AVAYA

What is New in Avaya Aura® Release 10.2.x

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

Introduction

Purpose

This document provides an overview of the new and enhanced features of Avaya Aura® Release 10.2.x components.

This document is intended for the following audience:

- Contractors
- Employees
- Channel associates
- Remote support
- Sales representatives
- Sales support
- On-site support
- Avaya Business Partners

Avaya Aura® Release 10.2.x components

Product component	Release version
System Manager	10.2.x
WebLM	10.1.3.x
Session Manager	10.2.x
Communication Manager	10.2.x
Branch Gateway	10.2.x
Presence Services	10.1.x
Application Enablement Services	10.2.x
AXP On-Prem	10.2.x
Media Server	10.2.x
Avaya Aura® Device Services	10.2.x

From Release 10.2 and later, Avaya Aura® does not support Avaya Device Adapter Snap-in.

Product compatibility

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

Technical Assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with feature administration and system applications, call the Avaya Technical Consulting and System Support (TC-SS) at 1-800-225-7585.

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Change history

Issue	Date	Summary of changes
7	May 2025	Updated the following section: • Topology on page 10
6	April 2025	Added the following sections for R10.2.1.1: • New in System Manager Release 10.2.1.1 on page 31 • New in Session Manager Release 10.2.1.1 on page 36 • New in Communication Manager Release 10.2.1.1 on page 42 • New in Avaya Aura Device Services Release 10.2.1.1 on page 54 Updated the following sections for Release 10.2.1.1: • Supported ESXi version on page 25 • System Manager feature matrix on page 33 • Session Manager feature matrix on page 39 • Communication Manager feature matrix on page 45
5	March 2025	Updated the product name from "Avaya Cloud Office" to "Avaya Cloud Office Hybrid"

Table continues…

What is New in Avaya Aura® Release 10.2.x

Issue	Date	Summary of changes
4	December 2024	Added the following sections for Release 10.2.1: • New in System Manager Release 10.2.1 on page 31 • New in Session Manager Release 10.2.1 on page 36 • New in Communication Manager Release 10.2.1 on page 43 • New in Application Enablement Services Release 10.2.1 on page 49 • New in Avaya Aura Device Services Release 10.2.1 on page 54 • Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 26 Updated the following sections for Release 10.2.1: • System Manager feature matrix on page 33 • Session Manager feature matrix on page 39 • Communication Manager feature matrix on page 45 • Software-only environment overview on page 13 • Avaya Aura applications upgrade on page 23 • Supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura application OVAs on page 23 • Solution Deployment Manager overview on page 18 • Solution Deployment Manager Client on page 19
3	May 2024	Updated the section: Software-only environment overview on page 13
2	April 2024	Updated the section Avaya Aura applications deployment offers on page 9
1	December 2023	Release 10.2

Chapter 2: Overview

Avaya Aura® overview

Avaya Aura® is a flagship communications solution that uses an IP and SIP-based architecture to unify media, modes, networks, devices, applications, and real-time, actionable presence across a common infrastructure. This architecture provides on-demand access to advanced collaboration services and applications that improve employee efficiency. Avaya Aura® is available under Core or Power Suite Licenses. Each suite provides a customized set of capabilities designed to meet the needs of different kinds of users. Customers might mix Core and Power licenses on a single system based on their needs.

The following are some of the capabilities that the Avaya Aura® solution provides:

- Support for up to 28 instances of Session Manager and 300,000 users and 1 million devices
- Support for up to 18,000 simultaneously registered H.323 endpoints out of 41,000 endpoints per single Communication Manager server and SIP endpoints in an enterprise
- Advanced Session Management Capabilities
- Converged voice and video call admission control
- SIP features, including E911, which reports the desk location of the caller

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), Avaya Solutions Platform S8300 (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 Environment:

- Avaya Solutions Platform 130 Release 5.1 (Dell PowerEdge R640) is a single host server with preinstalled ESXi 7.0 Standard VMware License.

- Avaya Solutions Platform S8300 with a preinstalled ESXi 7.0 Foundation License for Communication Manager and Branch Session Manager.

- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660) is a single host server with 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 customer-provided Virtualized Environment.

✱ **Note:**

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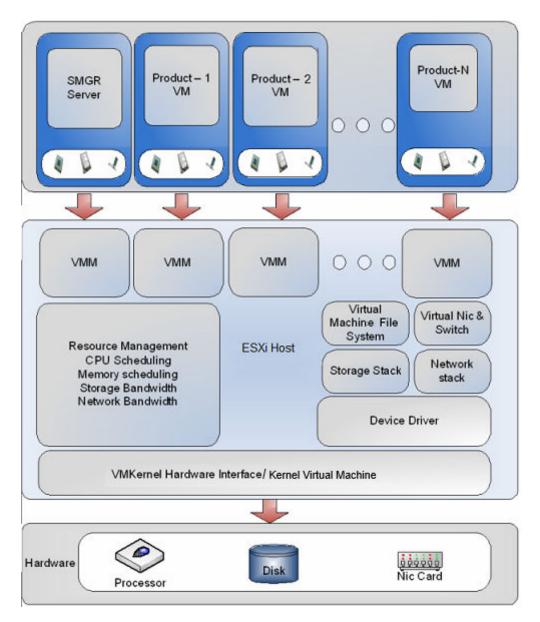
Supported applications in Virtualized Environment

- 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) or Avaya Solutions Platform S8300	
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 or Avaya Solutions Platform S8300.

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 for monitoring and administering 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.

Avaya Communication Manager Security Service Packs (SSP) can be incompatible or fail to install on a customer controlled operating system.

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

Supported third-party applications

With the software-only (ISO) offer, you can install third-party applications on the system. For the list of supported third-party software applications in Release 10.1 and later, see Avaya Product Support Notices.

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.

With Release 10.1 and later, there are no separate Kernel Service Packs (KSP), and Linux Security Update (LSU).

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.

> **✳ Note:**
>
> Branch Session Manager is not supported on Amazon Web Services, Google Cloud Platform, and Microsoft Azure.

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.

The Infrastructure as a Service environment supports the following offers:

Offer	Supported environments
ISO	Simplex • Amazon Web Services • Microsoft Azure • Google Cloud Platform • IBM Cloud for VMware Solutions Duplex • Amazon Web Services • Microsoft Azure • Google Cloud Platform • IBM Cloud for VMware Solutions

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.

Avaya Communication Manager Security Service Packs (SSP) can be incompatible or fail to install on a customer controlled operating system.

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

Supported third-party applications

With the software-only (ISO) offer, you can install third-party applications on the system. For the list of supported third-party software applications in Release 10.1 and later, see Avaya Product Support Notices.

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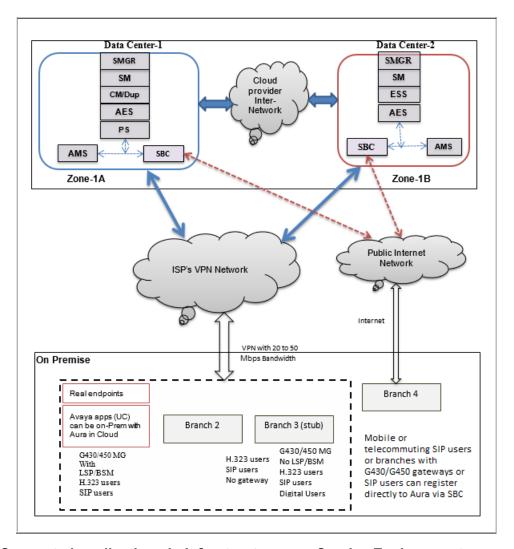
For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

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
Presence Services using Avaya Breeze® platform	Release 10.1.x	Y	—	—

Table continues…

Application	Release	Amazon Web Services	Microsoft Azure	Google Cloud Platform
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.

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*.

Related links

[Solution Deployment Manager Client](#) on page 19

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.
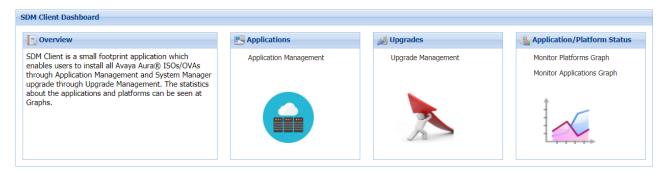

Figure 1: Solution Deployment Manager Client dashboard

Related links

[Solution Deployment Manager overview](#) on page 18

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)
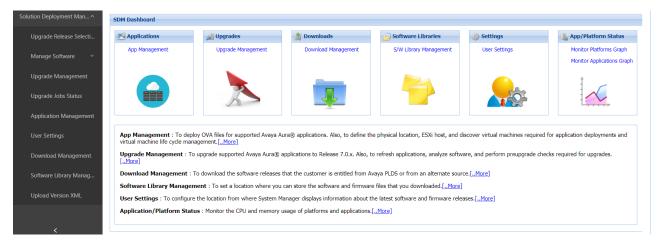- WebLM Release 7.x and later

> ✳ **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.

Avaya Aura® applications upgrade

With System Manager Solution Deployment Manager, you can upgrade the following Avaya Aura® applications to Release 10.2.x:

- Communication Manager
- Session Manager
- Branch Session Manager

 Note:

- You must upgrade System Manager to Release 10.2.x by using the Solution Deployment Manager client before you upgrade the Avaya Aura® applications to Release 10.2.x.
- When an application is deployed on a KVM host, Solution Deployment Manager does not support that application.

Supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura® application OVAs

The following table lists the supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura® application OVAs.

Red Hat Enterprise Linux operating system	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
Linux operating system Release 6.5 with 64-bit					
Linux operating system Release 7.2 with 64-bit	Y **Note:** Utility Services Release 7.1 uses the Red Hat Enterprise Linux operating system Release 7.3 with 64-bit.				

Table continues…

Red Hat Enterprise Linux operating system	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
Linux operating system Release 7.4 with 64-bit		Y ⚹ **Note:** System Manager Release 8.0.x only supports the Red Hat Enterprise Linux operating system Release 7.5 with 64-bit.			
Linux operating system Release 7.6 with 64-bit			Y		
Linux operating system Release 8.4 with 64-bit				Y	Y
Linux operating system Release 8.10 with 64 bit					Y (R10.2.1 onwards)

Supported Red Hat Enterprise Linux operating system versions for Software-only Environment

The following table lists the supported Red Hat Enterprise Linux operating system versions for deploying or upgrading Avaya Aura® applications in Software-only Environment.

Red Hat Enterprise Linux operating system	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
Linux operating system Release 7.4 with 64-bit			

Table continues…

Red Hat Enterprise Linux operating system	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
Linux operating system Release 7.6 with 64-bit	Y ✱ Note: Session Manager Release 8.1.1 and later support the Red Hat Enterprise Linux operating system Release 7.6 through 7.9 with 64-bit.		
Linux operating system Release 8.4 with 64-bit		Y	Y
Linux operating system Release 8.10 with 64 bit			Y

Supported ESXi version

The following table lists the supported ESXi versions of Avaya Aura® applications:

ESXi version	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
ESXi 5.0	N	N	N	N	N
ESXi 5.1	N	N	N	N	N
ESXi 5.5	Y	N	N	N	N
ESXi 6.0	Y	Y	Y	N	N
ESXi 6.5	Y	Y	Y	N	N
ESXi 6.7	N	Y	Y	Y	N
ESXi 7.0	N	N	Starting from Release 8.1.3: Y	Y	Y
ESXi 8.0	N	N	N	N	Y

✱ **Note:**

- Avaya Solutions Platform 130 Appliance and Avaya Solutions Platform S8300 R6.0 supports Avaya-supplied KVM on RHEL 8.10. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell or RHEL website, this results in an unsupported configuration.

- Avaya Aura® Release 10.2.x supports VMware 8.0, VMware 8.0 Update 2, and VMware 8.0 Update 3.

Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the Broadcom website (formerly VMware).

- As of October 15, 2022, VMware has ended support for VMware vSphere 6.x. Therefore, it is recommended to upgrade to supported vSphere versions.

For customer-provided environments and how to upgrade to supported vSphere version, see the VMware website.

- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.

- From VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.

- Avaya Aura® applications support the particular ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 7.0 can be VMware ESXi 7.0 Update 3.

- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0, ESXi 8.0 Update 2 (U2) deployments, and ESXi 8.0 Update 3 (U3) deployments.

Supported ASP R6.0.x (KVM on RHEL 8.10) version

The following table lists the supported KVM versions of Avaya Aura® applications:

Avaya Solutions Platform (KVM on RHEL 8.10)	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
KVM Release 8.10	Y	Y Not supported for Session Manager Not supported for System Manager	Y

✳ **Note:**

- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x are Avaya-supplied KVM on RHEL 8.10. The Avaya Solutions Platform 130 can be either a Dell R660 or Dell R640. The Dell R660 only ships with and supports KVM on RHEL 8.10. The initial Release of Avaya Solutions Platform 130 Release 4.0 supported Avaya-supplied ESXi 6.5 and Avaya Solutions Platform 130/S8300 R5.x supported Avaya-supplied ESXi 7.0.

- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x software is KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R660 server only supports

KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R640 and the ASP S8300 S8300E support both ESXi 7.0 and KVM on RHEL 8.10. Avaya Solutions Platform 130 Dell R640 Release 4.0 supported ESXi 6.5

- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660) is a single host server with 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.

- Avaya Solutions Platform130 Release 6.0.x (Dell PowerEdge R640, R660, S8300E) is a single host server with preinstalled KVM on RHEL R8.10 software.

- With the introduction of Avaya Solutions Platform R6.0.x there is no longer a specific license key needed as was present with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Supported servers for Avaya Aura® applications

The following table lists the Avaya sourced supported servers for the Avaya Aura® applications:

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
S8300D	Y	N	N	N	N
S8300E[1]	Y	Y	Y	Y	Y
HP ProLiant DL360 G7 (CSR1)	Y	N	N	N	N
HP ProLiant DL360p G8 (CSR2)	Y	Y	Y	N	N
HP ProLiant DL360 G9 (CSR3)	Y	Y	Y	N	N
Dell™ PowerEdge™ R610 (CSR1)	Y	N	N	N	N
Dell™ PowerEdge™ R620 (CSR2)	Y	Y	Y	N	N
Dell™ PowerEdge™ R630 (CSR3)	Y	Y	Y	N	N
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 [2]	N	Y	Y	N	N

Table continues…

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 and R660 [3]	N	Y	Y Avaya Solutions Platform 130 Release 5.x/6.x	Y Avaya Solutions Platform 130 Release 5.x/6.x	Y Avaya Solutions Platform 130 Release 5.1/6.x
Avaya Solutions Platform S8300 [4]	N	N	N	Y Release 5.1	Y Release 5.1/6.x

[1] You can migrate the S8300E server to Avaya Solutions Platform S8300 Release 6.x. For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300* on the Avaya Support website.

[2] Avaya Solutions Platform 120 Appliance uses Appliance Virtualization Platform to support virtualization.

[3] You can migrate the Avaya Solutions Platform 120 Appliance to Avaya Solutions Platform 130 Appliance Release 6.x. For information, see *Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130* on the Avaya Support website.

Avaya Solutions Platform 130 Appliance 5.1.x uses VMware vSphere ESXi software to support virtualization. Avaya Solutions Platform 130 Appliance 6.x uses KVM on RHEL software to support virtualization.

[4] Avaya Solutions Platform S8300 5.1.x supports virtualization using VMware vSphere ESXi foundation license for Communication Manager and Branch Session Manager. Avaya Solutions Platform S8300 6.x supports virtualization using KVM on RHEL 8.10 software.

Avaya Solutions Platform 130 Appliance R4/5 uses VMware vSphere ESXi Standard License to support virtualization

✱ **Note:**

- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.

- From Avaya Aura® Release 10.1 and later, Avaya-provided HP ProLiant DL360p G8, HP ProLiant DL360 G9, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, and Avaya Solutions Platform 120 servers are not supported.

  However, in Release 10.2.x, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 6.0.

- From Avaya Aura® Release 8.0 and later, S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers are not supported.

With the introduction of Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10), you no longer need a specific license key as was the case with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Supported gateways

The following table lists the supported gateways of Avaya Aura® applications.

Supported gateways	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
G430 Branch Gateway	Y	Y	Y	Y	Y
G450 Branch Gateway	Y	Y	Y	Y	Y
G650 Media Gateway	Y	Y	Y		

> ✱ **Note:**
>
> From Avaya Aura® Release 10.2 and later, G650 Media Gateway is no longer functional.

Supported browsers

The following table lists the minimum tested versions of the browsers for Avaya Aura® Release 10.2.x applications.

For information about older Avaya Aura® Release browser support, see the earlier version of this document.

Avaya Aura® Release	Avaya Aura® application and supported browsers			
	System Manager/ WebLM 10.1.2	Session Manager	AE Services	Communication Manager
10.2.x	• Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93	• Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93	• Mozilla Firefox Release 112 • Google Chrome Release 113 • Microsoft Edge Release 112	• Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93
10.1.x	• Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93	• Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93	• Mozilla Firefox Release 112 • Google Chrome Release 113 • Microsoft Edge Release 112	• Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93

Comments on this document?

> **Note:**
>
> - From June 2022, the Internet Explorer 11 is not supported. For more information, see the Microsoft website.
>
>   To access Avaya Aura® applications, move to other supported web browsers.
>
> - From Avaya Aura® Release 10.1 and later, Microsoft Internet Explorer is no longer supported.
>
> - Later versions of the browsers can be used. However, it is not explicitly tested.

JITC support

The following table lists the JITC support for Avaya Aura® Release 10.2.x applications.

Avaya Aura® Release	Avaya Aura® application				
	Communication Manager	Session Manager	System Manager	WebLM	AE Services
10.2	Y	Y	Y		Y
10.1.2 or 10.1.3					
10.1.0.2	Y	Y	Y	NA	N
10.1.0.1					
10.1					

> **Note:**
>
> In Release 10.1.0.2, Communication Manager, System Manager, Session Manager, and G4xx are JITC compliant and are the currently certified solution on the DoDIN APL. As per the latest DISA STIG requirements, RHEL 8.4 is also tested for JITC certification.

Discontinued support for IP Server Interface (TN2312, commonly known as "IPSI")

With Release 10.2, Communication Manager does not support the IP Server Interface (IPSI). As a result, access and functionality are removed. This means, the IPSI connected cabinets and gateways do not work with Communication Manager Release 10.2. Examples of IPSI connected cabinets and systems include G3cfs, G3csi, G3i, G3r, G3s, G3si, G3vs, G3x, G600, G650, MCC, SCC, CMC, IPSI, IP Server Interface, and IP port network.

Discontinued support also includes the TN8412, which previously paired with the TN8400 blade server. TN8412 was last supported with Communication Manager Release 5.x.

For more information, see the [End of sale G650 document](#) published on the Avaya Support website.

Discontinued support for Avaya Device Adapter Snap-in

From Release 10.2 and later, Avaya Aura® does not support Avaya Device Adapter Snap-in.

Chapter 3: System Manager

What's new in System Manager

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

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

New in this release

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.

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
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

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x	Release 10.2.x
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
Emergency Location Management Solution			Y	Y	Y
Support for TLS 1.3				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 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)

Chapter 4: Session Manager

What's new in Session Manager

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

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

New in this release

New in Session Manager Release 10.2.1.1

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

HTTP proxy

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

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

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

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

New in Session Manager Release 10.2.1

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

Avaya Aura® X for Zoom Workplace

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

count. Enable Avaya Aura® X for Zoom Workplace feature through the System Manager web console. For more information about enabling Avaya Aura® X for Zoom Workplace feature, see *Administering Avaya Aura® Session Manager*.

Avaya Cloud Office Hybrid

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

Support for System Manager Web Services implicit user roles

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

Support for Software-Only Deployment on Nutanix Environment

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

Red Hat Enterprise Linux (RHEL) 8.10 support

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

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

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

New in Session Manager Release 10.2

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

Enhancement to the patchSM command with the --snapshot option

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

Support of the vmsnapshot command

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

Edge friendly branch survivability

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

With Avaya Aura® 10.2, the migration to cloud is made more easier by allowing the survivable components, SRS and Branch Session Manager, in the G4xx media gateways to connect to

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

With Release 10.2:

- To deploy the edge Branch Session Manager set up in a virtualized environment, a new **Edge Topology BSM** option is added in the Branch Session Manager Settings section.

- To configure the edge Branch Session Manager server, a new `edgeSetup` command is added.

- To enable edge topology for core Session Manager and edge Branch Session Manager on the **Elements** > **Session Manager** > **Global Settings** page, the **Enable Edge Topology** check box is added.

- To create core Session Manager and edge Branch Session Manager SIP entities on the **Elements** > **Routing** > **SIP Entities** page, the **Network Topology**, **SBC Public IP Address or FQDN**, and **SBC Private IP Address or FQDN** fields are added.

- To display the core Session Manager and edge Branch Session Manager SIP entities configuration on the Session Manager Dashboard page, a new **Topology** column is added.

- To add an edge Branch Session Manager instance on the **Elements** > **Session Manager** > **Session Manager Administration** > **Branch Session Manager Instances** page, when you select the edge Branch Session Manager SIP entity, Session Manager:

  - Renames the **Management Access Point FQDN/IP** field to **Management Access Point FQDN**.

  - Displays the **Network Topology** and **Remote Access Configuration** fields.

Enhancement to the Remote Access Configuration page

With Release 10.2, on the Remote Access Configuration page:

- A new **SIP Proxy Public FQDN (Reference A)** column is added in SIP Proxy Mapping Table.

- If **Enable Edge Topology** is enabled on the Global Settings page, the system displays the **Translate Address** column in SIP Proxy Private IP Addresses.

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

Support of Stir/Shaken message normalization and adaptation module

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

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

With Release 10.2, you can configure the following:

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

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

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

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

Support for VMware 8.0

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

Session Manager feature matrix

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

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x	Release 10.2.x
OVA signing	Y	Y	Y	Y	Y
IPv6 support	Y	Y	Y	Y	Y
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y	Y
Compliance with DISA security STIGs	Y	Y	Y	Y (R 10.1.0.2 onwards)	Y
Extended Security Hardening	Y	Y	Y	Y	Y
Conference factory URI	Y	Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y	Y
Customer Root Access		Y	Y	Y	Y
Preserve security hardening modes on upgrade		Y	Y	Y	Y
SIP Resiliency		Y	Y	Y	Y
Extended host name validation		Y	Y	Y	Y
Cassandra clustering	Y	Y	Y	Y	Y

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 Software-only deployment		Y	Y	Y	Y
Support for 16 digit dial plan		Y	Y	Y	Y
Support for Hyper-V in Software-Only environment		Y	Y	Y	Y
Support for Regular Expression based adaptation module		Y	Y	Y	Y
Support for Call Journaling Server High Availability		Y	Y	Y	Y
Cassandra security hardening		Y	Y	Y	Y
Support for multiple customer accounts		Y	Y	Y	Y
Support for role-based access control		Y	Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance		Y	Y		
Support for Avaya Solutions Platform 130 Appliance		Y	Y	Y	Y
Syslog server configuration			Y	Y	Y
Data Encryption			Y	Y	Y
Branch Visiting User			Y	Y	Y
Apple Push notification			Y	Y	Y
Support for VMware ESXi 7.0			Y	Y	Y
Policy-based Assignment of Users to Session Manager				Y	Y
Registration of SIP Clients to four Session Managers				Y	Y
Support for TLS 1.3				Y	Y
Android Push notification				Y	Y

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 Red Hat Enterprise Linux (RHEL) 8.4				Y	Y
Support for Red Hat Enterprise Linux (RHEL) 8.10					Y (R 10.2.1 onwards)
Avaya Solutions Platform S8300 for Branch Session Manager				Y	Y
Support for VMware ESXi 8.0					Y
Support for Edge friendly branch survivability					Y
Support of Stir/ Shaken message normalization and adaptation module					Y
Support of Avaya Aura® X for Zoom Workplace				Y	Y
Support of Avaya Cloud Office Hybrid					Y
Support for Avaya Solutions Platform S8300 Release 5.x				Y	Y
Support for Avaya Solutions Platform S8300 Release 6.0.x			Y	Y	Y
Support for Avaya Solutions Platform 130 Release 5.x			Y	Y	Y
Support for Avaya Solutions Platform 130 Release 6.0.x			Y	Y	Y
Support for HTTP Proxy					Y R10.2.1.1 onwards

Chapter 5: Communication Manager

What's new in Communication Manager

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

For more information about these features and administration, see:

- *Avaya Aura® Communication Manager Feature Description and Implementation*
- *Avaya Aura® Communication Manager Screen Reference*

New in this release

New in Communication Manager Release 10.2.1.1

With Release 10.2.1.1, Avaya Aura® Communication Manager supports the following new enhancements:

Enhancement to Communication Manager License Expiration

With Release 10.2.1.1, Communication Manager is changing its licensing behavior to keep customers informed about license expiration dates so they can renew licenses on time and avoid service disruption. Communication Manager is introducing two new alarms that warns customers about license expiration date and its impact:

- LIC-EXP90: This alarm is raised 90 days before the expiration of Communication Manager license.
- LIC-EXP60: This alarm is raised 60 days before the expiration of Communication Manager License.

The Communication Manager enters into a 30-day Grace Period on expiration of License. After 30-day grace period expiry, if license is not renewed:

- Call Processing, including Emergency calling, will be blocked. That is, Communication Manager will not process any type of calls.
- System Administration will be blocked.

Customer must renew their licenses on time to avoid this disruption.

This feature enhancement is applicable only for main Communication Manager and not for Local Survivable Processor (LSP) and Enterprise Survivable Server (ESS).

Enhancement to Survivable License Grace Period

With Release 10.2.1.1, Communication Manager supports configurable Survivable License Grace Period for the Enterprise Survivable Server (ESS). This field is applicable only for ESS, and not for LSP.

New in Communication Manager Release 10.2.1

With Release 10.2.1, Avaya Aura® Communication Manager supports the following new features and enhancements:

Red Hat Enterprise Linux (RHEL) 8.10 support

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

Support for Software-Only Deployment on Nutanix Environment

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

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

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

Optional upgrade sequence

An alternate upgrade sequence that allows you to upgrade your core Communication Manager before you upgrade your Survivable Remote Servers, formerly known as Local Survivable Processors (LSP). While you use the latest features from the core Communication Manager, you can continue to upgrade your Survivable Remote Servers (LSP) to the same or a higher software version than your core Communication Manager. This sequence of upgrading has a limitation of configurations not synchronizing between the upgraded core Communication Manager and yet-to-be-upgraded Survivable Remote servers (LSP).

Ensure to read the complete details of the Optional Upgrade Sequence feature before you implement this upgrade sequence. For more information, see *Upgrading Avaya Aura® Communication Manager*

New in Communication Manager Release 10.2

With Release 10.2, Avaya Aura® Communication Manager 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 Trellix AV (formerly known as McAfee) in Virtualized Deployments

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

AV on Avaya Aura®, see *Application Note for Support of Trellix AV on Avaya Aura®* on the Avaya Support website at https://support.avaya.com.

Support for J139, J159, J189, and J189CC endpoints

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

To administer these endpoints, use System Manager.

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

Edge Friendly Branch Survivability

In the previous Avaya Aura® Release 10.1, support for Edge Friendly Branch Survivability feature was introduced, which made it easier to have seamless connections between your on-premise G4xx Gateways and the Core Communication Manager hosted on the Cloud. Avaya designed this innovation to protect your investments, especially when you are considering a shift to a Cloud-based infrastructure.

With Avaya Aura® Release 10.2, migrating to the Cloud is even more streamlined. You can now configure edge topology for Cloud deployment. Survivable components like Local Survivability Processor (LSP) and Branch Session Manager (BSM) within G4xx Gateways can connect to Core Communication Manager and Session Manager on the Cloud. This connection between Gateways and Cloud can be established over the Internet or through SD-WAN, providing significant advantages in terms of Total Cost of Ownership (TCO).

To configure LSP topology to edge, do the following:

- Download TLS certificates to the new **Edge Topology (E)** repository. The certificates are required to set up a new WebSocket connection between the main Communication Manager and the Communication Manager LSP.

- On the Communication Manager SMI, go to **Administration** > **Server (Maintenance)** > **Server Configuration** > **Server Role** page and configure the **LSP Topology Configuration** section.

- On the main Communication Manager SAT, go to the change survivable-processor screen and do the following:

  - Configure the LSP topology as "Edge".

  - In the **Serial Number** field, enter the serial number of Communication Manager LSP.

Line Load Control (LLC) feature enhancement

In previous releases, you must configure LLC using System Manager or Communication Manager SAT only, but now you can easily configure LLC using Feature Access Codes.

Avaya Aura® Release 10.2 enhances the LLC feature for enhanced security. It provides an option to implement two-factor authentication for LLC setup, requiring the entry of a security code, which strengthens the security process.

In Avaya Aura® Release 10.2, you can limit the scope of LLC at the site level of your organization. It means that LLC can be applied selectively, exclusively to users of your organization associated with the site from which you initiated the LLC. It offers a more precise and site-specific approach to LLC deployment, enhancing the flexibility and control over LLC configurations.

Support to record the call originated from bridged line appearances

Communication Manager's Bridged Appearance feature is a widely used feature in both Unified Communications (UC) and Contact Center (CC) environments. In previous releases, a call originated using bridged appearance in a SIP environment was never recorded. This gap is addressed in this current release.

With Release 10.2, Avaya Aura® sends the required events for recording over Adjunct Switch Applications Interface (ASAI) when the call is initiated using Bridged Appearance.

Mask CLI and Station Name support on SIP

In Release 10.2, Avaya Aura® further enhances its functionality by extending the capability to mask the calling party number and name on outgoing calls. You can achieve this functionality using the **send-nn** button on SIP Phones. This feature enables your organization to keep the caller's identity confidential, thus enabling the implementation of a standardized approach for callback interactions.

Alerting internal users with a tone during external communications

In Release 10.2, Avaya Aura® introduces a security enhancement that notifies internal users with an audible tone when they are communicating with external parties. This unique tone is heard only by internal users. You can adjust the time interval between these tones through the System-Parameter Features form. Additionally, you can apply this feature to selective trunk groups, ensuring it operates only on the configured trunk groups.

STIR/Shaken support for verification level display on phones

STIR/Shaken is a set of protocols designed to counter caller ID spoofing on public telephone networks. Avaya Aura® Release 10.2 supports STIR/Shaken and enables the display of the attestation or verification level set by service providers on user or agent phones. This feature works exclusively over SIP trunks. You can enable or disable this feature at the Avaya Aura® solution level based on your preferences.

New field added to the Coverage path page

With Release 10.2, the **Description** field is added to Coverage path page. You can use the **Description** field to specify a name for a coverage path to distinguish the coverage paths.

Discontinued support of legacy technologies

Avaya Aura® Release 10.2 discontinued the following legacy technologies to reduce the risk to Business Continuity for customers:

- G650 or any cabinet/Gateway that connects to Communication Manager using IP Server Interface (IPSI) is no longer supported. For more information, see the End of sale G650 document published on the Avaya Support website.

- VMware ESXi version 6.7 or lower versions are not supported.

- Avaya Device Adapter Snap-in is no longer supported.

Communication Manager feature matrix

The following table lists the feature matrix of Communication 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, Release 8.1.1, and Release 8.1.2	Release 8.1.3	Release 10.1.x	Release 10.2.x
OVA signing	Y	Y	Y	Y	Y	Y
IPv6 support	Y	Y	Y	Y	Y	Y
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y	Y	Y
Compliance with DISA security STIGs	Y	Y	Y	Y	Y (R 10.1.0.2 onwards)	Y
Extended Security Hardening	Y	Y	Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y	Y	Y
Customer Root Access		Y	Y	Y	Y	Y
Preserve security hardening modes on upgrade		Y	Y	Y	Y	Y
SIP trunk optimization		Y	Y	Y	Y	Y
Automatic Call Distribution	Y	Y	Y	Y	Y	Y
Emergency Calling Services	Y	Y	Y	Y	Y	Y
Alphanumeric URI dialing	Y (R 7.1.2 onwards)	Y	Y	Y	Y	Y
Extended security hardening	Y (R 7.1.2 onwards)	Y	Y	Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1, Release 8.1.1, and Release 8.1.2	Release 8.1.3	Release 10.1.x	Release 10.2.x
Support for Avaya Solutions Platform 120 Appliance		Y	Y	Y		Y
Support for Avaya Solutions Platform 130 Appliance		Y	Y	Y	Y	Y
Support for J-Series phone migration				Y	Y	Y
Support for VMware ESXi 7.0				Y	Y	Y
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 (R 10.2.1 onwards)
Avaya Solutions Platform S8300					Y	Y
Optional Upgrade Sequence					Y	Y

Table continues…

What is New in Avaya Aura® Release 10.2.x
Comments on this document?

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1, Release 8.1.1, and Release 8.1.2	Release 8.1.3	Release 10.1.x	Release 10.2.x
License expiration (Blocking of call processing and system administration)						Y (R 10.2.1.1 onwards)

Chapter 6: Application Enablement Services

What's new in Application Enablement Services

This chapter provides an overview of the new and enhanced features of Application Enablement Services Release 10.2.x.

For more information about these features and administration, see:

- *Administering Avaya Aura® Application Enablement Services*
- *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment*
- *Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments*
- *Upgrading Avaya Aura® Application Enablement Services*

New in this release

New in Application Enablement Services Release 10.2.1

Avaya Aura® Application Enablement Services Release 10.2.1 supports the following new features and enhancements:

Support for Software-Only Deployment on Nutanix Environment

With Release 10.2, Application Enablement Services Software-Only application can be deployed on Nutanix 6.5 and later.

Red Hat Enterprise Linux 8.10 support

With Release 10.2.1, Application Enablement Services supports Red Hat Enterprise Linux Release 8.10.

Addition of a new SNMP alarm for AES

With Release 10.2.1, a new test alarm is added to the set of pre-existing alarms, to verify if the SNMP is correctly triggered.

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

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

New in Application Enablement Services Release 10.2

Avaya Aura® Application Enablement Services Release 10.2 supports the following new features and enhancements:

AE Services TSAPI Unencrypted Services port default changed

Earlier to Release 10.2, by default, both the Encrypted Services Port and Unencrypted Services Port were enabled.

With Release 10.2, by default, TSAPI Unencrypted Services Port is disabled and TSAPI Encrypted Services Port is enabled.

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 of Root EULA for AE Services OVA deployment

With Release 10.2, AE Services displays the:

- A new **ROOT ACCESS ACCEPTANCE STATEMENT** tab is added next to the existing **End User License Agreement** tab added to accept the root EULA on the **License Agreements** page when deploying the AE Services OVA by using the ESXi directly.

- A new **Eula Acceptance page** > **ROOT ACCESS ACCEPTANCE STATEMENT** subpage is added to the existing **AVAYA GLOBAL SOFTWARE LICENSE TERMS** subpage when deploying the AE Services OVA by using Solution Deployment Manager.

AE Services REST APIs (Web Telephony interface)

The Web Telephony interface (WTI) service was introduced in AE Services Release 10.1.2. In AE Services Release 10.2, all the existing APIs are included as follows:

- The existing DMCC recovery design is extended to the WTI service.
- WTI service provides APIs corresponding to all the APIs provided by DMCC.
- The WTI service supports a WebSocket interface, enabling access to all AES APIs and Events.

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.

Chapter 7: Branch Gateway

What's new in Branch Gateway

This chapter provides an overview of the new and enhanced features of Branch Gateway Release 10.2.x.

For more information about these features and administration, see:

- *Administering Avaya G430 Branch Gateway*
- *Administering Avaya G450 Branch Gateway*
- *Avaya G430 Branch Gateway CLI Reference*
- *Avaya G450 Branch Gateway CLI Reference*

New in this release

New in Branch Gateway Release 10.2

The following section describes new features and enhancements that are available in Branch Gateway 10.2.

TLS 1.3

With Release 10.2, Branch Gateway supports TLS 1.3.

Removed the ip license-server command

From Release 10.2, discontinued support for licensing of Communication Manager Release 5.2.1 and earlier, use Communication Manager Release 10.1.x and later with Branch Gateway Release 10.2.

New command in G430 Branch Gateway

Release 10.2 adds the following Command-line interface (CLI) command:

- **`snmp-server test trap`**: Command to send a test trap to configured destinations.

New commands in G450 Branch Gateway

Release 10.2 adds the following Command-line interface (CLI) commands to configure the Branch Gateway:

- **`snmp-server test trap`**: Command to send a test trap to configured destinations.
- **`set server-blade-monitoring`**: Command to control the heartbeat monitoring of an S8300 server in slot v1 and slot v5.

- **show server-blade-monitoring**: Command to display monitoring process of an S8300 server.
- **server-blade-vlan** - Command to set the main VLAN for the server in the selected slot.
- **show server-blade-vlan**: Command to display the server-blade-vlan.
- **server-blade-oob-vlan**: Command to set Out Of Band management VLAN for the server in the selected slot.
- **no server-blade-oob-vlan**: Command to clear the Out of Band management VLAN for a server in the selected slot.
- **show server-blade-oob-vlan**: Command to display the status of server-blade-vlan configured as the ICC Out of Band management interface.

Branch Gateway feature matrix

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

Feature name	Release 7.1.2 or 7.1.3	Release 8.0	Release 8.1.x	Release 10.1	Release 10.2.x
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y	Y
16-digit dial plan extension	N	Y	Y	Y	Y
Login authentication password complexity	N	Y	Y	Y	Y
Syslog over TLS	N	N	Y	Y	Y
Support of DC power supply forG450 Branch Gateway	N	N	Y	Y	Y
Edge Gateway mode	N	N	N	Y	Y
Support of TLS 1.3	N	N	N	N	Y

Chapter 8: CC Elite

What's new in AXP On-Prem

This chapter provides an overview of the new and enhanced features of AXP On-Prem Release 10.2.x.

New in AXP On-Prem Release 10.2

AXP On-Prem Release 10.2 supports the following features:

A combined total of eight communication links from Communication Manager to CMS, IQ and Work Assignment Engine servers is allowed.

Similar to previous versions, no more than two IQ servers can be configured and no more than two Work assignment Engines can be configured.

With no IQ server or Work Assignment engine links configured, eight CMS links can be configured on one Communication Manager.

Q-calls button is now configurable on J series UC endpoints: J169, J179 and J189.

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.

Chapter 9: Avaya Aura Device Services

What's new in Avaya Aura® Device Services

This chapter provides an overview of the new and enhanced features of Avaya Aura® Device Services Release 10.2.x.

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

Related links

New in Avaya Aura® Device Services Release 10.2.1.1

Avaya Aura® Device Services Release 10.2.1.1 supports the following new features and enhancements:

System Manager contacts filtration

With Release 10.2.1.1, Avaya Aura® Device Services restrict the display of contacts specific to System Manager upon searching the contacts.

HTTP Proxy support for client ID mapping

With Release 10.2.1.1, Avaya Aura® Device Services support HTTP Proxy configuration for client ID mapping.

Addition of a new ED signature for macOS

With Release 10.2.1.1, the Avaya Aura® Device Services support adding ED signature for macOS binary upload.

Related links

New in Avaya Aura® Device Services Release 10.2.1

Avaya Aura® Device Services Release 10.2.1 supports the following new features and enhancements:

Support for Software-Only Deployment on Nutanix Environment

With Release 10.2, Avaya Aura® Device Services Software-Only application can be deployed on Nutanix 6.5 and later.

Red Hat Enterprise Linux 8.10 support for Avaya Aura® Device Services

With Release 10.2.1, Avaya Aura® Device Services supports Red Hat Enterprise Linux Release 8.10.

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

With Release 10.2, Avaya Aura® Device Services can be deployed on Avaya-supplied KVM on RHEL Release 8.10 hypervisor (Avaya Solutions Platform 130 R6.0).

Keycloak with FIPS support

With Release 10.2.1 Avaya Aura® Device Services provide Keycloak with FIPS support.

Related links

New in Avaya Aura® Device Services Release 10.2.0.1

The following is a summary of changes in Release 10.2.0.1 of Avaya Aura® Device Services:

- Added support to a new Enterprise-Directory Type, ActiveDirectory_2022.
- Rollback to previous AADS version below 10.2.0.1 is not supported.

Related links

New in Avaya Aura® Device Services Release 10.2

The following is a summary of new functionalities added to Avaya Aura® Device Services in Release 10.2:

Enable/Disable logging

- Before Release 10.2, AADS supported extended logging at the system level only. With AADS Release 10.2, you can enable or disable logging at an individual user level.
- LOG_VERBOSITY property is added in the AADS dynamic configuration at a user level.

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.

Client ID configuration

Before Release 10.2, client ID used by J100 phones was hard-coded in AADS and couldn't be configurable. With Release 10.2, you can configure the client-id in AADS, which enables IAM to apply customer-specific requirements in the access token when the client authenticates.

Dynamic configuration for telecommuter number

Using AADS auto-config service API, the administrator can configure the telecommuter number and associate it with agents using Workplace. With this release, only one telecommuter number is supported.

Upgraded Keycloak version

Upgraded Keycloak version from Release 6.0.1 to Release 22.0.4.

Added MS Graph API support

AADS now supports MS Graph API as a replacement for MS Azure API, which Microsoft retired this year.

For more information on MS Graph API replacing MS Azure API, see PSN at https://download.avaya.com/css/public/documents/101086282 for details.

> ✳ **Note:**
>
> Microsoft announced EoS for Azure AD Graph API. MS Graph API will replace Azure AD Graph API.

Chapter 10: Resources

Resources

Documentation

The following table lists the documents related to the components of Avaya Aura® Release 10.2.x. Download the documents from the Avaya Support website at https://support.avaya.com.

Title	Description	Audience
Implementation		
Deploying Avaya Aura® System Manager in Virtualized Environment	Deploy the Avaya Aura® System Manager application in a virtualized environment.	Implementation personnel
Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments	Deploy the Avaya Aura® System Manager application in a software only and Infrastructure as a Service Environments	Implementation personnel
Upgrading Avaya Aura® System Manager	Upgrade the Avaya Aura® System Manager application.	System administrators and IT personnel
Deploying Avaya Aura® Communication Manager in Virtualized Environment	Describes the implementation instructions while deploying Communication Manager in virtualized environment.	Implementation personnel
Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments	Describes the implementation instructions while deploying Communication Manager in a software only and Infrastructure as a Service environments.	Implementation personnel
Upgrading Avaya Aura® Communication Manager	Describes instructions while upgrading Communication Manager.	System administrators and IT personnel
Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Implementation personnel

Table continues…

Comments on this document?

Title	Description	Audience
Deploying Avaya Aura® Session Manager in Software-Only and Infrastructure as a Service Environment	Describes how to deploy the Session Manager in a software only and Infrastructure as a Service environments.	Implementation personnel
Upgrading Avaya Aura® Session Manager	Provides common administration scenarios.	System administrators and IT personnel
Deploying Avaya Aura® Application Enablement Services in Virtualized Environment	Deploy Application Enablement Services applications in Virtualized Environment	Implementation personnel
Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments	Deploy Application Enablement Services applications in a software only and Infrastructure as a Service environments.	Implementation personnel
Upgrading Avaya Aura® Application Enablement Services	Upgrading Application Enablement Services applications.	System administrators and IT personnel
Administration		
Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network components of Communication Manager, such as gateways, trunks, FAX, modem, TTY, and Clear-Channel calls.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administering Avaya Aura® Communication Manager	Describes the procedures and screens used for administering Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administering Avaya Aura® System Manager	Describes the procedures for configuring System Manager Release 10.2.x and the Avaya Aura® applications and systems managed by System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Avaya Aura® Presence Services Snap-in Reference	Describes the steps to deploy and configure Presence Services.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Using		
Using the Solution Deployment Manager client	Deploy and install patches on Avaya Aura® applications.	System administrators
Understanding		

Table continues…

Title	Description	Audience
Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Avaya Aura® Communication Manager Screen Reference	Describes the screen and detailed field descriptions of Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administering Avaya Aura® Session Manager	Describes how to administer Session Manager by using System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware devices that can be incorporated in a Communication Manager telephony configuration.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Planning for Deploying Avaya Aura® applications	Provides planning information for deploying Avaya Aura® applications on supported platforms.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Planning for Upgrading Avaya Aura® applications	Provides planning information for upgrading Avaya Aura® applications on supported platforms.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Maintenance and Troubleshooting		
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers	Provides commands to monitor, test, and maintain hardware components of Avaya servers and gateways.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course 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

Table continues…

Course code	Course title
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.

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.

Appendix A: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) for any software update. For example, a PCN must accompany a service pack or an update that must be applied universally. Avaya issues a product-support notice (PSN) to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a work around for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at https://support.avaya.com and log in.

2. On the top of the page, in **Search Product**, type the product name.

   The Avaya Support website displays the product name.

3. Select the required product name.

4. In the **Choose Release** field, select the specific release from the drop-down list.

5. On the product page, click **Product Documents**.

6. In the Latest Support, Service and Product Correction Notices section, click **View All Notices**.

7. Select the appropriate filters as per your search requirement.

   For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new service packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to https://support.avaya.com and search for "Guide to Managing Your Avaya Access Profile for Customers and Partners".

   Under the Search Results section, click Guide to Managing Your Avaya Access Profile for Customers and Partners.

2. Set up e-notifications.

   For detailed information, see the **Subscribe to E-Notifications** procedure.

Index

Numerics

A

B

C

D

E

F

I

J

K

L

N

what's new *(continued)*

Comments on this document?