application, is installed as a System Platform template on a single server. Midsize Enterprise supports enterprises with 250 - 2400 users, 1 to 5 locations.

Hardware

The HP ProLiant DL360 G7 is the only supported server for Midsize Enterprise 6.2.2. For details on Mid-size Enterprise Session Manager, see the *Avaya Aura® Solution for Midsize Enterprise documentation*, available on the support site.

Operating System compatibility

Session Manager 6.3 and Branch Session Manager 6.3 support Red Hat Enterprise Linux (RHEL) 6.2. The underlying SIP container is IBM WAS 8.0.x server.

The Branch Session Manager 6.3 and Midsize Enterprise Solution 6.3 templates include RHEL 6.2 as the underlying operating system for the Branch Session Manager and the Session Manager components running on an Avaya Aura® Midsize Enterprise Solution.

Third-Party PBX Integration

Session Manager works with Cisco UCM, Siemens Highpath, Alcatel Lucent OmniPBX, and Aastra systems with direct SIP connections. You can program each of these third-party PBXs so that Session Manager can perform inter-PBX routing.

Chapter 4: Performance specifications

Capacity and scalability specification

Entities	*Numbers (supported limits)*	*Notes*
Core Avaya Aura® Session Manager (SM) instances	10	
Dial Patterns * Locations/ Pattern * Routing Policies	300,000	Assuming 20 telephone numbers for each SIP Entity. The number can be interpreted as only 300,000 individual phone numbers can be routed, but these are patterns. If the numbers can be grouped for a given destination, fewer entries are required.
SIP Domains	1,000	
SIP Entities	25,000	
SIP Entity Links	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. In both cases, the inter-Session Manager entity links need to be counted towards the limit.
SIP Entity Links / SM	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 Entity may not require any Adaptation.
Adaptation Entries	250,000	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.
User Records	100,000	
Registered Devices/User	1	
Handles/User	3	
Buddy List/Contacts for each User	20	Assuming an average of 20 per user (max of 250).
Simultaneously Registered Stations/SM	20,000	
Simultaneously Subscribed Stations/SM • If Presence implemented • No. of CC Agents/SM	11,111 (under normal condition) and 12,000 (under failure condition) • 12,000 • 10,000	Assuming 100,000 users with an average of one logged in phone per user = 100,000 endpoints. Each endpoint is registered to two Session Managers. The endpoints are spread evenly over a network of 10 Session Manager instances. Hence 200,000 registrations are spread over 10 SM instances = 20,000 registrations per Session Manager. **Note:** 1. Avaya one-X® Communicator Shared Control consumes more than one registration per subscription, but not double. 2. A user with more than one registered device consumes one registration per subscription for each device. Thus, if 200 users are registered with 3 devices, then the consumption is 600 towards the limit of 20,000.
Simultaneously Registered Stations/User (Communication Profile)	10	

Users/SM on VMware		See *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* on the Avaya support site.
SM Communication Profiles (Users)	100,000	The number will be less if users have Presence.
SM Communication Profiles/SM	12,000	Same as Simultaneous Subscribed Stations/ SM.
Maximum no. of Primary Users/SM	10,000 12,000 (under failure condition)	
System Manager administrators	250	
System Manager Simultaneously Active Sessions	50	
Branch SM instances	250	
Per Branch SM performance • Users/survivable embedded • User/survivable	• 700 • 2,000	
BHCC / SM	360,000	
Session creations/second/ SM	100	
Session creations / second/ BSM	10	
Session creations/ second /survivable embedded SM	3	
Simultaneous sessions/SM	90,000	

For details about the listed entities, see *Administering Avaya Aura® Session Manager Release 6.3*.

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 Avaya Aura 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:

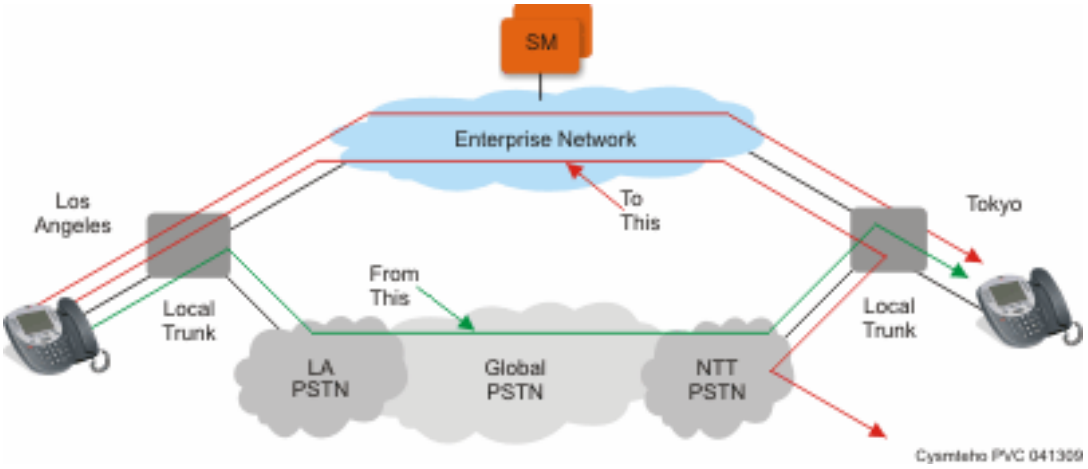
- E.164 Public Numbering Plan
- Enterprise Canonical (Private Numbering Plan)

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 truly 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 with an option to allow voice to use bandwidth from unused video allocations when network conditions require. Session Managerr intercepts every SIP request for service, examines the SIP messages 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 *downspeed-able* video bandwidth by location to insure a level of video quality.

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

Redundancy and high availability

Session Manager provides redundancy by supporting up to 10 Session Manager instances in an enterprise. You can implement the Session Manager instances in the same data center or

in data centers that are separated geographically, even around the world. These instances need not exist on the same subnet.

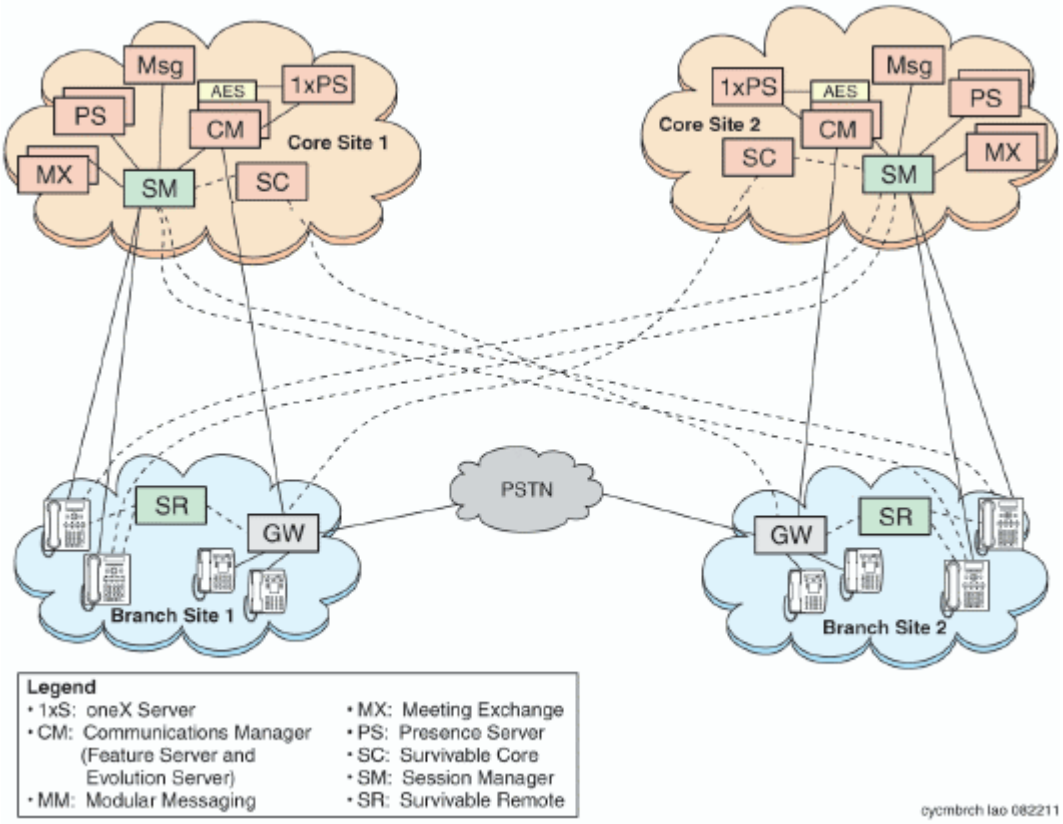
Session Manager redundancy supports networks with round trip delays of less than one second.

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 means that:

- A failure of one of the Session Manager instances does not interrupt service.
- A System Manager can be used to administer all the Session Managers.
- The centralized dial plan governs Avaya and third party PBXs and enables them to connect using SIP (either directly or using a SIP gateway) to one of the Session Manager instances.
- When SIP endpoints register simultaneously with two Session Managers at the core and with one Branch Session Manager, the SIP endpoints continue to be operational if any one of the associated Session Managers fails.

The following figure illustrates solution-level survivability in the enterprise:



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 (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 5: Security

Security specification

Since 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 thereby protecting customers from toll fraud and other malicious attacks.

Session Manager runs on the RHEL Linux operating system which is hardened to provide only those functions necessary for securing mission 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.

Hence, 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.

Port utilization

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

Chapter 6: Licensing requirements

The Licensing feature for both core and branch Session Manager uses:

- Product Licensing and Delivery System (PLDS) for the order-to-license function, including license entitlement management, license activation, and license file delivery.
- Web License Manager (WebLM) for the product-side license management function, including use of WebLM server, or to manage the license file.

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 number of users administered and the number of Session Manager instances administered is licensed.

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

- Purchase additional Session licenses from Avaya.
- Analyze the Session 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) prior to applying any license enforcement.

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.
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.
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).
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

T

V

W