Avaya Aura® System Manager Overview and Specification

Release 10.2.x
Issue 9
March 2026

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

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

This document is intended for anyone who wants to gain a high-level understanding of System Manager features, functions, capacities, and limitations within the context of solutions and verified reference configurations.

Changes to platform support

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

Discontinued Platforms:

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

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

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

Change history

Issue	Date	Summary of changes
9	March 2026	Added the section: Changes to platform support on page 6
8	February 2026	Updated the following sections: • Supported servers on page 21 • Virtualized Environment overview on page 39
7	December 2025	Added the following section for Release 10.2.1.3: • New in System Manager Release 10.2.1.3 on page 10
6	May 2025	Updated the following section: • Topology on page 40
5	April 2025	Added the following sections for Release 10.2.1.1: • New in System Manager Release 10.2.1.1 on page 10 • Certificate revocation list overview on page 54
4	December 2024	Added the following section for Release 10.2.1: • New in System Manager Release 10.2.1 on page 11
3	May 2024	Updated Software-only environment overview on page 43.
2	April 2024	Updated Avaya Aura applications deployment offers on page 39.
1	December 2023	Initial issue of Release 10.2 document.

Chapter 2: System Manager overview

Avaya Aura® System Manager is a central management system that provides a set of shared management services and a common console. All shared and element-specific management for Avaya Aura® applications that System Manager supports is performed from the common console. System Manager provides the following key capabilities:

- Centralized software management solution to support deployments, migrations, upgrades, and updates to the suite of Avaya Aura® applications.
- Avoid duplicate data entry through shared management services.
- Centralized access to all Avaya Aura® applications through a browser-based management console with single sign on.
- Optimization of IT skill sets with consistency of management functions across Avaya solutions.
- Integration with enterprise IT infrastructure, such as identity management, authentication, authorization, security, and enterprise directory

System Manager feature matrix

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

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x	Release 10.2.x
OVA signing	Y	Y	Y	Y	Y
IPv6 support	Y	Y	Y	Y	Y
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y	Y
Compliance with DISA security STIGs	Y	Y	Y	Y (R 10.1.0.2 onwards)	Y
Extended Security Hardening	Y	Y	Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x	Release 10.2.x
Support for TLS 1.2	Y	Y	Y	Y	Y
Customer Root Access		Y	Y	Y	Y
Preserve security hardening modes on upgrade		Y	Y	Y	Y
Extended host name validation		Y	Y	Y	Y
Support for 16-digit extension		Y	Y	Y	Y
Product Initiated Registration		Y	Y	Y	Y
Support for Software-only deployment		Y	Y	Y	Y
Support for deployment on Cloud Services	Y	Y	Y	Y	Y
Support for Geographic Redundancy in mixed deployment environment		Y	Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance		Y	Y	Y	
Support for Avaya Solutions Platform 130 Appliance		Y	Y	Y	Y
Support for Data Encryption			Y	Y	Y
Support for encrypted backup and restore			Y	Y	Y
Support for log file retention period management			Y	Y	Y
Support for the Avaya Subscription license			Y	Y	Y
Support for VMware ESXi 7.0			Y	Y	Y
Support for J-Series phone migration			Y	Y	Y
SCEP Enrollment Enhancement to improve Certificate Management for endpoints			Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x	Release 10.2.x
Emergency Location Management Solution			Y	Y	Y
Support for TLS 1.3				Y	Y
Support for Red Hat Enterprise Linux (RHEL) 8.4				Y	Y
Support for Red Hat Enterprise Linux (RHEL) 8.10					Y (10.2.1 onwards)
Support for VMware ESXi 8.0					Y
Support for HTTP proxy					Y (10.2.1.1 onwards)

New in this Release

New in System Manager Release 10.2.1.3

External Admin Connect Properties

From Release 10.2.1.3, the new section **External Admin Connect Properties** is added to configure the System Manager with Avaya Infinity™ server.

For more information on Avaya Infinity™, refer to Avaya.

New in System Manager Release 10.2.1.1

Avaya Aura® System Manager Release 10.2.1.1 supports the following new feature and enhancements:

HTTP proxy support for CRL download

From release 10.2.1.1 and later, Avaya Aura® supports HTTP proxy to download Certificate revocation lists (CRL). CRL download using a proxy eliminates the requirement for a direct connection to the Certificate Authority (CA), which can be a security risk.

This release supports the HTTP proxy type with basic authentication, which requires a username and password. Alternatively, customers can configure proxy support without authentication.

Customers can configure the frequency with which Avaya Aura® checks for updates to CRLs and downloads a new CRL. To enable this functionality, customers can configure a CRL download job.

System Manager and Session Manager use these configuration settings in tandem. So, it is important to understand the implications of these settings for Session Manager. For more

information, see *Administering Avaya Aura® System Manager* and *Administering Avaya Aura® Session Manager*.

New in System Manager Release 10.2.1

Avaya Aura® System Manager Release 10.2.1 supports the following new features and enhancements:

System Manager data integrity protection

- Protection of System Manager database during synchronization: From Release 10.2.1, an error message displays, and synchronization stops if there is a risk of deleting System Manager station data. In previous releases, an incremental synchronization was switched to an initializing synchronization for an upgraded System Manager or Communication Manager. In 10.2.1 onwards, this is no longer the case. If you attempt to run an incremental synchronization for an upgraded System Manager or Communication Manager, the snychronization stops and an error message is displayed.
- Support for running synchronization forcefully: From Release 10.2.1, a new option enables administrators to run an initializing synchronization forcefully. If you run the synchronization forcefully, System Manager performs the initial synchronization without checking for any data discrepancy between Communication Manager and System Manager.

Enhanced logging

From Release 10.2.1, the IP and hostname of the Communication Manager during synchronization are logged. This information enables administrators to easily identify a specific Communication Manager for duplex pairs.

Support for Software-Only Deployment on Nutanix Environment

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

CLI alternative to Serviceability Agents

The Serviceability Agent is an enhanced version of the SAL agent for forwarding logs, harvesting logs, and for alarming. The Serviceability Agent sends SNMPv2 and SNMPv3 traps and notifies the configured NMS destinations where System Manager and the SAL gateway are the two mandatory destinations.

With the Serviceability Agent user interface, System Manager supports Command Line Interface (CLI) scripts for each serviceability task. Avaya offers this CLI support as an alternative to the Serviceability Agent user interface.

Red Hat Enterprise Linux (RHEL) 8.10 support

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

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

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

New in System Manager Release 10.2

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

Support for VMware 8.0

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

Support for J139, J159, J189, and J189CC endpoints

With Release 10.2, System Manager supports the following J-Series endpoints: J139, J159, J189, and J189CC

To add or edit these endpoints, go to the **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** page on the System Manager web console. You cannot edit these endpoints from the **Elements** > **Communication Manager** > **Element Cut-Through** page on the System Manager web console or from the Communication Manager command-line interface.

When you add these endpoints from System Manager, you can view these stations on the Element Cut-Through page on the System Manager web console and on the Communication Manager command-line interface.

Communication Manager displays these endpoints in the **Type** field of the **Station** form as **AvyaSIP** or **AvyaSIPCC**, and the actual endpoint type displays in the **Actual** field, such as J139 and J159.

Support for the send-nn and Q-call buttons on J-Series endpoints

With Release 10.2, the following endpoints support the **send-nn** and **Q-call** buttons:

- On System Manager: J139, J159, J169, J179, J179CC, J189, and J189CC
- On Communication Manager: AVYASIP and AVYASIPCC

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

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

Feature description

Overview

The following sections provide a brief description of the functionality of the feature that System Manager provides in support for various Avaya products. For detailed information on the services

available for a specific Avaya product, see the interoperability table in the *System Manager 10.2.x Product Offer Definition* on the Avaya Support website at http://support.avaya.com.

Common console

The common console is a common management interface for managing various applications in System Manager. It is a framework for the aggregation of management presentation views and supports dynamic extendibility and contraction as you add or remove management applications. You can use the web management console in a variety of scenarios ranging from product-specific management to suite management. The different scenarios can leverage the common look-and-feel and common components.

Solution Deployment Manager

Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® applications. Solution Deployment Manager supports the operations on the customer's Virtualized Environment and the Avaya Aura® Virtualized Appliance model.

Solution Deployment Manager supports migration of Virtualized Environment-based 8.1.x or 10.1.x applications to Release 10.2.x in the customer's Virtualized Environment. For migrating to Release 10.2.x and later, you must use Solution Deployment Manager Release 10.2.x and later.

Release 7.0 and later supports a standalone version of Solution Deployment Manager, the Solution Deployment Manager client. For more information, see *Using the Solution Deployment Manager client*.

System Manager with Solution Deployment Manager runs on:

- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.
- Software-Only environment: Avaya Aura® applications are deployed on the customer-owned hardware and the operating system.
- Avaya Solutions Platform 130: Avaya Aura® applications are deployed on the Avaya provided hardware.

Note:

- Solution Deployment Manager does not support that application deployment on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 Release 6.0.
- Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

With Solution Deployment Manager, you can do the following in Virtualized Environment, Avaya Solutions Platform 130, and Avaya Aura® Virtualized Appliance Release 8.x or earlier models:

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.

Note:

When an application is configured with Out of Band Management, Solution Deployment Manager does not support upgrade for that application.

For information about upgrading the application, see the application-specific upgrade document on the Avaya Support website.

- Download Avaya Aura® applications.
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications:
  - Communication Manager and associated devices, such as gateways, and media modules
  - Session Manager
  - Branch Session Manager
  - AE Services

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Refresh applications and associated devices and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade Avaya Aura® applications.
- Install software patch, service pack, or feature pack on Avaya Aura® applications.

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 10.2.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

Capability comparison between System Manager Solution Deployment Manager and the Solution Deployment Manager client

Centralized Solution Deployment Manager	Solution Deployment Manager Client
Manage virtual machine lifecycle.	Manage virtual machine lifecycle.
Deploy Avaya Aura® applications excluding the System Manager application.	Deploy Avaya Aura® applications including the System Manager application.
Deploy hypervisor patches only for Appliance Virtualization Platform Release 8.x or earlier.	Deploy hypervisor patches only for Appliance Virtualization Platform Release 8.x or earlier.
Upgrade Avaya Aura® applications excluding the System Manager application.	Upgrade System Manager. For information, see *Upgrading Avaya Aura® System Manager*.
Install software patches for Avaya Aura® applications excluding the System Manager application.	Install System Manager patches.

Table continues…

Centralized Solution Deployment Manager	Solution Deployment Manager Client
Discover Avaya Aura® applications.	-
Analyze Avaya Aura® applications.	-
Create and use the software library.	-

Solution Deployment Manager Client

For the initial System Manager deployment or when System Manager is inaccessible, you can use the Solution Deployment Manager client. The client must be installed on the computer of the technician. The Solution Deployment Manager client provides the functionality to deploy the OVAs or ISOs on an Avaya-provided server, customer-provided Virtualized Environment, or Software-only environment.

A technician can gain access to the user interface of the Solution Deployment Manager client from the web browser.

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Avaya appliances, VMware-based Virtualized Environment, and Software-only environment.
- Upgrade VMware-based System Manager from Release 8.1.x or 10.1.x to Release 10.2 and later.
- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.
- Create the Appliance Virtualization Platform Release 8.x or earlier Kickstart file.
- Generate the Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1 Kickstart file.
- Install Appliance Virtualization Platform patches.
- Restart and shutdown the Appliance Virtualization Platform host.
- Start, stop, and restart a virtual machine.
- Change the footprint of Avaya Aura® applications that support dynamic resizing. For example, Session Manager and Avaya Breeze® platform.

Note:

- You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.
- You must always use the latest Solution Deployment Manager client for deployment.
- Solution Deployment Manager does not support that application deployment on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 Release 6.0.
- Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

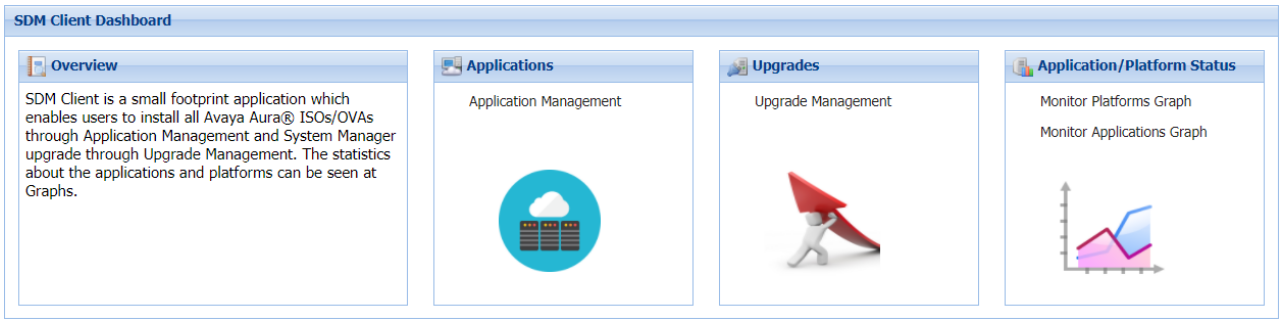


Figure 1: Solution Deployment Manager Client dashboard

Solution Deployment Manager client capabilities

The Solution Deployment Manager client provides the following capabilities and functionality:

- Runs on the following operating systems:
  - Windows 8.1, 64-bit Professional or Enterprise
  - Windows 10, 64-bit Professional or Enterprise
  - Windows 11, 64-bit Professional or Enterprise
  - Windows Server 2016, 64-bit Professional or Enterprise
  - Windows Server 2019, 64-bit Professional or Enterprise
  - Windows Server 2022, 64-bit Professional or Enterprise
- Supports the same web browsers as System Manager.
- Provides the user interface with similar look and feel as the central Solution Deployment Manager in System Manager.
- Supports deployment of System Manager. The Solution Deployment Manager client is the only option to deploy System Manager.
- Supports the Flexible footprint feature. The size of the virtual resources depends on the capacity requirements of Avaya Aura® applications.
- Defines the physical location for Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier, ESXi host, or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0), and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Manages lifecycle of the OVA applications that are deployed on the Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.

  Note:

  For the Avaya Aura® Messaging element, trust re-establishment is not required.
- Deploys the Avaya Aura® applications that can be deployed from the central Solution Deployment Manager for Avaya Aura® Virtualized Appliance and customer Virtualized Environment. You can deploy one application at a time.

Note:

- System Manager must be on the same or higher release than the application you are upgrading to. For example, you must upgrade System Manager to 10.2 before you upgrade Communication Manager to 10.2.

  All the applications that are supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for the version of applications that are supported by System Manager, see Avaya Aura® Release Notes on the Avaya Support website.

- Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 10.2 OVA, Solution Deployment Manager Client version must be on Release 10.2 or higher. Solution Deployment Manager Client cannot be on Release 10.1.

- Configures application and networking parameters required for application deployments.
- Supports selecting the application OVA file from a local path or an HTTPS URL. You do not need access to PLDS.
- Supports changing the hypervisor network parameters, such as IP Address, Netmask, Gateway, DNS, and NTP on Appliance Virtualization Platform.
- Supports installing patches for the hypervisor on Appliance Virtualization Platform.
- Supports installing software patches, service packs, and feature packs only for System Manager.

  Note:

  To install the patch on System Manager, Solution Deployment Manager Client must be on the same or higher release as the patch. For example, if you are deploying the patch for System Manager Release 10.2, you must use Solution Deployment Manager Client Release 10.2 or higher.

  However, to install the patch on System Manager Release 10.2, Solution Deployment Manager Client must be on Release 10.2.

  Avaya Aura® applications use centralized Solution Deployment Manager from System Manager to install software patches, service packs, and feature packs. For the applications that cannot be patched from centralized Solution Deployment Manager, use the application Command Line Interface or web console.

  For more information about supported releases and patching information, see Avaya Aura® Release Notes on the Avaya Support website.

- Configures Remote Syslog Profile.
- Creates the Appliance Virtualization Platform Kickstart file.
- Creates the Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1 Kickstart file.

- Supports the Pre-staging feature to prestage the System Manager OVA, service pack or feature pack, or data migration utility files to deploy, upgrade, or update the System Manager application.

Solution Deployment Manager

Solution Deployment Manager simplifies and automates the deployment and upgrade process.

With Solution Deployment Manager, you can deploy the following applications:

- System Manager
- Session Manager
- Branch Session Manager
- Communication Manager
- Application Enablement Services
- Avaya WebLM
- Avaya Diagnostic Server (Secure Access Link)
- Avaya Session Border Controller Release 8.0 and later
- Avaya Breeze® platform Release 3.3 and later
- Avaya Aura® Media Server

For the latest and most accurate information about other Avaya product compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Note:

When an application is deployed on a KVM host, Solution Deployment Manager does not support that application.

With Solution Deployment Manager, you can migrate, upgrade, and update the following applications:

- Hardware-based Session Manager
- System Platform-based Communication Manager
  - Duplex CM Main / Survivable Core with Communication Manager
  - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- System Platform-based Branch Session Manager
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services

  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- Session Manager Release 7.1.3.x and later
- Communication Manager Release 7.x and later
- Branch Session Manager Release 7.x and later
- Application Enablement Services Release 7.x and later
- Avaya Breeze® platform Release 3.3 and later
- System Manager Release 7.1.3.x and later (using SDM client only)
- WebLM Release 7.x and later

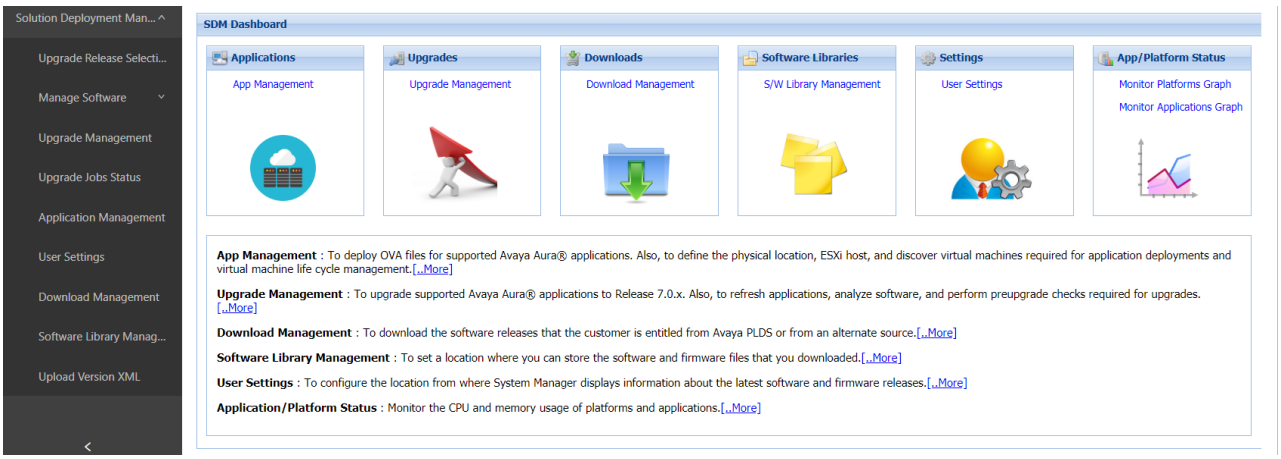
Note:

You must manually migrate the Services virtual machine that is part of the template.

The centralized deployment and upgrade process provides better support to customers who want to upgrade their systems to Avaya Aura® Release 10.2.x. The process reduces the upgrade time and error rate.

Solution Deployment Manager dashboard

You can access the Solution Deployment Manager dashboard from the System Manager web console or by installing the Solution Deployment Manager client.



Solution Deployment Manager capabilities

With Solution Deployment Manager, you can perform deployment and upgrade-related tasks by using the following links:

- **Upgrade Release Setting**: To select **Release 7.x Onwards** or **6.3.8** as the target upgrade. **Release 7.x Onwards** is the default upgrade target.
- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module, and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **Application Management**: To deploy OVA files for the supported Avaya Aura® application.
  - Configure Remote Syslog Profile.

  - Generate the Appliance Virtualization Platform Release 8.x or earlier Kickstart file.
  - Generate the platform Kickstart file for the following Appliance Virtualization Platform or Avaya Solutions Platform platforms:
    - Appliance Virtualization Platform 8.0.x
    - Appliance Virtualization Platform 8.1.x
    - Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1
- **Upgrade Management**: To upgrade Avaya Aura® applications to Release 10.2.x.
- **User Settings**: To configure the location from where System Manager displays information about the latest software and firmware releases.
- **Download Management**: To download the OVA files and firmware to which the customer is entitled. The download source can be the Avaya PLDS or an alternate source.
- **Software Library Management**: To configure the local or remote software library for storing the downloaded software and firmware files.
- **Upload Version XML**: To save the `version.xml` file to System Manager. You require the application-specific `version.xml` file to perform upgrades.

Automated upgrades and migrations of Avaya Aura® applications

From System Manager Release 7.0 and later, several Avaya Aura® applications support an automated migration path by using System Manager Solution Deployment Manager. The migration process can include the following tasks:

- Changing the server, operating system, and the hypervisor.
- Creating and restoring a backup in addition to the normal upgrade process for the application.

The key objectives of the automated upgrade and migration are:

- Move from a manual procedure on the application server to an automated migration procedure on a centralized System Manager.
- Eliminate the time spent in waiting for each migration step. With an automated sequencing of tasks, the application migration events run automatically in the background.
- Move from multiple manual tasks that require human intervention and assessment that might be error prone to reliable integrated checks that assess and confirm migration readiness.

Release 7.0 and later support automated migrations for:

- System Platform-based Communication Manager Release 6.x and Branch Session Manager Release 6.x
- Linux-based Session Manager Release 6.x and Communication Manager Release 5.2.1

The automated migration functionality applies to the:

- Avaya-provided virtual appliance offer Appliance Virtualization Platform.
- Customer-provided Virtualized Environment.

Supported servers

The following servers are supported for deployments and upgrades to Release 10.2.x and later:

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

For fresh installations, use Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640.

Dual stack support

System Manager Release 7.1 and later support dual stack. In dual stack, the system can handle both IPv4 and IPv6 addresses simultaneously. For applications with management interface over both IPv4 and IPv6, System Manager supports only IPv4 addresses until explicitly configured to support IPv6 addresses.

IPv6 Support

System Manager Release 7.1 and later support IPv6 addresses with dual stack capabilities. The System Manager administrator can configure IPv6 addresses for features such as Geographic Redundancy, Certificates with IPv6 address, System Upgrade, and Discovery of network elements.

Out of Band Management in System Manager

Out of Band Management is two physically or logically separated network connections or both that connects to a private management network of the customer. The network connection provides secure management and administration of Avaya products. With Out of Band Management, you can separate the management network and data network traffic to System Manager.

System Manager provides the following network interfaces:

- The regular eth0 interface that was present in releases earlier than System Manager Release 10.2.x, is called the Management interface or Out of Band Management interface. The IP address is called as the Management IP address. The Management interface is mandatory for configuration.

  The following are the examples of System Manager Management network traffic:

  - Database replication with Session Manager
  - Element management. For example, Session Manager, Communication Manager, and Avaya Breeze® platform.
  - User management
  - Solution deployment, upgrades, and software patch install

- If Out of Band Management is enabled, then the public interface is configured with Public IP address and used for the nonmanagement traffic. This is an optional configuration.

  The following are the examples of System Manager nonmanagement or public network traffic:

  - End-user self-provisioning

- Client devices getting certificates through SCEP
- Tenant Management

Out of Band Management configuration persists across System Manager upgrades, updates, and restarts.

For configuring Out of Band Management in System Manager, System Manager must be deployed on an Avaya Solutions Platform 130 host that is configured with Out of Band Management. To configure Out of Band Management on Avaya Solutions Platform 130, see *Installing the Avaya Solutions Platform 130 Series*.

Note:

Once OOBM is enabled on System Manager, public interface eth1 is no longer reachable using ping command from other systems that are present in a public network. However, System Manager can reach other systems on a public interface.

Out of Band Management in a Geographic Redundancy setup

When you configure Geographic Redundancy, provide Management network details only. Validation fails if you configure Geographic Redundancy with Public network details. In Geographic Redundancy setup, you do not disable or enable Out of Band Management on both primary and secondary System Manager virtual machine. You can enable Out of Band Management on the primary System Manager virtual machine and disable Out of Band Management on the secondary System Manager virtual machine, and vice versa.

Restoring System Manager backup

While restoring backup on System Manager with different Out of Band Management network details, the restore operation fails at validation phase.

Tenant Management on Out of Band Management-enabled System Manager

By default, the Multi Tenancy feature is disabled on System Manager when Out of Band Management is enabled. You must enable Multi Tenancy on Out of Band Management-enabled System Manager for the Tenant Management administrator to manage tenant users.

Geographic Redundancy

The System Manager Geographic Redundancy service replicates the Avaya Aura® element support for two geographically distant System Manager sites with separate subnetworks and across a WAN so that the System Manager management services can change from one site to another when one of the sites or servers fails. The System Manager Geographic Redundancy sites are set up in pairs with each site in a System Manager standalone or System Manager HA configuration. You can designate one server from the pair as the primary System Manager server and the other as the secondary System Manager server.

In normal operation also called sunny-day scenario, the primary System Manager provides all element administration and automatically replicates the administrative changes made on the primary System Manager server to the secondary System Manager server on a batch transaction basis. The secondary System Manager functions in the warm standby mode or the read-only mode and provides a subset of System Manager services, such as the System Manager Geographic Redundancy status or statistics, Inventory, and Authentication and Authorization.

In the event of catastrophic failure or split network, also called rainy-day scenario, you can activate the System Manager server that you designated as secondary to assume full management of all supported Avaya Aura® elements. The elements that support the Active-Standby mode include Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Geographic Redundancy-unaware elements might require manual intervention to gain services from the secondary System Manager server that is active.

The primary and the secondary System Manager servers can be in active mode in the split network scenarios.

After deactivation of the secondary System Manager server, the system administrator selects the database of the primary or the secondary System Manager server as the master database. The System Manager feature provides tools to select the database. After the database recovery and replication, the System Manager Geographic Redundancy servers revert to the normal operation mode, Active-Standby.

Geographic Redundancy configuration prerequisites

With System Manager 7.1, the System Manager administrator must perform the following in sequence before enabling and configuring Geographic Redundancy:

1. Adding the primary System Manager server as Certificate Revocation List (CRL) in the secondary System Manager server.
2. Adding trusted certificate of primary System Manager server to secondary System Manager server.

Data Replication Service

Data Replication Service (DRS) replicates data stored on the System Manager server to other element nodes or the slave nodes. DRS uses and extends SymmetricDS as the underlying mechanism for data replication.

SymmetricDS is an asynchronous data replication software that supports multiple subscribers and bi-directional synchronization. SymmetricDS uses Web and database technologies to replicate tables between relational databases in near real time. The system provides several filters while recording the data, extracting the data that has to be replicated to a slave node, and loading the data on the slave node.

Databases provide unique transaction IDs to rows that are committed as a single transaction. SymmetricDS stores the transaction ID along with the data that changed, so that it can play back the transaction at the destination node exactly the way it happened. This means that the target database maintains the same integrity as the source.

DRS provides a mechanism wherein elements can specify their data requirements in an XML document. On the basis of the XML document, DRS creates database triggers on the specified application tables and captures the database events for delivery to other element nodes. The client nodes then fetch these database events.

Data replication happens in two distinct phases:

- Full-sync. This is the initial replication phase, wherein whatever data the replica node requests is replicated to the client node.

- Regular-sync. This is the phase after full-sync, wherein subsequent change events are replicated to the replica node.

DRS supports the following modes of replication:

- Replication in Repair mode. In the repair mode, DRS replicates all of the requested data from the master database to the database of the replica node. Repair should only be necessary if there is a post-install failure of DRS.
- Automatic synchronization mode. After the database of the replica node is loaded with the requested data, the subsequent synchronizations of the master database and the replica database occur automatically. DRS replicates only the data that has been updated since the last replication. Automatic synchronization is a scheduled activity and occurs after each fixed interval of time as set in the configuration files.

The data from the master database is sent to the replica node in batches. DRS creates replication batches whenever the data in the master database is added, modified, and deleted.

Using DRS, you can:

- View replica nodes in a replica group.
- Repair the replica nodes that are not synchronized. The repair action replicates the required data from System Manager.

Management of users, public contacts, and shared address

Management of users

User Profile Management (UPM) is a shared service that supports a logically centralized data store. Through the System Manager web console, applications can gain access to the data store and obtain the user information that applications require. Administrators or end users do not need to provide user information for each application.

UPM uses data synchronization to achieve a single-point user administration. UPM synchronizes a user data event that is generated at the application level with the central user space and other connected applications.

If an enterprise directory is connected, then UPM maintains synchronization at the enterprise level. UPM adapts to the changes that occur in the enterprise directory, specifically additions, deletions, and modifications.

Management of public contacts

As an administrator, you can:

- Define public contacts of users in System Manager for an enterprise.
- Share the public contacts with all the users in System Manager.

Management of shared address

You can manage the shared address of the users in the enterprise. All users in the enterprise share the common addresses. As an administrator, you can:

- Create a new shared address.
- Modify and delete an existing shared address.

Fault management

The Fault management service presents the status of alarms, traps, and notifications received by System Manager and its components, and the other elements that are integrated with the System Manager SAL agent. The Fault management service maps events to alarms and tracks the state of alarms. Using the Fault Management service, you can acknowledge and clear alarms.

The Alarm management service provides a central point for receiving alarms that System Manager and other components generate. The service supports alarm monitoring, acknowledgement, configuration, clearing, and retiring. You can also browse System Manager for historical alarm events.

Logging service

The Logging service provides configuration capabilities and overall management of logs. It receives and stores log events and harvests file-based logs or local database logs.

The log viewer is integrated with the common console to provide consistent presentation of log messages for System Manager and the adopters. It displays a list of logs where you can view the details of each log, search for logs, and filter specific logs. Log details include information about the event that generates the log and the severity level of the log. You can search logs based on search conditions and set filters to view logs that match the filter criteria.

Log Harvester

The Log Harvester service manages the retrieval, archival, and analysis of harvested log files stored in hosts or elements on which Serviceability Agent is enabled. The Serviceability Agent harvests the logs and sends the harvested logs to the Logging service through HTTPS. The logging service does the following:

- Identifies a successful harvest request related to a harvest profile.
- Accepts the file segments.
- Creates a well-defined file structure, and saves the request in the System Manager node.

You can harvest log files for one or more products of the same or different types running on the same or different computers. The system displays the list of file archives and respective profiles on the log harvesting user interface, and the status of each archive is available in the user interface table.

Audit Logging

System Manager Release 7.1 and later support the Audit Logging configuration. By using this configuration, System Manager can notify the administrator and perform the configured action during one or all of the following events:

- Audit failure
- 75% occupation of audit partition
- 90% occupation of audit partition

Scheduler

The Scheduler service provides a generic job scheduling service for System Manager and the adopting products. It provides an interface to execute a task on demand or on a periodic basis. So you can schedule a job to generate an output immediately or set the frequency of the task execution to run on a periodic basis. You can also modify the frequency for a periodic job. After you define a task or a job, System Manager creates instances of the task, monitors the execution of the task, and updates the status of the task.

Scheduled jobs can be of following three types:

- system scheduled
- admin scheduled
- on-demand

Bulk import and export

In System Manager, you can import and export user profiles and global settings in bulk. To import data in bulk, you must provide an XML file or an Excel file as input file. System Manager validates any file that you upload during the bulk import operation.

System Manager filters uploaded files based on the file extension and mime type or bytes in the file.

The system exports the data to an XML file and an Excel file. The System Manager database stores the imported user profiles and global settings data.

You can import and export the following user attributes in bulk:

- Identity data
- Communication profile set
- Handles
- Communication profiles

  The supported communication profiles are CM Endpoint, CM Agent, Messaging, Session Manager, CS 1000 Endpoint, IP Office, Presence, Avaya Breeze® platform, Work Assignment, Avaya Messaging, and Avaya Meetings Server.

You can import and export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- Default access control list (ACLs)

Important:

System Manager does not support import and export of roles in bulk.

Bulk import and export using the Excel file

In System Manager, you can import and export user profiles in bulk by using an Excel file and an XML file. To import data in bulk, provide an XML file or an Excel file as input that System Manager

supports. When you export the data from the System Manager web console, the system exports the data to an XML file and an Excel file that System Manager supports.

Microsoft Office Excel 2007 and later support bulk import and export in the `.xlsx` format. You can download the Excel file from the User Management page.

Importing and exporting in bulk by using the Excel template provides the following features:

- Supports the following types of user information:
  - Basic. The identity attributes of the user that include user provisioning rule name for the user, the tenant, and organization hierarchy details
  - Profile Set. Entries for all communication profile sets for all users

    The Profile Set sheet contains an entry for each communication profile set for a user. The user must set only one communication profile set as *true* for a user in the **Is Default** column. The value *true* indicates that the communication profile set of the user is the default.
  - Handle. The communication address of the user
  - Session Manager profile
  - Avaya Breeze® platform profile
  - CM Endpoint profile with all attributes of the station communication profile
  - CM Agent profile with all attributes.
  - Messaging profile
  - Avaya Messaging profile
  - IP Office Endpoint profile
  - CS 1000 Endpoint profile
  - Presence profile
  - Work Assignment profile
  - Avaya Meetings Server profile
- Supports more than one communication profile set.
- Supports the creation, updation, and deletion of the user by using the same Excel file. However, you can only perform one operation at a time.
- For updation, supports only the partial merge operation.

  Bulk import and export by using Excel does not support complete or partial replace of the user for imports in bulk.

Bulk import and export by using Excel supports a subset of user attributes that XML supports. For example, Excel does not support user contacts, address, and roles.

The Excel file

The sample Excel file contains the sample data of some key attributes of the user. The Excel file provides a description of header fields. When you download the Excel template from the User Management page, the values remain blank. To use the Excel file, export some users for reference in an Excel file.

The login name in the **Basic** worksheet is the key attribute that you use to link the user records in other worksheets.

The login name of the user and the profile set name in the **Profile Set** worksheet are used to link to the user records in other worksheets for that user profile.

- Although you can edit the header fields in the Excel template, do not change any details of any headers in the worksheets. The import or export might fail if you change the details of the header.
- Do not change the column position in the Excel file or the structure of the Excel template.
- Do not sort the data in worksheets.

CM Endpoint communication profile

The Excel file contains all attributes for the CM station endpoint profile that are spread in different worksheets. The parent sheet provides a link to the same user profile record in the child worksheet. The link points to the first record in the child sheet if the user profile contains multiple records in the child worksheet.

Multi Tenancy

Using the Multi Tenancy feature, tenants can share the same instance of the application, while allowing the tenants to manage users to fit the customer needs as if the application runs on a dedicated environment.

You can manage Multi Tenancy from the System Manager web console. System Manager supports the following capabilities:

- Administer the tenant.
- Administer tenant administrators for a tenant.
- Administer the organization hierarchy of the tenant.
- View the tenant hierarchy on the Tenant Management and User Management pages.
- View the tenant associated with a user.
- Create and edit the user associated with a tenant from the User Management page.

System Manager provides a tenant administration dashboard that requires administrator credentials.

By default, the Multi Tenancy feature is disabled. To use the Multi Tenancy feature, you must manually enable it. After enabling the Multi Tenancy feature, you cannot disable the feature.

System Manager supports maximum 250 tenant partitions as part of System Manager Multi Tenant Management.

User provisioning rule

The administrator can create users by using the user provisioning rule. When the administrator creates a user, the system displays the default values, the communication addresses, and the communication profiles that are defined in the rule. The administrator must provide minimal user information.

The administrator can:

- provision the user by using the user provisioning rules from the System Manager web console, web services, directory synchronization, and bulk import services.
- assign only one user provisioning rule to a user.

System Manager supports creating, editing, duplicating, and deleting the user provisioning rule. You can use the User Management link on the System Manager web console to associate the user provisioning rule with users while creating and editing users.

Configuration management

Configuration management provides a configuration repository for System Manager services. Configuration management is responsible for storing configuration data, also called as profiles, for System Manager services and notifying the services of configuration changes.

You can view and edit a profile of a service using Configuration management.

Security features

OVA Signing

OVA signing is a security feature where OVA files are digitally signed to ensure file integrity. The system verifies the digital signature of the OVA, feature pack, and service pack before deploying, upgrading, and patching operations.

Security hardening

Using the security hardening feature, you can enable or disable military grade hardening or commercial grade hardening for System Manager. Enabling military grade hardening in System Manager enables commercial grade hardening by default.

It also facilitates a system with higher security and restricts unauthorized access and changes to the system settings.

Certificate-based authentication

With System Manager 7.1, you can disable the password-based login and configure the certificate-based authentication for system login.

The certificates for this authentication can be issued by System Manager as the certificate authority or by a third-party certificate authority.

To authenticate the user, the system provides the option to retrieve only the selected fields from the certificate.

Backup encryption

With System Manager 7.1, you can encrypt system backups using a password. Encrypted backups of a military grade hardened system can be restored to a matching type of hardened system: military grade, commercial grade, and standard.

Encrypted backups of a commercial grade hardened system can be restored only on a commercial grade hardened system or a standard hardened system. Likewise, encrypted backups of standard hardened system can be restored only on a standard hardened system.

Enhanced Access Security Gateway (EASG) overview

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

Element management

Inventory maintains a repository that records elements deployed on System Manager, including their runtime relationships. An element in the Inventory refers to a single or clustered instance of a managed element. Inventory provides a mechanism for creating, modifying, searching, and deleting elements and the access point information from the repository. Inventory retrieves information about elements that are added or deleted from the repository.

Inventory integrates the adopting products with the common console of System Manager. Through Inventory, element type can provide a link that can redirect to the Web page of the element manager. System Manager Web Console displays the links for only specific element types.

Inventory supports the creation and updation of application systems by importing data from an XML file. You can import elements only through the Web console.

Group management

Group and Lookup Service (GLS) is a shared service that provides group administration and lookup service for managed resources. GLS encapsulates the mechanisms for creating, changing, searching, and deleting groups and group memberships. Use GLS to group resources in ways that work best for the business, such as organizing resources by location, organization, and function.

On the System Manager web console, with GLS, you can assign different roles to administrators and allow administrators to perform only limited tasks on group of resources. For example, you can create a user group so that only an authorized user can manage the user group.

GLS supports group administration for the following common resources:

- Shared across elements, such as roles and users
- Unshared element-specific resources

GLS contains a repository of groups and memberships from System Manager and other applications that use the GLS service. GLS synchronizes the resources with other Avaya applications and services that manage these resources. GLS maintains resource IDs and their group memberships. With GLS, you can search for one or more resources based on their attribute values and get resource attributes for one or more resources.

With GLS, you can perform the following operations:

- Create groups.
- View and change groups.
- Create duplicate groups by copying properties of existing groups.
- Move groups across hierarchies.
- Assign and remove resources for groups.
- Delete groups.
- Synchronize groups.

As a shared service, GLS reduces the time and effort involved by defining reusable groups of managed resources that more than one application or service requires. For example, you can use the group of resources to assign permissions through Role Based Access Control (RBAC).

License management

System Manager provides Web-based license manager (WebLM) to centrally manage licenses for one or more Avaya software products for your organization. All Avaya applications that use WebLM for license management use WebLM that System Manager provides instead of WebLM on System Platform.

System Manager WebLM supports the Centralized licensing feature for Avaya Aura® Communication Manager.

To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

System Manager Communication Manager capabilities overview

System Manager provides a common, central administration of some IP Telephony products. With the central administration feature, you can consolidate the key capabilities of Integrated Management administration products with other Avaya Management tools on a common software platform. With System Manager, you can administer Avaya Aura® Communication Manager, Communication Manager Messaging, Avaya Aura® Messaging, and Modular Messaging. The following sections provide some features of System Manager.

Managing Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. With System Manager, you can add, edit, view, or delete objects through Communication Manager.

Endpoint management

Using endpoint management you can create and manage endpoint objects and add, change, remove, and view endpoint data.

Template management

Using Templates, you can specify specific parameters of an endpoint or a subscriber once and reuse the template for subsequent tasks of adding endpoints or subscribers. You can use default templates or add your own custom templates.

The two categories of templates are: default templates and user-defined templates. You cannot edit or delete the default templates. However, you can modify or remove user-defined templates at any time.

Subscriber management

Using Subscriber Management, you can manage, add, change, remove, and view subscriber data. Subscriber management supports Avaya Aura® Messaging, Communication Manager Messaging, and Modular Messaging objects.

Discovery Management

You can discover specific devices within the network using the Discovery Management capability of System Manager. You can also manage the Simple Network Management Protocol (SNMP) access parameters used for the discovery process. Device discovery discovers your network, including subnets and nodes.

Element Cut Through

Using the Element Cut-Through link, you can gain access to the Communication Manager cut through the Element Cut-Through page. As an administrator, you have permission to gain access to the Communication Manager cut through.

Granular role-based access control

With the Granular role-based access control feature, you can restrict access to Communication Manager resources, such as gateways and servers, and objects on resources, such as Agent Login ID.

Based on the role that a user has, System Manager supports range permissions along with the operation permissions assigned to the user. You can assign permissions or a combination of permissions to users. The permissions include adding, editing, deleting, and duplicating objects. For example, if you assign a range of 1000:4000 and define permissions for Add, Edit, and Delete operations, the user can create, edit, and delete extensions within the range of 1000:4000.

The default value in the specific **Range** field is asterisk (*). If you retain this value, the user has access to the entire defined range.

You can define range-level granular permissions for the following Communication Manager objects:

- Endpoints
- Agent Login ID
- Announcement
- Audio Group
- Best Service Routing Pickup Group

- Holiday Table
- Variables
- Vector
- Vector Directory Number (VDN)
- Vector Routing Table
- Service Hours Table
- Coverage Answer Group
- Coverage Path
- Coverage Remote
- Coverage Time-of-Day
- Group-Page
- Hunt-Group
- Intercom Group
- Pickup Group
- Terminating Extension Group
- Route-Pattern
- Class of Restriction (COR)

Communication Manager feature concurrency enhancements

- Improve navigation speed of User management and Endpoint management webpages on System Manager.
- Concurrency with new Communication Manager and SIP Phone features:
  - Service observing from SIP Phone support, new **sip-sobsv** button and **listen-only** sub-field within the **sip-sobsv** button is available.
  - VOA Repeat or Interrupt for SIP CC Phone support, new **voa-repeat** button is available.
  - Add or Remove Agent Skill from SIP Phone support, new **add-rem-skill** button is available.
  - Auxiliary Agents Considered Idle support, new **AUX Agent Considered Idle** field to administer on the Agent LoginId object.
  - Forced Agent Logout from Auxiliary Work by Aux Reason Code Support, new fields are available.
  - Streaming Music-on-Hold from an external source, such as cloud, new **LiveStreamSource** field is available.
  - Hunt Position Busy Button support, new **hntpos-bsy** button is available.

Certification validation

With System Manager Solution Deployment Manager and Solution Deployment Manager client, you can establish a certificate-based TLS connection between the Solution Deployment Manager

service and a host that is running Avaya Aura® 7.x and later applications. This provides secure communications between System Manager Solution Deployment Manager or the Solution Deployment Manager client and Appliance Virtualization Platform or ESXi hosts or vCenter.

The certificate-based sessions apply to the Avaya Aura® Virtualized Appliance offer using host self-signed certificates and the customer-provided Virtualization Environment using host self-signed or third-party certificates.

You can check the following with certificate-based TLS sessions:

- Certificate valid dates
- Origin of Certificate Authority
- Chain of Trust
- CRL or OCSP state
- Log Certificate Validation Events

Solution Deployment Manager checks the certificate status of hosts. If the certificate is incorrect, Solution Deployment Manager does not connect to the host.

For the correct certificate:

- The fully qualified domain or IP address of the host to which you are connecting must match the value in the certificate SAN or the certificate Common Name and the certificate must be in date.
- Appliance Virtualization Platform and VMware ESXi hosts do not automatically regenerate their certificates when host details such as IP address or hostname and domain changes. The certificate might become incorrect for the host.

If the certificate is incorrect:

- For the Appliance Virtualization Platform host, Solution Deployment Manager regenerates the certificate on the host and then uses the corrected certificate for the connection.
- For the VMware ESXi host or vCenter, the system denies connection. The customer must update or correct the certificate on the host or vCenter.

  For more information about updating the certificate, see “Updating the certificate on the ESXi host from VMware”.

Note:

Solution Deployment Manager:

- Validates certificate of vCenter
- Validates the certificates when a virtual machine is deployed or upgraded on vCenter managed hosts

With Solution Deployment Manager, you can only accept certificate while adding vCenter. If a certificate changes, the system gives a warning that the certificate does not match the certificate in the trust store on Solution Deployment Manager. You must get a new certificate, accept the certificate as valid, and save the certificate on the system.

To validate certificates, you can open the web page of the host. The system displays the existing certificate and you can match the details.

Bulk import and export enhancements

System Manager provides the following bulk import and export enhancements:

- An option to export user data by using Excel or XML files.
- Time zone field for Avaya Aura® Messaging subscribers.

  The value must be in the standardized name format. For example, America/Phoenix. Otherwise, the system sets the Avaya Aura® Messaging subscriber time zone to the System Manager server time zone.

Avaya Aura® Device Services element

System Manager supports Avaya Aura® Device Services as an element.

With Avaya Aura® Device Services, clients and endpoints can store centrally and retrieve data such as configuration and deployment data. You can manage the data from any device.

Avaya Aura® Device Services supports the following services for devices:

- Contact Services: The service provides the following end-user focused services that are centrally located:
  - Directory Service: Manages your contacts from any of your devices. Performs an enterprise search of existing sources of contacts such as System Manager through PPM, exchanges local contacts, and enterprise directory.

    Only a provisioned user can use Contact Services.
  - User Service: Sets and retrieves information such as your preferred names, picture, and other preferences.
  - Picture Service: Supports creating (overrides default enterprise), deleting, and updating a picture of the user. It provides a centralized, firewall-friendly interface to present picture URLs in the contact information or search results.
- Notification Service: Provides a common infrastructure for a client or endpoint to subscribe to receive events from many service resources with a single connection.
- Dynamic Configuration Service: Provides discovery of configuration settings to UC Clients that can be customized on a global, group, individual, or platform basis. This simplifies the configuration process of users, and skips manual configuration and makes ready for use. Clients only need to provide identity information such as email addresses or Windows userid and enterprise credentials.
- Web Deployment Service: Supports publishing and deploying of UC client updates for end-users.

Security hardening options

System Manager provides the following security hardening options:

- selinux

- audit
- fips
- aide
- TLSv1, TLSv1.1, TLSv1.2, and TLSv1.3
- fapolicy

  By default, fapolicy is disabled.

You can enable or disable one or more security hardening options. While you can enable all the options, you can only disable selinux, audit, aide, and fapolicy.

Note:

If the FIPS option is selected or already enabled, you cannot select the TLSv1 and TLSv1.1 options.

Third-party certificate support

You can use third-party signed certificates in System Manager. A Certificate Signing Request (CSR) needs to be generated and shared with the third-party.

After the third-party signs the CSR, the certificate is valid. Third-party certificates can be used for application on Avaya Virtualization Platform. These certificates can also be used for certificate-based and common access card-based authentications.

Extended Hostname Validation

With the Extended Hostname Validation (EHV) feature, the system validates the host name or domain name of the server with the value in the **subject** or **subjectAltName** (SAN) field in the identity certificate for establishing the SSL connection.

Customer root account

With Release 8.0 and later, for accessing the root account, you can select the **Enable Customer Root Account for this Application** check box on the **Configuration Parameters** tab at the time of deploying or upgrading the application.

Preserve security hardening modes on upgrade

When you upgrade an application from Release 7.1.x to Release 8.0 and later, the system preserves the security modes that are configured on the Release 7.1.x application.

Data Encryption

From Release 10.1, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Avaya Solutions Platform 130 and VMware Virtualized Environment. Once you deploy the application with data encryption, you cannot disable data encryption after deployment.

By enabling Data Encryption, your Communication Product's certain Operational data and Log Files will be encrypted. You will be prompted to enter a passphrase that will be used to create or access an encryption key. You must remember the encryption passphrase, if not it can result in locking up the system. Secondly, you will be asked to configure the option for local key storage.

It is important to note that the encryption of the disk may have a performance impact. For further information, refer to the Avaya Product Administration guide(s). Before you select an encryption option, please read the Data Privacy Guideline so that you may better understand these options.

By disabling Data Encryption, your Communication Product's Operational data and Log Files will not be stored in encrypted partitions.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is selected, you need to reenter the encryption passphrase whenever the application reboots.

During reboot, the application prompts you to enter the encryption passphrase on VM console at first boot and upon entering the correct encryption passphrase, the system mounts all the encrypted disks.

Note the following:

- If a common encryption passphrase is used for all the encrypted partitions, but an incorrect encryption passphrase is entered in first attempt, then you have to enter the correct encryption passphrase for every partition at least once.
- Multiple failures on encryption passphrase boots the system into the Maintenance/ Emergency mode. To get the prompt again, you need to reboot the system.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is not selected during OVA deployment, the application creates the Local Key Store and the system does not prompt you to type the encryption passphrase whenever the application reboots to mount the encrypted disks. You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application.

Important:

An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa.

Encryption of System Manager partitions

When you enable data encryption for System Manager, the system encrypts the following partitions that have personal data.

- `/var/log`
- `/var/log/audit`
- `/var/lib/pgsql/data`
- `/var/opt/nortel/cnd`

Certificate renewal command overview

From System Manager Release 10.1.0.1 onwards, you can use the newly added command to renew the System Manager Identity (Server) certificates. The System Manager Certificate

Authority (CA), the System Manager subordinate CA (SubCA), or a third-party CA (EJBCA) can sign the System Manager Identity certificates.

Run the certificate renewal command to issue new System Manager CA issued Identity certificates for all System Manager services. The new System Manager CA issued Identity certificates are valid for 730 days or from the time the command runs till the System Manager CA expiry date, whichever is lesser.

You must run the command with the -FORCE argument in any of the following scenarios:

- If the System Manager services are secured using the third-party CA issued Identity certificates.
- If there is a problem with the System Manager certificates causing the System Manager web console to be down.

If you run the certificate renewal command with -FORCE argument, the -FORCE argument replaces the third-party CA issued and System Manager issued certificates with the System Manager CA issued certificates.

Use the certificate renewal command only if certificate management is not possible through **Services** > **Inventory** > **Manage Elements** on the primary System Manager. The best practice is to perform all the certificate management operations from the System Manager web console.

In System Manager configured with Geographic Redundancy, if the primary and secondary System Manager certificates expire, you must first renew the certificates on the primary System Manager. Before you renew the certificates on the secondary System Manager, ensure that the primary System Manager web console is up and running and you can log in. If there are expired certificates on the secondary System Manager, you cannot issue the secondary System Manager certificates from the primary System Manager web console.

You can find the certificate renewal command logs at the following location: `/var/log/Avaya/folder`

Important:

If your System Manager Certificate Authority expires, the command does not work. If the System Manager Certificate Authority expires or is nearing expiry, see the procedure in PSN005555u on the Avaya Support site.

You can run the certificate renewal command with the -FORCE argument or without any arguments.

Chapter 3: Avaya Aura® overview

Avaya Aura® applications deployment offers

Avaya Aura® supports the following deployment offers:

- Avaya Aura® Virtualized Environment (VE): Avaya Solutions Platform 130 (Dell PowerEdge R640, ESXi 7.0) and Customer-provided VMware infrastructure.

  Avaya Solutions Platform 130 R6.0 (Avaya-Supplied KVM on RHEL R8.10) or Avaya Solutions Platform S8300 R6.0 (Avaya-Supplied KVM on RHEL R8.10).

- Software-only and Infrastructure as a Service environment: Deployment on the Red Hat Enterprise Linux operating system.

  Note:

  The deployment of Avaya Aura® applications as software only is available but a restricted offer for net new deployments and requires Avaya Aura® BU approval before proceeding. If you have a business requirement to deploy Avaya Aura® as software only, please get in touch with your Avaya Sales team. Existing customers using software only deployments continue to be supported.

Virtualized Environment overview

You can deploy the Avaya Aura® Release 10.2.x applications in one of the following Virtualized Environments:

- Avaya Solutions Platform 130 Release 5.1 (Dell PowerEdge R640) is a single host server with a preinstalled ESXi 7.0 Standard VMware License.
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single host server with a preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.
- VMware in a customer-provided Virtualized Environment.

Note:

For more information about deploying applications, see the product-specific Software-Only and Infrastructure as a Service guide.

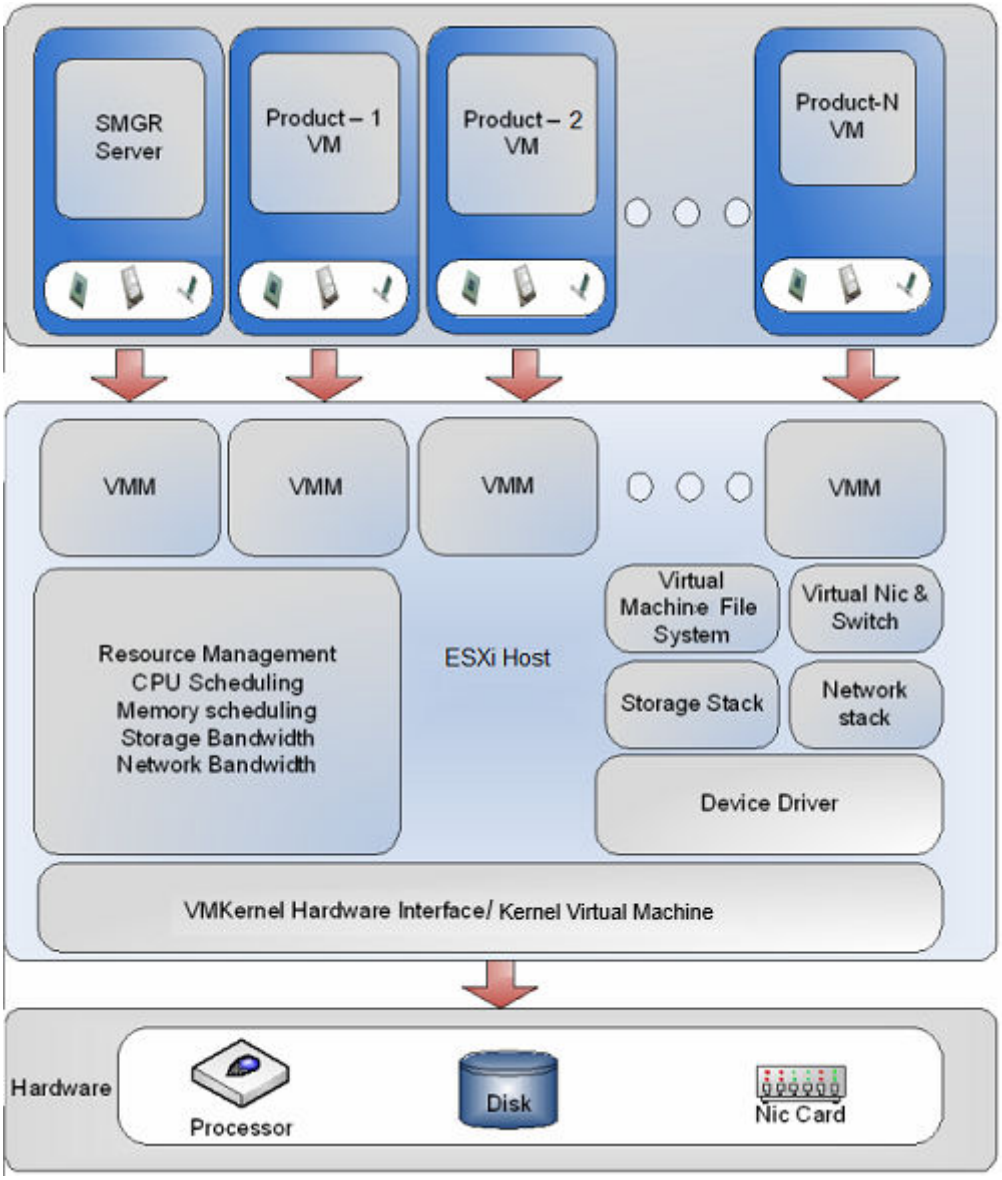
Supported applications in Virtualized Environment

- Avaya Aura® System Manager Release 10.2.x
- Avaya WebLM Release 10.1.3.x
- Avaya Aura® Session Manager Release 10.2.x
- Avaya Aura® Communication Manager Release 10.2.x
- Avaya Aura® Application Enablement Services Release 10.2.x
- Avaya Aura® Media Server Release 10.2.x

For the latest and most accurate information about other Avaya product compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Topology

The following is an example of a deployment infrastructure for System Manager on VMware.



Virtualized Environment components for VMware

Virtualized component	Description
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.
Customer-provided VMware or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0)	
ESXi	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.

Table continues…

Virtualized component	Description
ESXi Embedded Host Client	The ESXi Embedded Host Client is a native HTML and JavaScript application and is served directly from the ESXi host.
vSphere Client (HTML5)	Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.
vCenter Server	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion. This is not applicable for Avaya Solutions Platform 130.

Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10)

Virtualized component	Description
Avaya Solutions Platform 130 (Avaya-Supplied KVM on RHEL R8.10) or Avaya Solutions Platform S8300 (Avaya-Supplied KVM on RHEL R8.10).	
KVM Cockpit	Cockpit is a system administration tool that provides a user interface to monitor and administer servers through a web browser. Cockpit administrators can create and manage KVM-based virtual machines on the host system.

Support for VMware components

Avaya Aura® Release 10.2.x supports deployment and upgrades on the following VMware components in Virtualized Environment.

- VMware® vSphere ESXi 7.0
- VMware® vCenter Server 7.0
- VMware® vSphere ESXi 8.0
- VMware® vCenter Server 8.0

Note:

- Avaya Aura® Release 10.2 and later does not support vSphere ESXi 6.7.
- Avaya Aura® Release 10.1 and later does not support vSphere ESXi 6.0 and 6.5.
- Avaya Aura® Release 8.1.x and later supports KVM on RHEL Release 8.10 hypervisor.

  For more information about upgrading from RHEL 8.4 to RHEL 8.10, see:

  - *Upgrading Avaya Aura® Communication Manager*
  - *Upgrading Avaya Aura® Session Manager*
  - *Upgrading Avaya Aura® System Manager*
  - *Upgrading Avaya Aura® Application Enablement Services*

Support for KVM components

Avaya Aura® Release 10.2.x supports deployment and upgrades on the following KVM component in Virtualized Environment.

- KVM on RHEL 8.10

Software-only environment overview

In a software-only installation, the customer owns the operating system and must provide and configure the operating system for use with Avaya Aura® application. With the software-only offer, the customer can install and customize the operating system to meet the requirements to install the Avaya Aura® application.

You must run the software-only offer on the supported environments to enable the use of Avaya approved third-party applications for anti-virus, backup, and monitoring.

Customers and/or Service Providers must procure a server or virtual machine that meets the recommended hardware requirements and the appropriate version of Red Hat Enterprise Linux® Operating System.

Software security updates

Avaya Security Service Packs (SSP) are built for customers who do not use the software-only distribution. In a software-only deployment, the customer provides the operating system. The customer is responsible for installing the appropriate operating system and applying the relevant security patches from Red Hat.

For more details, see *Avaya Aura® Release Notes* on the Avaya Support website.

Avaya Aura® Software-Only environment RPMs

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020617u that Avaya publishes periodically on the Avaya Support website.

Note:

For information about RPM updates for the Red Hat Enterprise Linux operating system and required changes to operating system files on Software only installation, see *Avaya Aura® Software Only White paper* on the Avaya Support website.

Supported platforms

You can deploy the Avaya Aura® application software-only *ISO image* on the following:

- On-premise platforms:
  - VMware
  - Kernel-based Virtual Machine (KVM)
  - Hyper-V
  - Nutanix 6.5 and later

- Cloud platforms:
  - Amazon Web Services
  - Google Cloud Platform
  - Microsoft Azure
  - IBM Cloud for VMware Solutions

    Specifications for Avaya Aura® applications on IBM Cloud for VMware Solutions is same as that of the Virtualized Environment offer.

    For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

Supported applications in Software-only Environment

- Avaya Aura® System Manager Release 10.2.x
- Avaya WebLM Release 10.1.3.x
- Avaya Aura® Session Manager Release 10.2.x
- Avaya Aura® Communication Manager Release 10.2.x
- Avaya Aura® Application Enablement Services Release 10.2.x
- Avaya Aura® Media Server Release 10.2.x

Infrastructure as a Service environment overview

Infrastructure as a Service (IaaS) environment enables enterprises to securely run applications on the virtual cloud. The supported Avaya Aura® applications on IaaS can also be deployed on-premises. Avaya Aura® application supports the following platforms within this offer:

- Amazon Web Services

  Note:

  With Release 10.1.x and later, Avaya Aura® will no longer have the Amazon Web Services OVA. Deployment on Amazon Web Services is supported through the software only offer.
- Microsoft Azure
- Google Cloud Platform
- IBM Cloud for VMware Solutions

  For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

Supporting the Avaya Aura® applications on the IaaS platforms provide the following benefits:

- Minimizes the capital expenditure on infrastructure. The customers can move from capital expenditure to operational expense.
- Reduces the maintenance cost of running the data centers.
- Provides a common platform for deploying the applications.

- Provides a flexible environment to accommodate the changing business requirements of customers.
- Allows you to pay per-use licensing.
- Allows you to upgrade at a minimal cost.
- Supports mobility to move from one network to another.
- Allows you to stay current with latest security updates provided by the service provider.

You can connect the following applications to the Avaya Aura® IaaS instances from the customer premises:

- Avaya Aura® Messaging Release 6.3 and later
- G430 Branch Gateway and G450 Branch Gateway

Software security updates

Avaya Security Service Packs (SSP) are built for customers who do not use the software-only distribution. In a software-only deployment, the customer provides the operating system. The customer is responsible for installing the appropriate operating system and applying the relevant security patches from Red Hat.

For more details, see *Avaya Aura® Release Notes* on the Avaya Support website.

Amazon Web Services overview

Amazon Web Services is an Infrastructure as a Service platform that enables enterprises to securely run applications on the virtual cloud. The key components of Amazon Web Services are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

Microsoft Azure overview

Microsoft Azure is an Infrastructure as a Service platform that enables enterprises to securely deploy and manage applications through a global network of Microsoft-managed data centers.

Google Cloud Platform overview

Google Cloud Platform is a suite of public cloud computing services offered by Google.

IBM Cloud for VMware Solutions overview

IBM Cloud for VMware Solutions is a suite of public cloud computing services offered by IBM.

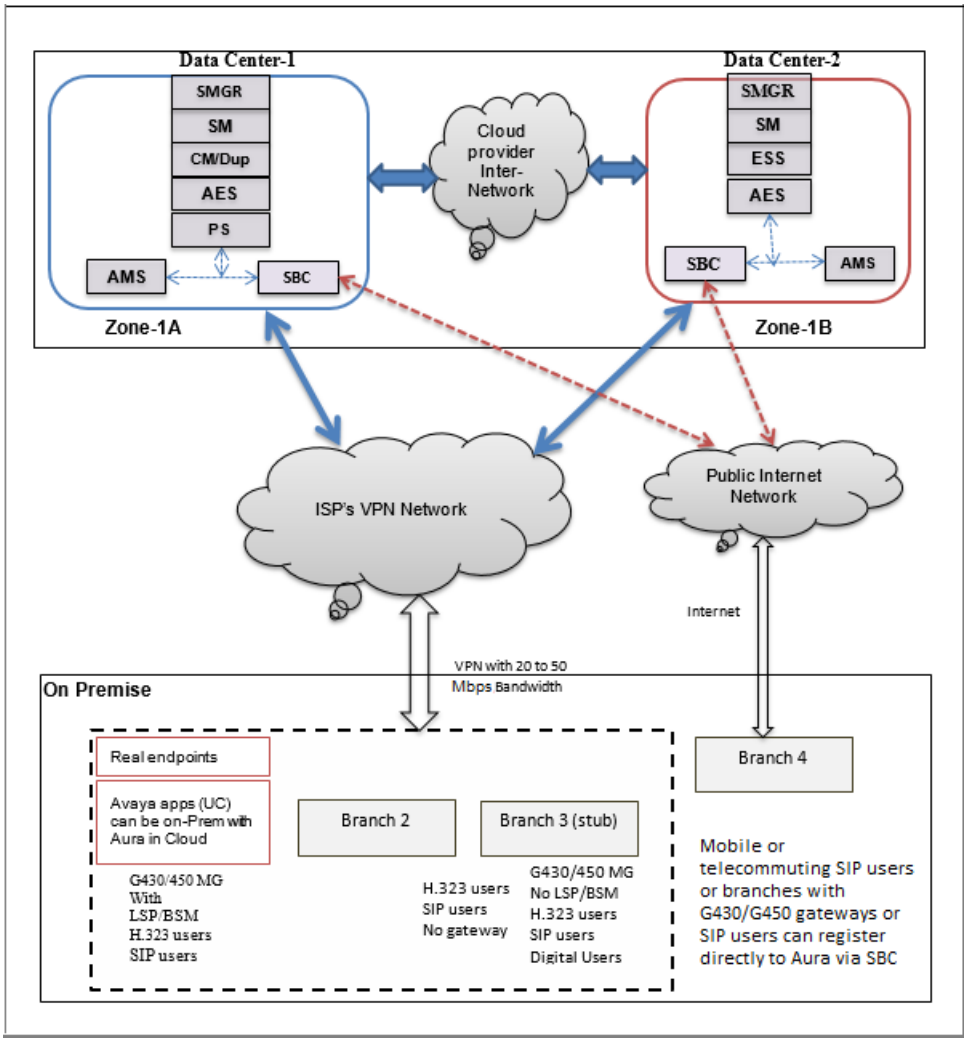
For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

Topology

The following diagram depicts the architecture of the Avaya applications on the Infrastructure as a Service platform. This diagram is an example setup of possible configuration offered by Avaya.

Important:

The setup must follow the Infrastructure as a Service deployment guidelines, but does not need to include all the applications.



Supported applications in Infrastructure as a Service Environment

Application	Release	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Avaya Aura® System Manager	Release 10.2.x	Y	Y	Y
Avaya WebLM	Release 10.1.3.x	Y	Y	Y
Avaya Aura® Session Manager	Release 10.2.x	Y	Y	Y
Avaya Aura® Communication Manager	Release 10.2.x	Y	Y	Y
Avaya Aura® Application Enablement Services (Software only)	Release 10.2.x	Y	Y	Y

Table continues…

Application	Release	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Presence Services using Avaya Breeze® platform	Release 10.1.x	Y	—	—
Avaya Aura® Media Server (Software only)	Release 10.2.x	Y	Y	Y

For the latest and most accurate information about other Avaya product compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Chapter 4: Interoperability

Product compatibility

For the latest and most accurate compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Chapter 5: Licensing requirements

When you place an order for the following products using the Avaya Solution Designer, you can include a new System Manager or an upgrade of System Manager as an entitlement:

- New Communication Manager, Session Manager, or CS 1000
- Upgrade of Communication Manager, Session Manager, or CS 1000

Additionally, you can add the System Manager DVD and the System Manager server to the order.

Chapter 6: Performance specifications

Capability and scalability specification

The table provides the maximum capacities supported for each element type.

Note:

Only one System Manager is available with each Avaya Aura® deployment. Therefore, the solution number is not the sum of all supported elements listed in the table.

Capacity	Maximum limit	Notes
Administrator logins	250	
Simultaneous logins	50	
Total administered endpoints of all types	300,000	To see the total number of endpoints, go to the **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** page on the System Manager web console.
Total administered users defined in the System Manager database	300,000	The total number of administered users with an Identity is configured in System Manager and might not have a communication profile defined. To see the defined users, go to the **Users** > **User Management** > **Manage Users** page on the System Manager web console.
Messaging mailboxes	300,000	
Contacts per user	250	
Public contacts	1,000	
Personal contact lists per user	1	
Members in a personal contact list	250	
Groups	300	
Members in a group	400	
Elements	25,000	
Communication Manager or CS 1000 or both	500	Specifies the capacity counts against the total number of elements.
Main Communication Manager	100	

Table continues…

Capacity	Maximum limit	Notes
Session Managers	28	
Branch Session Manager	5,000	
SIP Users	300,000	Total number of SIP users.
Total SIP devices	1,000,000	Total number of SIP devices.
IP Office	3,500	To support central licensing of 3500 IP Office 9.x and later, local WebLM licensing servers that are slaved to System Manager licensing are required. For more information, see the IP Office 9.x and later product offer.
IP Office Unified Communication Module or Application servers as part of Branch deployments	3,500	
Roles	200	
Roles per user	20	
Licensing clients	1,000	
Concurrent License requests per WebLM	300	
License requests during any 9 minute window per WebLM	50,000	
Local WebLM	22	
Trust management clients	2,500	
Tenants (System Manager Multi-Tenant)	250	

Geographic Redundancy

The System Manager Geographic Redundancy service replicates Avaya Aura® application support for two geographically distant System Manager sites with separate subnetworks and across a WAN. You can change the System Manager management services from one site to another when one of the sites or servers fails. System Manager Geographic Redundancy sites are set up in pairs. From the server pair, one server is designated as the primary System Manager server and the other server as the secondary System Manager server.

Chapter 7: Security

Security specification

As the management console for some Avaya products, System Manager must be resilient to attacks that might cause service disruption, malfunction, or unauthorized access to data. As a part of the Avaya Aura® solution, System Manager must be protected from security threats, such as:

- Unauthorized access or modification of data
- Theft of data
- Denial of Service (DoS) attacks
- Viruses and Worms
- Web-based attacks that include Cross-Site Scripting and Cross-Site Forgery

For information about security-related considerations, features, and services for System Manager, see *Avaya Aura® System Manager Security Design* on the Avaya Support website at https://support.avaya.com/security.

Related links

Trust Management on page 52

Trust Management

System Manager uses Trust Management to provision and manage certificates of various applications, servers, and devices thereby enabling a secure, inter-element communication. Trust Management provides Identity (Server) and Trusted (Root/CA) certificates that applications can use to establish mutually authenticated TLS sessions.

System Manager uses a third-party open source application as a Certificate Authority, Enterprise Java Beans Certificate Authority (EJBCA), to issue Identity and Trusted certificates to applications through Simple Certificate Enrollment Protocol (SCEP).

For information about getting the endpoint certificates, see the endpoint specific documentation on the Avaya Support website.

Related links

Security specification on page 52

External authentication

You can configure System Manager to authenticate administrative users through external authentication services, such as an enterprise directory, Kerberos, or a RADIUS server. An administrative account is provisioned within System Manager during installation for initial access.

System Manager supports the following authentication authorities:

- Local users
- External RADIUS users
- External LDAP users
- External Security Assertion Markup Language (SAML) users

The authentication scheme policy determines the order in which you can use the authentication authorities. The authentication servers policy controls the settings for the external SAML, LDAP, RADIUS, and KERBEROS servers.

Related links

SAML authentication on page 53

SAML authentication

For enterprise level Single Sign On, System Manager provides Security Assertion Markup Language (SAML) authentication. System Manager uses SAML implementation version 2.0 of OpenAM Release 9.5.4 to provide SAML-based authentication with external Identity Providers. System Manager uses the web browser Single Sign On profile of the SAML authentication.

Related links

External authentication on page 53

Role Based Access Control

In System Manager, you require appropriate permissions to perform a task. The administrator grants permissions to users by assigning appropriate roles. Role Based Access Control (RBAC) in System Manager supports the following types of roles:

- Built-in
- Custom

With these roles, you can gain access to various elements with specific permission mappings.

Built-in roles are default roles that authorize users to perform common administrative tasks. You can assign built-in roles to users, but you cannot delete roles or change permission mappings in the built-in roles.

You can perform LDAP synchronization of Microsoft Active Directory or other supported directory server administrator roles with System Manager administrator roles. The capability includes system roles and custom roles on System Manager.

Note:

Granular RBAC is not supported for managing Avaya Meetings Server, Web Gateway, and Work Assignment elements by creating custom roles.

Certificate revocation list overview

In simple terms, a Certificate Revocation List (CRL) is a type of blocklist of digital certificates that Certificate Authority organizations (CAs) deem as untrustworthy or that they are no longer willing to vouch for. It is a list of digital certificates that have been revoked by the issuing CA.

From release 10.2.1.1 and later, Avaya Aura® supports HTTP proxy to download CRLs. CRL download using a proxy eliminates the requirement for a direct connection to the Certificate Authority (CA), which can be a security risk.

This release supports the HTTP proxy type with basic authentication, which requires a username and password. Alternatively, customers can configure proxy support without authentication. Customers can configure up to three proxies as a maximum at any time.

Customers can configure the frequency with which Avaya Aura® checks for updates to CRLs and downloads a new CRL. To enable this functionality, customers can configure a CRL download job.

System Manager and Session Manager use these configuration settings in tandem. So, it is important to understand the implications of these settings for Session Manager.

Session Manager uses the HTTP proxy settings for both CRL download and Push Notification. The new feature for HTTP proxy overrides any configuration on the Global Settings for Session Manager. Session Manager uses HTTP proxy configurations in priority order, as they appear on the HTTP Proxy screen. For more information, see *Administering Avaya Aura® Session Manager*.

Chapter 8: Resources

System Manager documentation

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

Title	Description	Audience
Design		
Avaya Aura® System Manager Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Administering Avaya Aura® System Manager	Administering System Manager applications and install patches on System Manager applications.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Certificate Management	Understand certificate management.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Data Privacy Guidelines	Describes how to administer System Manager to fulfill Data Privacy requirements.	System administrators and IT personnel
Using		
Using the Solution Deployment Manager client	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Implementation		
Upgrading Avaya Aura® System Manager	Upgrade Avaya Aura® System Manager.	Implementation personnel
Deploying Avaya Aura® System Manager in Virtualized Environment	Deploy System Manager applications in Virtualized Environment.	Implementation personnel

Table continues…

Title	Description	Audience
Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments	Deploy System Manager applications in Software-Only and Infrastructure as a Service environments.	Implementation personnel
Maintenance and Troubleshooting		
Avaya Aura® System Manager SNMP Whitepaper	Monitor System Manager using SNMP.	System administrators and IT personnel
Troubleshooting Avaya Aura® System Manager	Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators and IT personnel

Finding documents on the Avaya Support website

Procedure

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

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

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

Accessing the port matrix document

Procedure

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

This field is not available if there is only one release for the product.

5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

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

Important:

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

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

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

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

You can do the following:

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

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

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After you login to the website, enter the course code or the title in the **Search** field and click **Go** to search for the course.

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 59

Using the Avaya InSite Knowledge Base

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

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

- Links to other pertinent information.

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

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

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

Related links

Support on page 59

Glossary

Elements	An element is an instance of an Avaya Aura® network entity managed by System Manager, for example, a Session Manager server or a Communication Manager server.
Geographic Redundancy-aware element	An element that supports Geographic Redundancy, such as Avaya Aura® Session Manager Release 6.3.
Geographic Redundancy-unaware element	An element that does not support Geographic Redundancy, such as Avaya Aura® Session Manager release earlier than 6.3.
Primary System Manager server	The first or the master System Manager server in a Geographic Redundancy setup that serves all system management requests.
Secondary System Manager server	The System Manager server that functions as a backup to the primary System Manager server in a Geographic Redundancy setup. The secondary System Manager server provides the full System Manager functionality when the system fails to connect to the primary System Manager server.

Index

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X