Whats New in Avaya Aura® Release 10.1.x

Release 10.1.x
Issue 16
August 2025

© 2022-2025, Avaya LLC
All Rights Reserved.

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 mediums which may include product information, 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. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“**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.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

Named User License (NU). End User may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below);

or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. 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

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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 for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction 8
Purpose 8
Avaya Aura® Release 10.1.x components 8
Product compatibility 9
Technical Assistance 9
Change history 9
Chapter 2: Avaya Aura® overview 13
Avaya Aura® applications deployment offers 13
Virtualized Environment overview 14
Software-only environment overview 16
Solution Deployment Manager overview 21
Solution Deployment Manager Client 22
Solution Deployment Manager 23
Avaya Aura® applications upgrade 26
Supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura® application OVAs 26
Supported Red Hat Enterprise Linux operating system versions for Software-only Environment 28
Supported ESXi version 29
Supported servers for Avaya Aura® applications 30
Supported gateways 32
Supported browsers 32
JITC support 33
Chapter 3: What's new in System Manager 34
New in this release 34
New in System Manager Release 10.1.3.3 34
New in System Manager Release 10.1.2 34
New in System Manager Release 10.1.0.2 35
New in System Manager Release 10.1.0.1 36
New in System Manager Release 10.1 37
System Manager feature matrix 40
Chapter 4: What's new in WebLM 42
New in this release 42
New in WebLM Release 10.1.2 42
WebLM feature matrix 44
Chapter 5: What's new in Session Manager 45
New in this release 45
New in Session Manager Release 10.1.3.4 45
New in Session Manager Release 10.1.3 45
New in Session Manager Release 10.1.2 45

New in Session Manager Release 10.1.0.2 46
New in Session Manager Release 10.1.0.1 46
New in Session Manager Release 10.1 46
Session Manager feature matrix 49
Chapter 6: What's new in Communication Manager 51
New in this release 51
New in Communication Manager Release 10.1.3.6 51
New in Communication Manager Release 10.1.3 52
New in Communication Manager Release 10.1.2 52
New in Communication Manager Release 10.1.0.2 53
New in Communication Manager Release 10.1 54
Communication Manager feature matrix 56
Chapter 7: What's new in Presence Services 59
New in this release 59
New in Presence Services Release 10.1 59
Presence Services feature matrix 60
Chapter 8: What's new in Application Enablement Services 62
New in this release 62
New in Application Enablement Services Release 10.1.3.1 62
New in Application Enablement Services Release 10.1.3 62
New in Application Enablement Services Release 10.1.2 63
New in Application Enablement Services Release 10.1.0.2 64
New in Application Enablement Services Release 10.1 64
Application Enablement Services feature matrix 66
Chapter 9: What's new in Branch Gateway 69
New in this release 69
New in Branch Gateway Release 10.1 69
Branch Gateway new features 73
Chapter 10: What's new in Avaya Aura® Media Server 74
New in Avaya Aura® Media Server 10.1.0 74
Chapter 11: What's new in Avaya Experience Platform™ On-Prem 75
New in Avaya Experience Platform™ On-Prem Release 10.1.2 75
New in Avaya Experience Platform™ On-Prem Release 10.1.0.2 75
New in Avaya Experience Platform™ On-Prem Release 10.1 76
Chapter 12: What's new in Avaya Device Adapter 77
New in this release 77
What's New in Avaya Device Adapter Release 10.1.2 77
What's new in Avaya Device Adapter Release 10.1 77
Avaya Device Adapter feature matrix 78
Chapter 13: Resources 87
Documentation 87
Training 89

Viewing Avaya Mentor videos..... 90
Support..... 90
Using the Avaya InSite Knowledge Base..... 91
Appendix A: PCN and PSN notifications..... 92
PCN and PSN notifications..... 92
Viewing PCNs and PSNs..... 92
Signing up for PCNs and PSNs..... 93

Chapter 1: Introduction

Purpose

This document provides an overview of the new and enhanced features of Avaya Aura® Release 10.1.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 10.1.x components

Product component	Release version
System Manager	10.1.x
WebLM	10.1.3.1
Session Manager	10.1.x
Communication Manager	10.1.x
Branch Gateway	10.1.x
Presence Services	10.1.x
Application Enablement Services	10.1.x
Avaya Experience Platform™ On-Prem	10.1.x
Device Adapter	10.1.x
Media Server	10.1.x

Product compatibility

For the latest and most accurate compatibility information, go to Product Compatibility Matrix.

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
16	August 2025	Updated the following section with a direct link to the Product Compatibility Matrix on Avaya Support site. • Product compatibility on page 9
15	June 2025	Added the section: New in Communication Manager Release 10.1.3.6 on page 51
14	October 2024	Added the section: New in Session Manager Release 10.1.3.4 on page 45
13	June 2024	Added the section: New in System Manager Release 10.1.3.3 on page 34
12	January 2024	Updated the section: Supported ESXi version on page 29.
11	August 2023	Added the section: New in Application Enablement Services Release 10.1.3.1 on page 62
10	July 2023	Updated the section: New in System Manager Release 10.1 on page 37

Table continues…

Issue	Date	Summary of changes
9	May 2023	For Release 10.1.3, added the following sections: • New in Session Manager Release 10.1.3 on page 45 • New in Communication Manager Release 10.1.3 on page 52 • New in Application Enablement Services Release 10.1.3 on page 62
8	February 2023	Added the section: JITC support on page 33
7	February 2023	For Release 10.1.2, added the following sections: • New in System Manager Release 10.1.2 on page 34 • New in WebLM Release 10.1.2 on page 42 • New in Session Manager Release 10.1.2 on page 45 • New in Communication Manager Release 10.1.2 on page 52 • New in Application Enablement Services Release 10.1.2 on page 63 • New in Avaya Experience Platform On-Prem Release 10.1.2 on page 75 • What's New in Avaya Device Adapter Release 10.1.2 on page 77 For Release 10.1.2, updated the following sections: • Avaya Aura Release 10.1.x components on page 8 • Supported applications in Virtualized Environment on page 14 • Supported applications in Software-only Environment on page 17 • Supported applications in Infrastructure as a Service Environment on page 20 • Supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura application OVAs on page 26 • Supported Red Hat Enterprise Linux operating system versions for Software-only Environment on page 28

Table continues…

Issue	Date	Summary of changes
6	September 2022	For Release 10.1.0.2, added the following sections: • New in System Manager Release 10.1.0.2 on page 35 • New in Session Manager Release 10.1.0.2 on page 46 • New in Communication Manager Release 10.1.0.2 on page 53 • New in Application Enablement Services Release 10.1.0.2 on page 64 • New in Avaya Experience Platform On-Prem Release 10.1.0.2 on page 75 For Release 10.1.0.2, updated the following sections: • System Manager feature matrix on page 40 • Session Manager feature matrix on page 49 • Communication Manager feature matrix on page 56
5	April 2022	For Release 10.1.0.1, added the following sections: • New in System Manager Release 10.1.0.1 on page 36 • New in Session Manager Release 10.1.0.1 on page 46 • New in Avaya Aura® Media Server 10.1.0 on page 74 Updated the following sections: • New in System Manager Release 10.1 on page 37 • New in Application Enablement Services Release 10.1 on page 64
4	March 2022	Updated the following sections: • Virtualized Environment overview on page 14 • Virtualized Environment components on page 15 • Solution Deployment Manager on page 23 • Supported servers for Avaya Aura applications on page 30 • New in Branch Gateway Release 10.1 on page 69
3	February 2022	Updated the following sections: • System Manager feature matrix on page 40 • Session Manager feature matrix on page 49 • Communication Manager feature matrix on page 56 • Presence Services feature matrix on page 60 • Application Enablement Services feature matrix on page 66 • Avaya Device Adapter feature matrix on page 78

Table continues…

Issue	Date	Summary of changes
2	January 2022	Updated the section: Communication Manager feature matrix on page 56
1	December 2021	Release 10.1 document.

Chapter 2: 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 Communication Server 1000 SIP networking and feature transparency
- Session Manager SIP routing adaptations
- A central management application, System Manager, for all Avaya Aura® applications and Avaya Communication Server 1000, with a single authentication

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

Virtualized Environment overview

You can deploy the Avaya Aura® Release 10.1.x applications in one of the following Virtualized Environment:

- Avaya Solutions Platform 130 Release 5.x (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.
- VMware in customer-provided Virtualized Environment.

Note:

With Release 10.1.x and later, Avaya Aura® will no longer have the KVM OVA. Deployment on KVM virtualized environment is supported through the Software-Only offer.

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

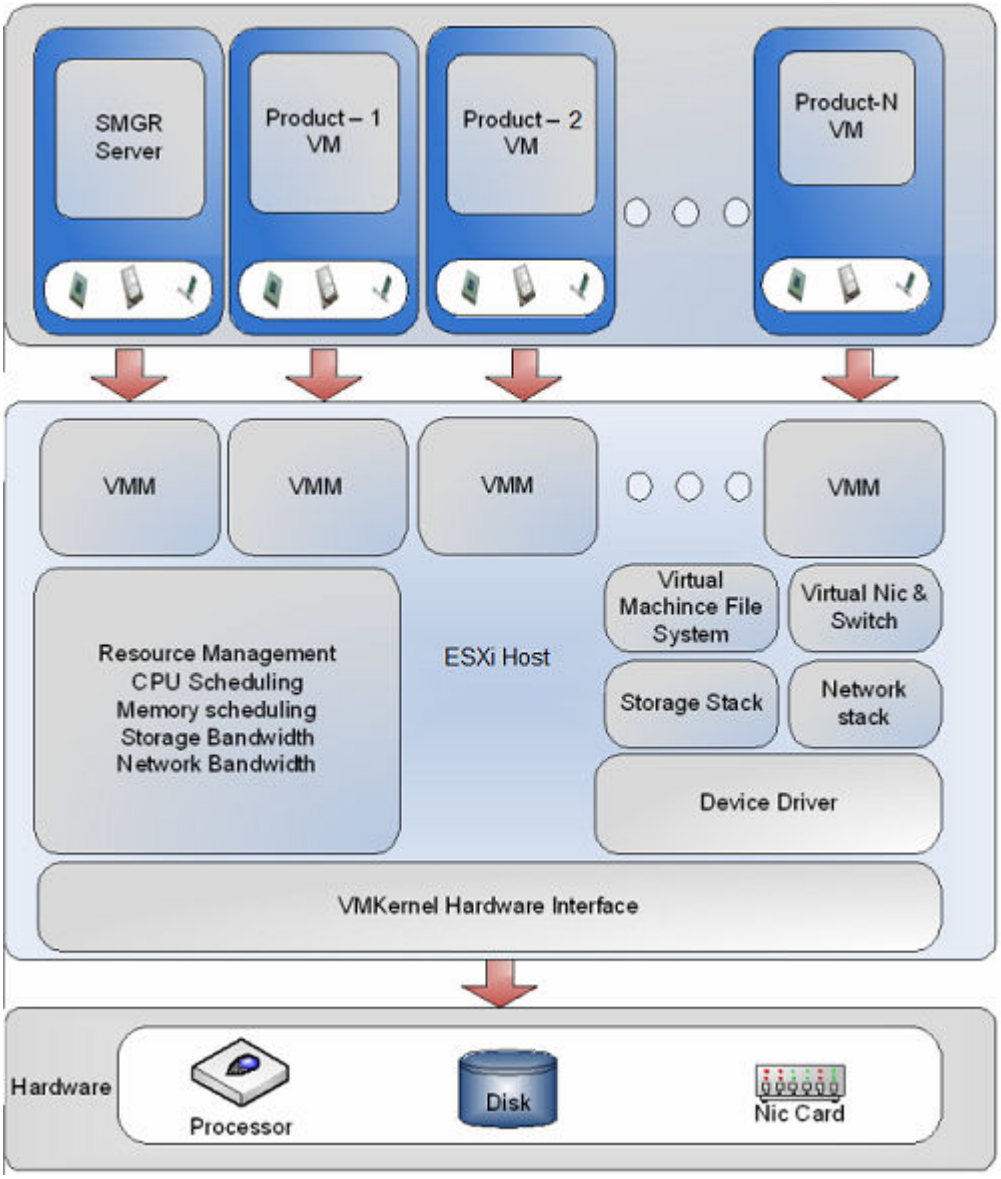
Supported applications in Virtualized Environment

- Avaya Aura® System Manager Release 10.1.x
- Avaya WebLM Release 10.1.2
- Avaya Aura® Session Manager Release 10.1.x
- Avaya Aura® Communication Manager Release 10.1.x
- Avaya Aura® Application Enablement Services Release 10.1.x
- Avaya Aura® Media Server Release 10.1.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

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 Host	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.

Note:

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

Support for VMware components

Avaya Aura® Release 10.1.x supports deployment and upgrades on the following VMware components in Virtualized Environment.

- VMware® vSphere ESXi 6.7
- VMware® vCenter Server 6.7
- VMware® vSphere ESXi 7.0
- VMware® vCenter Server 7.0

Note:

Avaya Aura® Release 10.1 and later does not support vSphere ESXi 6.0 and 6.5.

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 PSN020558u 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
- 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 10.1.x

- Avaya WebLM Release 10.1.2
- Avaya Aura® Session Manager Release 10.1.x
- Avaya Aura® Communication Manager Release 10.1.x
- Avaya Aura® Application Enablement Services Release 10.1.x
- Avaya Aura® Media Server Release 10.1.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, G450 Branch Gateway, and G650 Media 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.

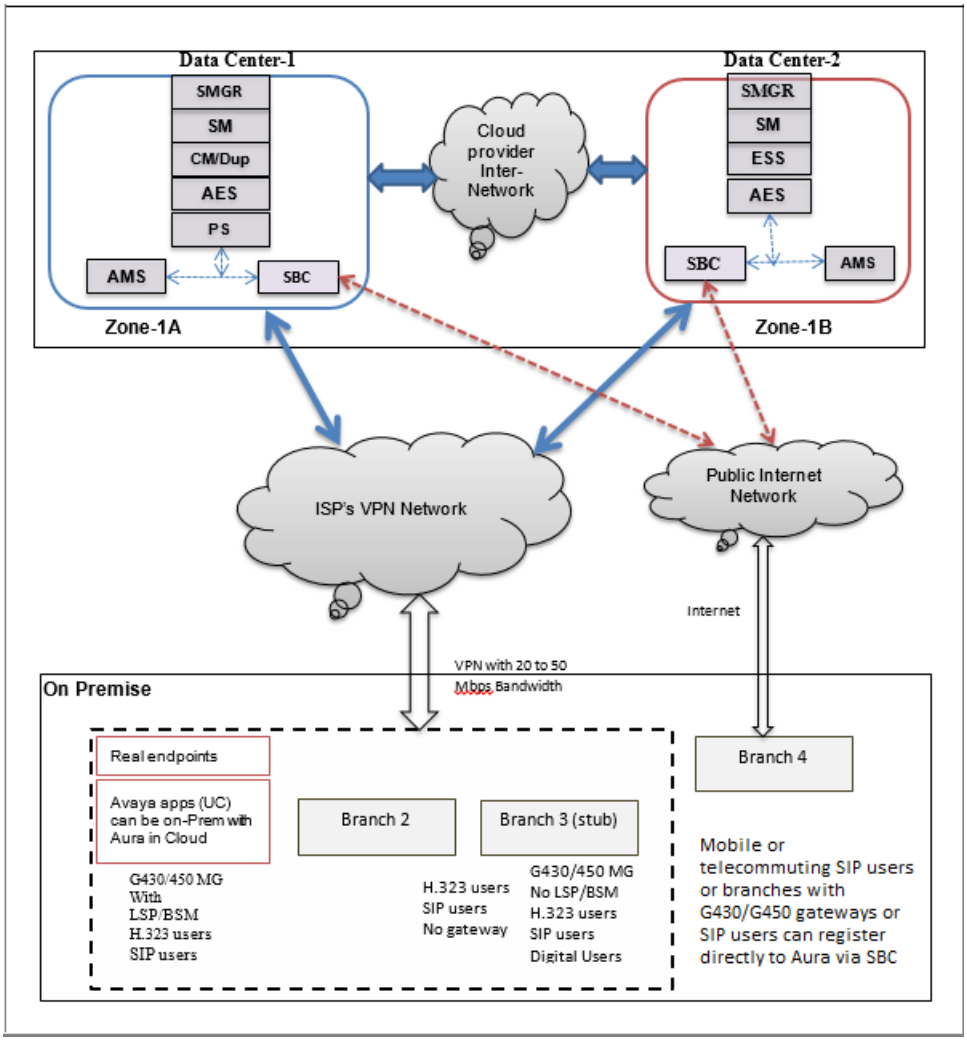
For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

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 10.1.x	Y	Y	Y

Table continues…

Application	Release	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Avaya WebLM	Release 10.1.2	Y	Y	Y
Avaya Aura® Session Manager	Release 10.1.x	Y	Y	Y
Avaya Aura® Communication Manager	Release 10.1.x	Y	Y	Y
Presence Services using Avaya Breeze® platform	Release 10.1.x	Y	—	—
Avaya Aura® Application Enablement Services (Software only)	Release 10.1.x	Y	Y	Y
Avaya Aura® Media Server (Software only)	Release 10.1.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 7.x and 8.x applications to Release 10.1 in the customer's Virtualized Environment. For migrating to Release 10.1.x and later, you must use Solution Deployment Manager Release 10.1.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.

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, media modules, and TN boards.
  - Session Manager
  - Branch Session Manager
  - AVP Utilities Release 8.x
  - Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier, the ESXi host that is running on the Avaya Aura® Virtualized Appliance.
  - 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 10.1.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

Related links

Solution Deployment Manager Client on page 22

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 7.x, or 8.x to Release 10.1 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.

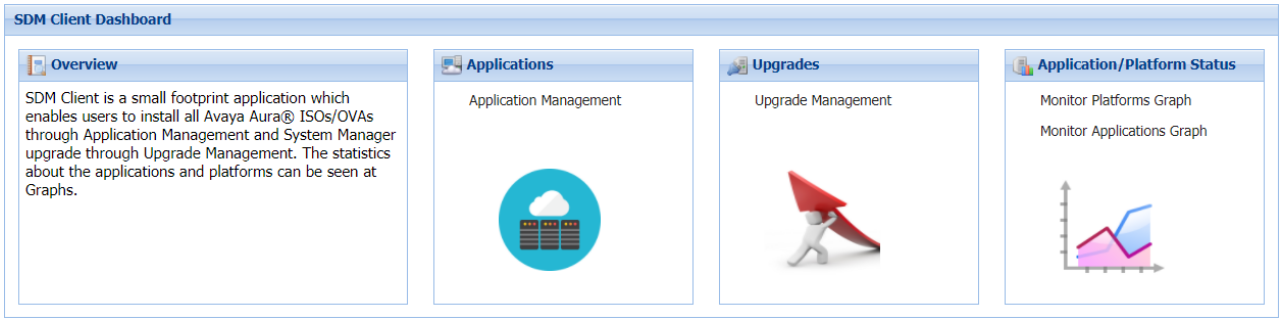


Figure 1: Solution Deployment Manager Client dashboard

Related links

Solution Deployment Manager overview on page 21

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.

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

- Hardware-based Session Manager 6.x
- 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.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
- AVP Utilities Release 7.x and later
- System Manager Release 7.x and later (using SDM client only)
- WebLM Release 7.x and later

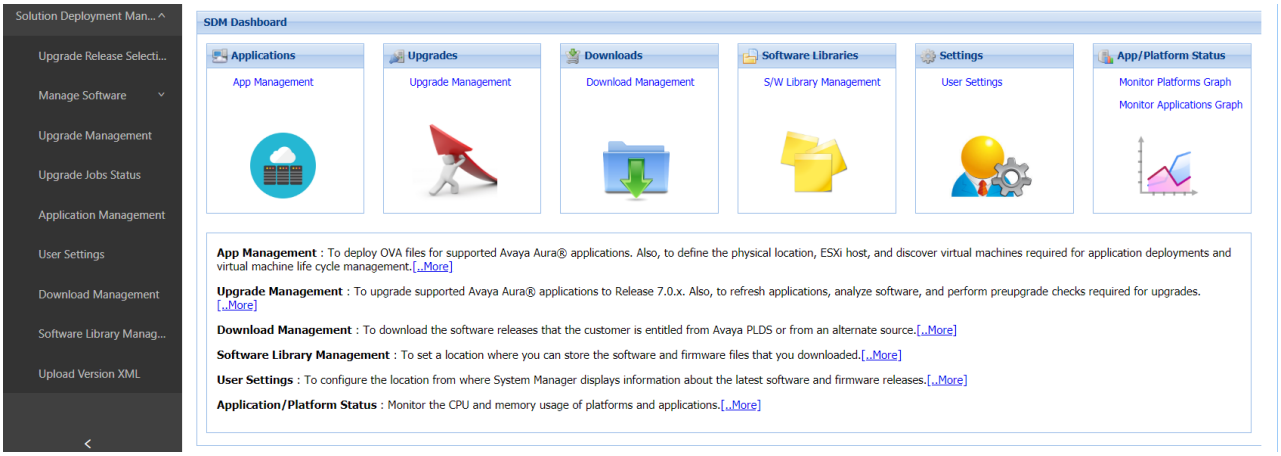
Note:

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 10.1.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 7.0
    - Appliance Virtualization Platform 7.1.x
    - 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 10.1.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 10.1.x:

- Communication Manager
- Session Manager
- Branch Session Manager

Note:

You must upgrade System Manager to Release 10.1.x by using the Solution Deployment Manager client before you upgrade the Avaya Aura® applications to Release 10.1.x.

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				
	7.0.x	7.1.x	8.0.x	8.1.x	10.1.x
Linux operating system Release 6.5 with 64-bit	Y **Note:** System Manager Release 7.0.x only supports the CentOS 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				
	7.0.x	7.1.x	8.0.x	8.1.x	10.1.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 **Note:** Avaya WebLM Release 10.1.2 supports Linux operating system Release 8.6 with 64-bit.

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		
	8.0.x	8.1.x	10.1.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 **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 **Note:** Avaya WebLM Release 10.1.2 supports Linux operating system Release 8.6 with 64-bit.

Supported ESXi version

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

ESXi version	Avaya Aura® Release				
	7.0.x	7.1.x	8.0.x	8.1.x	10.1.x
ESXi 5.0	Y	N	N	N	N

Table continues…

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

Note:

- 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 Avaya-provided environments (Avaya Solutions Platform 120 and 130 Release 4.0.x) only use Avaya-provided updates. Updating directly from the Dell or VMware's website will result in an unsupported configuration.

  For customer-provided environments and how to upgrade to supported vSphere version, see the VMware website.
- 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 6.7 can be VMware ESXi 6.7 Update 3.
- Device Adapter and Presence Services are deployed on the Avaya Breeze® platform, which supports VMware 6.7 and 7.0.
- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0 and 8.0 Update 2 (U2) deployments.

Supported servers for Avaya Aura® applications

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

Supported servers	7.0.x	7.1.x	8.0.x	8.1.x	10.1.x
S8300D	Y	Y	N	N	N
S8300E[1]	Y	Y	Y	Y	N

Table continues…

Supported servers	7.0.x	7.1.x	8.0.x	8.1.x	10.1.x
HP ProLiant DL360 G7 (CSR1)	Y	Y	N	N	N
HP ProLiant DL360p G8 (CSR2)	Y	Y	Y	Y	N
HP ProLiant DL360 G9 (CSR3)	Y	Y	Y	Y	N
Dell™ PowerEdge™ R610 (CSR1)	Y	Y	N	N	N
Dell™ PowerEdge™ R620 (CSR2)	Y	Y	Y	Y	N
Dell™ PowerEdge™ R630 (CSR3)	Y	Y	Y	Y	N
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 [2]	N	N	Y	Y	N
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 [3]	N	N	Y	Y Avaya Solutions Platform 130 Release 5.x	Y Avaya Solutions Platform 130 Release 5.x
Avaya Solutions Platform S8300 Release 5.1 [4]	N	N	N	N	Y

[1] You can migrate the S8300E server to Avaya Solutions Platform S8300 Release 5.1. 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 5.1.x.x. For information, see *Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130* on the Avaya Support website.

[4] Avaya Solutions Platform 130 Appliance uses VMware vSphere ESXi Standard License to support virtualization.

[5] Avaya Solutions Platform S8300 supports virtualization using VMware vSphere ESXi Foundation License for Communication Manager and Branch Session Manager.

Note:

- 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 10.1.x, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.x.
- From Avaya Aura® Release 8.0 and later, S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers are not supported.

Supported gateways

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

Supported gateways	Avaya Aura® Release					
	6.3.x	7.0.x	7.1.x	8.0.x	8.1.x	10.1.x
G250 Branch Gateway	Y	Y				
G350 Branch Gateway	Y	Y				
G430 Branch Gateway	Y	Y	Y	Y	Y	Y
G450 Branch Gateway	Y	Y	Y	Y	Y	Y
G650 Media Gateway	Y	Y	Y	Y	Y	Y
G700 Branch Gateway	Y	Y				

Supported browsers

The following table lists the minimum tested versions of the browsers for Avaya Aura® Release 10.1.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
10.1.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

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 10.1.x applications.

Avaya Aura® Release	Avaya Aura® application				
	Communication Manager	Session Manager	System Manager	WebLM	AE Services
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 version 8.4 is also tested for JITC certification.

Chapter 3: What's new in System Manager

This chapter provides an overview of the new and enhanced features of System Manager Release 10.1.x.

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

New in this release

New in System Manager Release 10.1.3.3

Avaya Aura® System Manager Release 10.1.3.3 supports the following new features and enhancements:

Protection of System Manager database during synchronization

From Release 10.1.3.3, 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 sychronization in the case of an upgraded System Manager or Communication Manager. In 10.1.3.3 onwards, this is no longer the case. If you attempt to run an incremental sychronization in the case of an upgraded System Manager or Communication Manager, the sychronization stops and an error message displays.

Support for running synchronization forcefully

From Release 10.1.3.3, there is a new option to enable administrators to run an initializing synchronization forcefully. If you run the synchronization forcefully, System Manager performs the initialize synchronization without checking for any data discrepency between Communication Manager and System Manager.

Enhanced logging

From Release 10.1.3.3, the IP and hostname of the Communication Manager are logged. This information enables administrators to easily identify a specific Communication Manager in the case of duplex pairs.

New in System Manager Release 10.1.2

Avaya Aura® System Manager Release 10.1.2 supports the following new features and enhancements:

Support for Fapolicy

In Release 10.1.0.2, the File Access Policy (fapolicy) service is always enabled in Military Grade hardening.

From Release 10.1.2, fapolicy is an optional attribute that you can enable or disable. By default, fapolicy is disabled.

Support of Avaya Aura® application OVA with SHA256 hash algorithm

From Release 10.1.2, Avaya Aura® applications support the SHA256 hash algorithm for OVAs.

Support of deployment and upgrade of OVA with SHA256 hash algorithm on Solution Deployment Manager

From Release 10.1.2, System Manager Solution Deployment Manager and Solution Deployment Manager Client support the deployment and upgrade of an application using the OVA with the SHA256 hash algorithm.

Enhancement to the Remove options

The following options are supported on the **Elements** > **Communication Manager** > **Element Cut-Through** > **Options** > **Usage Options** page on the **Remove Options** tab while removing the endpoints:

- Send NN button
- Busy-indicate button
- Auto-message-wait/manual message wait button
- Call forwarding button
- Call forward-busy don't answer button
- Call forward-Enhanced button
- No-hold-conference button
- Send All Calls button

New in System Manager Release 10.1.0.2

Avaya Aura® System Manager Release 10.1.0.2 supports the following new features and enhancements:

Security enhancements

- Support for tmux (terminal multiplexer) in operating system CLI along with automatic session locking.
- Support for fapolicyd.
- Support for configuring the single-user mode credentials to access the operating system in single-user mode.

Support for configuring operating system single-user mode credentials

From System Manager Release 10.1.0.2, you can use the **`setSingleUserModeCred.sh`** script to set the credentials for the single-user mode login. With these credentials the super user can reboot the operating system to edit, and access the GRUB (GRand Unified Bootloader) menu for

emergency maintenance or troubleshooting purpose. Without configuring these credentials, you cannot reboot the operating system into single-user mode.

Only the root users can run the **`setSingleUserModeCred.sh`** script and set the credentials for the single-user mode login.

Note:

The **`setSingleUserModeCred.sh`** script is not applicable for Software-Only deployments.

Solution Deployment Manager enhancements

To add Avaya Solutions Platform 130 Release 5.1 or Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1, the value of **Platform Type** is changed from **ASP 130** to **ASP 130/S8300** on the **Platforms** tab.

createCA utility enhancement

From System Manager Release 10.1.0.2, you can use the **`createCA`** utility even if System Manager CA certificate is expired.

Support for enabling or disabling the display of help text on the Communication Manager Element Cut-Through page

From System Manager Release 10.1.0.2, you can configure **Enable Help Text Retrieval on Element-cut through page** on the Edit Profile: Communication System Management Configuration page to enable or disable the help text on the **Elements** > **Communication Manager** > **Element Cut-Through** page.

Log4j upgrade from version 1.x to version 2.x

From Release 10.1.0.2, logging framework has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.

New in System Manager Release 10.1.0.1

Avaya Aura® System Manager Release 10.1.0.1 supports the following new features and enhancements:

Certificate renewal command

From System Manager Release 10.1.0.1, you can use the certificate renewal command to renew the System Manager Identity (Server) certificates. Run the certificate renewal command to issue new System Manager CA issued Identity certificates for all System Manager services.

Note:

Use the certificate renewal command only if certificate management is not possible through **Services** > **Inventory** > **Manage Elements** on the primary System Manager.

Support for Microsoft Active Directory 2022

From Release 10.1.0.1, System Manager supports Microsoft Active Directory 2022.

Support of Windows 11, Windows Server 2019, and Windows Server 2022 64-bit for Solution Deployment Manager client

From Release 10.1.0.1, you can install the Solution Deployment Manager client on the following Windows operating systems:

- Windows 11 64-bit
- Windows Server 2019 64-bit
- Windows Server 2022 64-bit

Enhancements to the System Manager Alert messages at login

From Release 10.1.0.1, System Manager displays the Session Manager and WebLM demo certificate usage warning message in an Alert Message pop-up window. The **Notifications** widget also displays the warning message. The alert message is audit logged and you can view the message on the Logging page with the event id `COMMON_CONS_WARNING_ACK`.

Enhancements to the System Manager Geographic Redundancy

If the PostgreSQL database disk partition utilization reaches threshold limit of 75%, System Manager generates a Warning alarm.

If the PostgreSQL database disk partition utilization reaches threshold limit of 85%, System Manager triggers auto-disable for the Geographic Redundancy system and generates a Critical alarm.

New in System Manager Release 10.1

Avaya Aura® System Manager Release 10.1 supports the following new features and enhancements:

Support of Unified Extensible Firmware Interface

With Release 10.1, Avaya Aura® application OVAs support the Unified Extensible Firmware Interface (UEFI) by default and replace the legacy BIOS. This helps the boot process to be faster, provides better security, and larger disk support.

Support of Secure Boot

With Release 10.1, Secure Boot is enabled on Avaya Aura® application OVAs. Secure Boot ensures only trusted software can be executed. By verifying the digital signature of any executable files, Secure Boot can help prevent viruses and other malicious software. It prevents hackers from installing rootkits (clandestine computer programs) in the time between bootup and handoff to the Operating System.

Support for pre-staging System Manager files using Solution Deployment Manager Client

Solution Deployment Manager Client supports the Pre-staging feature to pre-stage the System Manager OVA, service pack or feature pack, or data migration utility files to deploy, upgrade, or update the System Manager application. The Pre-staging feature is only available for deploying, upgrading, and updating the System Manager using OVA.

Support for TLS 1.3

From Release 10.1, System Manager supports the TLS version 1.3.

Support of Red Hat Enterprise Linux 8.4

With Release 10.1, System Manager supports Red Hat Enterprise Linux 8.4.

Infrastructure changes

- Application Server is updated to WildFly version 24.
- Database Server is updated to Postrgres version 13.3.

Supported browsers

With Release 10.1, the following are the supported versions of the supported browsers:

- Microsoft Chromium Edge Release 93 and later
- Google Chrome Release 91 and later
- Mozilla Firefox Release 93 and later

Note:

From Release 10.1 and later, Microsoft Internet Explorer is no longer supported.

Enhancement to the System Manager profile

With Release 10.1, the hard disk size of System Manager:

- Profile 2 is increased from 105 GB to 170 GB.
- Profile 3 is increased from 250 GB to 270 GB.

REST API for Geographic Redundancy operations

With Release 10.1, you can use the Geographic Redundancy REST API to do the following:

- Enable or disable Replication.
- Activate or deactivate the secondary System Manager.
- Restore Data on the primary or secondary System Manager.
- Perform the Manage or Unmanage operation on the element.
- Check the element status details.

Enhancements to the Session Manager communication profile

With Release 10.1, Session Manager supports the Policy-based Assignment of Users to Session Manager feature when you enable the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page. To support this feature, System Manager displays the **Policy** field for the Session Manager communication profile:

- On the **Users** > **User Management** > **Manage Users** page when performing a New or Edit operation.
- On the **Users** > **User Provisioning Rule** page in the **Communication Profile** tab, when performing a New or Edit operation.
- On the **Users** > **User Management** > **Manage Users** page, click **More Actions** > **Bulk Edit Users**. On the **User Bulk Editor** > **Communication Profile** page, in the Session Manager Profile section.

For more information, see *Administering Avaya Aura® Session Manager*.

Enhancements to the System Manager backup alarm

With Release 10.1, you can configure a threshold for raising the alarm when no successful System Manager backup is taken since the configured number of days. The configuration range is 1 through 30 days, and the default is 7.

End-of-support of SIP CA demo certificates for WebLM

With Release 10.1, the fresh deployment of System Manager will no longer package the SIP CA demo certificates for use with WebLM.

End-of-support of Avaya Aura® Conferencing

With System Manager Release 10.1, Avaya Aura® Conferencing will no longer be supported in System Manager. If a customer has conferencing data provisioned in System Manager, all the data related to conferencing is removed when migrating to System Manager Release 10.1.

Avaya Aura® Release 8.1.3.x is the last supported release for Appliance Virtualization Platform and AVP Utilities

From Avaya Aura® Release 10.1, Appliance Virtualization Platform is no longer available for deploying or upgrading the Avaya Aura® applications.

- To deploy the Avaya Aura® applications on Avaya-Supplied ESXi, use Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.x.
- To upgrade the Avaya Aura® applications, migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.x before upgrading the application.

  For information about migrating Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.x, see the product-specific Upgrading guides.

Unsupported Avaya-provided servers

With Release 10.1, the following Avaya-provided servers are not supported:

- HP ProLiant DL360p G8
- HP ProLiant DL360 G9
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630
- Avaya Solutions Platform 120 offers

  Avaya Solutions Platform 120 and Avaya Solutions Platform 130 have the same Dell PowerEdge R640 hardware configuration. Therefore, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.x.

Discontinued the AWS and KVM OVAs

From Release 10.1, Avaya Aura® applications will no longer provide the Amazon Web Services (AWS) and Kernel-based Virtual Machine (KVM) OVAs. Alternately, to continue to deploy the application on these platform, use the software-only offer.

For information about deploying, see the product-specific Software-only and Infrastructure As a Service Environments deployment guide.

For information about upgrading to Software-only, see the product-specific Upgrading guides.

Solution Deployment Manager enhancements

Solution Deployment Manager supports the following capabilities:

- Add Avaya Solutions Platform 130 Release 5.1 or Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1 as the **ASP 130** platform on the **Platforms** tab.

  You can perform the add, remove, restart, stop, enable or disable SSH, and generate the certificates operations by using Solution Deployment Manager.
- Generate the Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1 Kickstart file for installing Avaya Solutions Platform S8300.

System Manager feature matrix

The following table lists the feature matrix of System Manager from Release 7.x to Release 10.1.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
OVA signing	Y	Y	Y	Y
IPv6 support	Y	Y	Y	Y
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y
Compliance with DISA security STIGs	Y	Y	Y	Release 10.1.0.2: Y
Extended Security Hardening	Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y
Customer Root Access		Y	Y	Y
Preserve security hardening modes on upgrade		Y	Y	Y
Extended host name validation		Y	Y	Y
Support for 16-digit extension		Y	Y	Y
Product Initiated Registration		Y	Y	Y
Support for Software-only deployment		Y	Y	Y
Support for deployment on Cloud Services	Y	Y	Y	Y
Support for Geographic Redundancy in mixed deployment environment		Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance		Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x
Support for Avaya Solutions Platform 130 Appliance		Y	Y	Y
Support for Data Encryption			Y	Y
Support for encrypted backup and restore			Y	Y
Support for log file retention period management			Y	Y
Support for the Avaya Subscription license			Y	Y
Support for VMware ESXi 7.0			Y	Y
Support for J-Series phone migration			Y	Y
SCEP Enrollment Enhancement to improve Certificate Management for endpoints			Y	Y
Emergency Location Management Solution			Y	Y
Support for TLS 1.3				Y
Support for RHEL 8.4				Y

Chapter 4: What's new in WebLM

This chapter provides an overview of the new and enhanced features of WebLM Release 10.1.2.

For more information about these features and administration, see *Administering standalone Avaya WebLM*.

New in this release

New in WebLM Release 10.1.2

WebLM Release 10.1.2 supports the following new features and enhancements:

Support of Avaya Aura® application OVA with SHA256 hash algorithm

From Release 10.1.2, Avaya Aura® applications support the SHA256 hash algorithm for OVAs.

Support of deployment and upgrade of OVA with SHA256 hash algorithm on Solution Deployment Manager

From Release 10.1.2, System Manager Solution Deployment Manager and Solution Deployment Manager Client support the deployment and upgrade of an application using the OVA with the SHA256 hash algorithm.

Support for TLS 1.3

From Release 10.1.2, WebLM supports TLS version 1.3.

Support of new CLI command for managing the password policies

From Release 10.1.2, WebLM supports the **`setSecurityPolicy`** command to manage password policies using the command-line interface (CLI). This command is only applicable for changing or setting up the password for a CLI user or a root user that you create during deployment.

Support of the new Password Policy page

From Release 10.1.2, you can configure the WebLM password history and strength policies on the Password Policy page.

If the password policy is enabled, WebLM also applies those password policies while changing the WebLM password on the Change Password page of the WebLM web console.

Support to manage the WebLM Application server

From Release 10.1.2, WebLM supports the following new commands:

- **`weblmStart`** to start the WebLM Application server.
- **`weblmStatus`** to check the status of the WebLM Application server.
- **`weblmStop`** to stop the WebLM Application server.
- **`weblmRestart`** to restart the WebLM Application server.

Configuration of the whitelist for client certificate identity

From Release 10.1.2, you can configure the whitelist to validate the client certificate identity for the installed product license.

Support for configuring the user inactivity timeout value

From Release 10.1.2, you can configure the inactivity timeout for the user, after which the WebLM web console times out. To configure, you can use the **User inactivity timeout (minutes)** field on the Manage Users page.

Support to manage WebLM certificates in the WebLM server keystore

From Release 10.1.2, WebLM supports the following new commands:

- **`manageWebLMCertificate -display`** to view the WebLM certificate that is stored in the WebLM server keystore.
- **`manageWebLMCertificate -replace`** to replace the WebLM certificate with a new third-party certificate.
- **`manageWebLMCertificate -generateSelfSigned`** to replace the existing certificate with a new self-signed server certificate.

Support to manage CA certificates in the WebLM truststore

From Release 10.1.2, WebLM supports the following new commands:

- **`manageCACertificates -list`** to display a CA certificate stored in the WebLM server truststore.
- **`manageCACertificates -add`** to import a CA certificate into the WebLM truststore.
- **`manageCACertificates -remove`** to delete a CA certificate from the WebLM truststore.

Support to manage WebLM client certificate authentication

From Release 10.1.2, WebLM supports the following new commands:

- **`setWebLMClientAuth [1]`** to display existing WebLM client certificate authentication configuration.
- **`setWebLMClientAuth [2]`** to enable WebLM client certificate authentication.
- **`setWebLMClientAuth [3]`** to disable WebLM client certificate authentication.

WebLM feature matrix

The following table lists the feature matrix of WebLM.

Feature name	Release 7.1 and Release 7.1.1	Release 7.1.2 and Release 7.1.3	Release 8.0.x	Release 8.1.x	Release 10.1.2
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	
Extended Security Hardening	Y	Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y	Y
Customer Root Access			Y	Y	Y
Support for Software-only deployment			Y	Y	Y
Support for deployment on Cloud Services		Y	Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance			Y	Y	Y
Support for Avaya Solutions Platform 130 Appliance			Y	Y	Y
Centralized subscription licensing				Y	Y
Support for VMware ESXi 7.0				Y	Y
Support for the Avaya Subscription license				Y	Y
Support of Metering Collector configuration				Y	Y

Chapter 5: What's new in Session Manager

This chapter provides an overview of the new and enhanced features of Session Manager Release 10.1.x.

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

New in this release

New in Session Manager Release 10.1.3.4

Avaya Aura® Session Manager Release 10.1.3.4 supports the following new feature:

Avaya Aura® X for Zoom Workplace

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

New in Session Manager Release 10.1.3

Session Manager Release 10.1.3 supports the following new features and enhancements:

Support for displaying SIP user agent information of the endpoint

From Release 10.1.3, you can view the SIP User Agent information of the endpoint on the **Elements** > **Session Manager** > **System Status** > **User Registrations** page in the Details section under the **Device** tab.

New in Session Manager Release 10.1.2

Session Manager Release 10.1.2 supports the following new features and enhancements:

Support of Avaya Aura® application OVA with SHA256 hash algorithm

From Release 10.1.2, Avaya Aura® applications support the SHA256 hash algorithm for OVAs.

Support of deployment and upgrade of OVA with SHA256 hash algorithm on Solution Deployment Manager

From Release 10.1.2, System Manager Solution Deployment Manager and Solution Deployment Manager Client support the deployment and upgrade of an application using the OVA with the SHA256 hash algorithm.

Support for configuring the Time zone setting for J100 phones

Earlier to Release 10.1.2, the user can configure the J100 phones to get their time zone settings through a phone settings file. At a user level, it has been a complex work to set the time zone setting through the settings file.

Therefore, from Release 10.1.2, you can set the time zone configuration for J100 phones in the new **Time zone** field on the **Elements** > **Session Manager** > **Device and Location Configuration** > **Device Settings Groups** page. The endpoint can locally determine the Daylight Savings settings appropriate to the time zone selected.

New in Session Manager Release 10.1.0.2

Session Manager Release 10.1.0.2 supports the following enhancement:

Log4j upgrade from version 1.x to version 2.x

From Release 10.1.0.2, logging framework has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.

New in Session Manager Release 10.1.0.1

Avaya Aura® Session Manager Release 10.1.0.1 supports the following new feature:

Enhancements to the System Manager Alert messages at login

From Release 10.1.0.1, System Manager displays the Session Manager and WebLM demo certificate usage warning message in an Alert Message pop-up window. The **Notifications** widget also displays the warning message. The alert message is audit logged and you can view the message on the Logging page with the event id `COMMON_CONS_WARNING_ACK`.

New in Session Manager Release 10.1

Avaya Aura® Session Manager Release 10.1 supports the following new features and enhancements:

Support for TLS 1.3

From Release 10.1, Session Manager supports the TLS version 1.3.

Support of Red Hat Enterprise Linux 8.4

From Release 10.1, Session Manager supports the TLS version 1.3.

Support for Policy-based Assignment of Users to Session Managers

With Release 10.1, Session Manager supports the Policy-based Assignment of Users to Session Manager feature when you enable the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page.

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

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

- Fixed
- Fixed-region
- Location-region

To support policy-based assignment, the administration of a region and location to region mapping is performed on the Session Manager Groups page.

Note:

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

Support for Registration of SIP Clients to four Session Managers

With Release 10.1, you can assign up to 4 Session Managers to a user's profile. The additional two Session Managers allow both, local and geo-redundancy simultaneously for added reliability. The 4+1 registration setup is as follows:

- 2 Session Managers in Primary Data Center
- 2 Session Managers in Secondary Data Center
- 1 Local Branch Session Manager

Support for Android Push Notification Services

With Release 10.1, Session Manager provides telephony push notifications events through Google Firebase service to Client SDK based Android applications, such as Avaya Workplace Client for Android. Session Manager provides push notification events for incoming calls and voice messaging status updates. Avaya Workplace Client for Android should be on Release 3.24 or later to receive push notification services.

To configure the feature, enable the **Enable Mobile Push Notification** field on the Global Settings page. For administering the push notification provider and application, use the **Session Manager** > **Network Configuration** > **Push Notification** page.

Enhancement to the Session Manager profile

With Release 10.1, the hard disk size of Session Manager:

- Profile 1 and 2 is increased from 90 GB to 100 GB
- Profile 3 and 4 is increased from 120 GB to 135 GB
- Profile 5 and 6 is increased from 200 GB to 210 GB

Supported browsers

With Release 10.1, the following are the supported versions of the supported browsers:

- Microsoft Chromium Edge Release 93 and later
- Google Chrome Release 91 and later
- Mozilla Firefox Release 93 and later

Note:

From Release 10.1 and later, Microsoft Internet Explorer is no longer supported.

Avaya Aura® Release 8.1.3.x is the last supported release for Appliance Virtualization Platform and AVP Utilities

From Avaya Aura® Release 10.1, Appliance Virtualization Platform is no longer available for deploying or upgrading the Avaya Aura® applications.

- To deploy the Avaya Aura® applications on Avaya-Supplied ESXi, use Avaya Solutions Platform 130 Release 5.x.
- To upgrade the Avaya Aura® applications, you need to migrate from Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.x. For more information on upgrading and migrating the Avaya Aura® applications on Avaya-Supplied ESXi, please refer *Avaya Aura® Release 10.1 x Release Notes* and *Upgrading Avaya Aura® Session Manager*.
- If you have a S8300 server configured as Branch Session Manager, use Avaya Solutions Platform S8300 Release 5.1. For information about deploying or upgrading Branch Session Manager 10.1.x on Avaya Solutions Platform S8300 Release 5.1, see the product-specific documentation.

Unsupported Avaya-provided servers

With Release 10.1, the following Avaya-provided servers are not supported:

- HP ProLiant DL360p G8
- HP ProLiant DL360 G9
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630
- Avaya Solutions Platform 120 offers

  Avaya Solutions Platform 120 and Avaya Solutions Platform 130 have the same Dell PowerEdge R640 hardware configuration. Therefore, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.x.

Support for nftables and chronyd

With Release 10.1, Session Manager supports nftables firewall and chronyd.

End-of-support of iptables and NTP

With Release 10.1, Session Manager does not support iptables and NTP.

Discontinued the AWS and KVM OVAs

From Release 10.1, Session Manager will no longer have the Amazon Web Services (AWS) and Kernel-based Virtual Machine (KVM) OVAs. Alternately, you can continue to deploy the application

by using the software-only offer. For more information, see the *Deploying Avaya Aura® Session Manager in Software-Only and Infrastructure as a Service Environment* guide.

Session Manager feature matrix

The following table lists the feature matrix of Session Manager from Release 7.x to Release 10.1.x. The features listed in the table covers the key features only.

Feature name	Release 7.0.x	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x
OVA signing		Y	Y	Y	Y
IPv6 support		Y	Y	Y	Y
Enhanced Access Security Gateway (EASG)		Y	Y	Y	Y
Compliance with DISA security STIGs		Y	Y	Y	Release 10.1.0.2: Y
Extended Security Hardening		Y	Y	Y	Y
Conference factory URI		Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y	Y
Customer Root Access			Y	Y	Y
Preserve security hardening modes on upgrade			Y	Y	Y
SIP Resiliency			Y	Y	Y
Extended host name validation			Y	Y	Y
Cassandra clustering		Y	Y	Y	Y
Support for Software-only deployment			Y	Y	Y
Support for 16 digit dial plan			Y	Y	Y
Support for Hyper-V in Software-Only environment			Y	Y	Y
Support for Regular Expression based adaptation module			Y	Y	Y

Table continues…

Feature name	Release 7.0.x	Release 7.1.x	Release 8.0.x	Release 8.1.x	Release 10.1.x
Support for Call Journaling Server High Availability			Y	Y	Y
Cassandra security hardening			Y	Y	Y
Support for multiple customer accounts			Y	Y	Y
Support for role-based access control			Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance			Y	Y	
Support for Avaya Solutions Platform 130 Appliance			Y	Y	Y
Syslog server configuration				Y	Y
Data Encryption				Y	Y
Branch Visiting User				Y	Y
Apple Push notification				Y	Y
Support for VMware ESXi 7.0				Y	Y
Policy-based Assignment of Users to Session Manager					Y
Registration of SIP Clients to four Session Managers					Y
Support for TLS 1.3					Y
Android Push notification					Y
Support for RHEL 8.4					Y
Avaya Solutions PlatformS8300 for Branch Session Manager					Y
Support of Avaya Aura® X for Zoom Workplace				Y	

Chapter 6: What's new in Communication Manager

This chapter provides an overview of the new and enhanced features of Communication Manager Release 10.1.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 10.1.3.6

With Release 10.1.3.6, Avaya Aura® Communication Manager supports the following new enhancement:

Enhancement to Communication Manager License Expiration

Beginning with Release 10.1.3.6, 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.

Note:

- The Communication Manager checks the expiration dates of all features in the license file and uses the earliest date as the license expiration date. For example, if the Elite license expires on July 30 and the Communication Manager license expires on August 30, the Communication Manager will consider July 30 as the license expiration date.
- This feature enhancement is applicable only for main Communication Manager and not for Local Survivable Processor (LSP) and Enterprise Survivable Server (ESS).
- This feature enhancement is applicable only for Communication Manager and not for any other Avaya Aura Products.

New in Communication Manager Release 10.1.3

With Release 10.1.3, Avaya Aura® Communication Manager supports the following new features and enhancements:

Additional support to install Security Service Pack (SSP)

In earlier releases, Communication Manager CLI was used to install the Communication Manager SSP.

With Communication Manager R10.1.3, to install the Communication Manager SSP, you can use any of the following:

- Solution Deployment Manager (SDM)
- Communication Manager System Management Interface (SMI)
- Communication Manager Command Line Interface (CLI)

Support for Enterprise Mobility eXperience (EMX) sim-ring extensions

With Communication Manager R10.1.3, when you register a primary station on the Avaya Workplace Client, you can specify which extensions must ring simultaneously with the primary station when a call is made to the primary station. You can also specify which one of the simultaneous ring extensions can act as a callback extension for an outgoing call.

Note:

You cannot configure the EMX application if either EC500 or ONEX application is configured for a primary station.

New in Communication Manager Release 10.1.2

With Release 10.1.2, Avaya Aura® Communication Manager supports the following new features and enhancements:

Support of Avaya Aura® application OVA with SHA256 hash algorithm

From Release 10.1.2, Avaya Aura® applications support the SHA256 hash algorithm for OVAs.

Additional support for Fully Qualified Domain Name (FQDN) on the Access and FP Traps pages

With Release 10.1.2, the **IP address** field on the Access and FP Traps pages of the Communication Manager System Management Interface (SMI) is renamed to **FQDN / IP address**. You can now enter the FQDN or the IP address in the **FQDN / IP address** field.

Support to block service observe across tenants

With Release 10.1.2, you can configure the service observe feature to block across tenants. If the service observer feature is enabled, the service observer cannot monitor the agent if the service observer and agent are in different tenant partitions.

Support for listen-only mode for the intercom call receiver

With Release 10.1.2, you can configure the listen-only mode for the receiver when an intercom call is received. The intercom call receiver can listen to the other party but cannot speak with the other party. Communication Manager provides the lamp updates for the intercom button.

Listen-only mode is applicable for J100 series phones only.

Support of Enterprise Mobility eXperience (EMX) feature

With Release 10.1.2, Communication Manager supports the EMX feature. You can now configure up to 4 sim-ring extensions using Avaya Workplace Client 3.32 and above. The System Capacity page displays the maximum number of EMX ring extensions available and the number of EMX ring extensions used on Communication Manager.

Send All Calls on Ringing Bridge Leaves Call Ringing on Other Bridges

With Release 10.1.2, if a call rings on a bridging group and anyone in the group has the SAC enabled or presses the **SAC** button, the call completes the total number of rings. However, if the principal presses the **SAC** button, the call goes to the next coverage point without completing the total number of rings.

Increase in split recording capacity

With Release 10.1.2, Communication Manager supports up to 8000 split recordings. Communication Manager records the number of simultaneous split streams depending on the call configuration and call volumes. An increase of 8000 split stream recordings is only applicable for Large and Extra-Large platforms. Medium and small platforms remain with 300 and 75, respectively.

New in Communication Manager Release 10.1.0.2

With Release 10.1.0.2, Avaya Aura® Communication Manager supports the following new features and enhancements:

Support for Communication Manager duplex on Google Cloud Platform

With Release 10.1.0.2, you can deploy the duplex Communication Manager on Google Cloud Platform.

Support for Malicious Call Alert using the Crisis Alert button

With Release 10.1.0.2, Communication Manager notifies all the SIP endpoints with the **Crisis Alert** button for emergency calls or malicious calls, but not both.

Service observe support for Unified Communications SIP devices

With Release 10.1.0.2, Unified Communications SIP devices support the **sip-sobsrv** button with listen-only and coach options.

Event is created when H.323 station registers on a designated Communication Manager

With Release 10.1.0.2, Communication Manager creates an event when H.323 station tries to register on a designated Communication Manager that is on a passive mode.

Support for Call Work Code and Stroke Count

From Release 10.1.0.2 onwards, AE Services and Avaya Aura® Communication Manager support two new APIs, Call Work Code (CWC) and Stroke Count (SC). These third-party call control support APIs send CWC and SC to Avaya Aura® Communication Manager.

These APIs work if the ASAI version is 12 and above and the private data version is 18 and above for TSAPI and JTAPI applications. These APIs are exposed over JTAPI, TSAPI, DMCC, and CVLAN services on the AE Services server.

New fields added to Status Station page

With Release 10.1.0.2, the following new fields are added on the Status Station screen to display the phone status:

- **Active calls**
- **Busied out**
- **CTI monitoring**
- **Reachability Polling Active**
- **Reg Subscription**

Log4j upgrade from version 1.x to version 2.x

From Release 10.1.0.2, logging framework has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.

New in Communication Manager Release 10.1

Communication Manager Release 10.1 supports the following enhancements:

Avaya Aura® supports the latest transport methods

From Release 10.1, Avaya Aura® applications support the following transport methods:

- TLS 1.3
- Open SSL 1.1.1

Red Hat Enterprise Linux support

From Release 10.1, Communication Manager supports Red Hat Enterprise Linux 8.4.

Alarm when a demo certificate is identified

From Release 10.1, Communication Manager raises an alarm when a demo certificate is identified.

Supported browsers

From Release 10.1, the following are the minimum supported versions of the supported browsers:

- Microsoft Chromium Edge Release 93

- Google Chrome Release 91
- Mozilla Firefox Release 93

Note:

From Release 10.1 and later, Internet Explorer 11 is no longer supported.

Temporary certificate

From Release 10.1, Communication Manager SMI uses a new temporary certificate with a validity of 90 days.

Malicious Call Trace (MCT) enhancement

From Release 10.1, you can activate and deactivate the MCT feature without configuring the MCT controller. This is critical for customers with only SIP endpoints because a SIP endpoint cannot function as an MCT controller. When no MCT controller is configured, Communication Manager Release 10.1 sends SNMP to notify security personnel about the malicious call.

Policy-Based Assignment of Session Managers

From Release 10.1, if the **Enable Policy Based Assignment of Session Managers** field is enabled on the **Elements** > **Session Manager** > **Global Settings** page, System Manager displays the **Policy** field for the Session Manager communication profile to administer up to four Session Managers for a SIP station for the fixed policy type. Communication Manager displays the new Third Session Manager and Fourth Session Manager fields on the Station form.

SA9145 - Call Detail Recording records the extension of the answering station

From Release 10.1, if you enable the **CDR Record Answering Party for Bridged Appearances** field on the system-parameters special-applications screen, Call Detail Recording (CDR) records the extension of the answering station as the destination party if a bridged appearance answers the call.

For more information about the Special Application features, see the *Avaya Aura® Communication Manager Special Application Features* document.

Centralized licensing

From Release 10.1, in the **Centralized Licensing ID** field of WebLM web console, you must enter the IP address of Communication Manager in the following format: `CM @ <CM IP address>`.

Support for nftables and chronyd

From Release 10.1, Communication Manager supports nftables firewall and chronyd.

Avaya Aura® Release 8.1.3.x is the last supported release for Appliance Virtualization Platform and AVP Utilities

From Avaya Aura® Release 10.1, Appliance Virtualization Platform is no longer available for deploying or upgrading the Avaya Aura® applications.

- To deploy the Avaya Aura® applications on Avaya-Supplied ESXi, use Avaya Solutions Platform 130 Release 5.x.
- To upgrade the Avaya Aura® applications, migrate from Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.x. For more information about upgrading and migrating the Avaya Aura® applications on Avaya-Supplied ESXi, see *Avaya Aura® Release 10.1 x Release Notes* and *Upgrading Avaya Aura® Communication Manager*.

For more information about upgrading or migrating the Avaya Aura® applications on Avaya-Supplied ESXi, see *Avaya Aura® Release 10.1 x Release Notes*.

- If you have an S8300 server configured in embedded CM main, survivable remote, or embedded survivable remote configurations, use Avaya Solutions Platform S8300 Release 5.1. For information about deploying or upgrading Communication Manager 10.1.x on the Avaya Solutions Platform S8300 Release 5.1, see the product-specific documentation.

Unsupported Avaya-provided servers

From Release 10.1, the following Avaya-provided servers are not supported:

- HP ProLiant DL360p G8
- HP ProLiant DL360 G9
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630
- Avaya Solutions Platform 120

Discontinued the AWS and KVM OVAs

From Release 10.1, Avaya Aura® applications do not have the Amazon Web Services (AWS) and Kernel-based Virtual Machine (KVM) OVAs. You can continue to deploy the application using the software-only offer. For more information about deploying the software-only offer, see the product-specific Software-only and Infrastructure as a Service Environments guide.

End-of-support of iptables and NTP

From Release 10.1, Communication Manager does not support iptables and NTP.

End-of-support of SIP CA and demo certificates

From Release 10.1, fresh deployment of Communication Manager does not package:

- Demo certificates
- SIP CA for web repository

Communication Manager feature matrix

The following table lists the feature matrix of Communication Manager from Release 7.x to Release 10.1.x. The features listed in the table covers the key features only.

Feature name	Release 7.1 and Release 7.1.1	Release 7.1.2 and Release 7.1.3	Release 8.0.x	Release 8.1, Release 8.1.1, and Release 8.1.2	Release 8.1.3	Release 10.1.x
OVA signing	Y	Y	Y	Y	Y	Y

Table continues…

Feature name	Release 7.1 and Release 7.1.1	Release 7.1.2 and Release 7.1.3	Release 8.0.x	Release 8.1, Release 8.1.1, and Release 8.1.2	Release 8.1.3	Release 10.1.x
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	Release 10.1.0.2: 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
Preserve security hardening modes on upgrade			Y	Y	Y	Y
SIP trunk optimization			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	Y	Y	Y	Y
Extended security hardening		Y	Y	Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance			Y	Y	Y	

Table continues…

Feature name	Release 7.1 and Release 7.1.1	Release 7.1.2 and Release 7.1.3	Release 8.0.x	Release 8.1, Release 8.1.1, and Release 8.1.2	Release 8.1.3	Release 10.1.x
Support for Avaya Solutions Platform 130 Appliance			Y	Y	Y	Y
Support for J-Series phone migration					Y	Y
Support for VMware ESXi 7.0					Y	Y
Emergency Location Management Solution					Y	Y
Support for TLS 1.3						Y
Support for RHEL 8.4						Y
Avaya Solutions Platform S8300						Y

Chapter 7: What's new in Presence Services

This chapter provides an overview of the new and enhanced features of Presence Services Release 10.1.x.

For more information about these features and administration, see *Avaya Aura® Presence Services Snap-in Reference*.

New in this release

New in Presence Services Release 10.1

Presence Services Release 10.1 supports the following new features and enhancements:

Third-party antivirus support

With Release 10.1, Presence Services support the following third-party antivirus applications:

- Symantec Endpoint Protection
- Microsoft Defender ATP (Linux)

Subscribing for external contacts

With Release 10.1, Presence Services lets you subscribe for presence of external contacts.

Metrics report

With Release 10.1, Presence Services sends the metrics information to third-parties when third-parties sends an API request.

Enterprise directories

With Release 10.1, Presence Services lets you configure nine additional enterprise directory services instead of four.

Attachments with messaging

With Release 10.1, Presence Services lets you send the attachment with messaging facility for Cisco federation.

Push notification for Android

With Release 10.1, Presence Services lets you send the push notifications for android devices.

Alignment with Aura® 10.1 platform updates

With Release 10.1, Presence Services support the following Aura® updates:

- Breeze 3.8.1
- GS 15.X
- RHEL 8.4
- Common OS
- TLS 1.3
- OpenSSL 1.1.1

Presence Services feature matrix

The following table lists the feature matrix of Presence Services from Release 7.x to Release 10.1. The features listed in the table covers the key features only.

Feature	Release 7.1.x	Release 8.0.x	R 8.1.x	R 10.1
Android Push Notification	N	N	N	Y
Apple Push Notification service (APNs)	N	Y	Y	Y
Access control lists	Y	Y	Y	Y
Application Enablement Services collector	Y	Y	Y	Y
Exchange collector	Y	Y	Y	Y
Domino collector	Y	Y	Y	Y
Microsoft Real Time Communication federation	Y	Y	Y	Y
Inter-PS federation	Y	Y	Y	Y
XMPP federation	Y	Y	Y	Y
Spaces federation	Y	Y	Y	Y
Simple authentication and security layer	Y	Y	Y	Y
IM blocking in Do Not Disturb state	Y	Y	Y	Y
Instant message broadcast	Y	Y	Y	Y
Interoperability with Avaya Multimedia Messaging	Y	N	N	Y
Inter-domain presence	Y	Y	Y	Y
Inter-tenant communication control	Y	Y	Y	Y
Multi-tenancy	Y	Y	Y	Y

Table continues…

Feature	Release 7.1.x	Release 8.0.x	R 8.1.x	R 10.1
Message archiver	Y	Y	Y	Y
Offline IM storage	Y	Y	Y	Y
Avaya Solutions Platform servers	Y	Y	Y	Y
KVM	Y	Y	Y	Y
IPv6	Y	Y	Y	Y
Extended hostname validation		Y	Y	Y
Microsoft Office 365			Y	Y
Message Security			Y	Y
Multiple Front End pools			Y	Y
Microsoft Active Directory 2019			Y	Y

Chapter 8: What's new in Application Enablement Services

This chapter provides an overview of the new and enhanced features of Application Enablement Services Release 10.1.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 10.1.3.1

Avaya Aura® Application Enablement Services Release 10.1.3.1 supports the following new feature and enhancement:

AE Services TSAPI Encrypted Services port added

Earlier to Release 10.1.3.1, you can enable or disable the TSAPI port 450 for the TSAPI listener.

With Release 10.1.3.1, a new TSAPI Encrypted Services Port 453 is added in the TSAPI Ports section on the **Networking** > **Ports** page. Additionally, TSAPI Services Port 450 is changed to Unencrypted Services Port 450.

By default, the Encrypted Services Port and Unencrypted Services Port are enabled.

New in Application Enablement Services Release 10.1.3

Avaya Aura® Application Enablement Services Release 10.1.3 supports the following new features and enhancements:

AE Services REST APIs (Web Telephony interface)

The Web Telephony interface (WTI) service is introduced in AE Services Release 10.1.2. It aims to include all existing APIs across subsequent AE Services 10.x releases.

In AE Services Release 10.1.3, the new APIs are introduced. For more information, see *Avaya Aura® Application Enablement Services Overview and Specification*.

New in Application Enablement Services Release 10.1.2

Avaya Aura® Application Enablement Services Release 10.1.2 supports the following new features and enhancements:

Support of Avaya Aura® application OVA with SHA256 hash algorithm

From Release 10.1.2, Avaya Aura® applications support the SHA256 hash algorithm for OVAs.

Support of deployment and upgrade of OVA with SHA256 hash algorithm on Solution Deployment Manager

From Release 10.1.2, System Manager Solution Deployment Manager and Solution Deployment Manager Client support the deployment and upgrade of an application using the OVA with the SHA256 hash algorithm.

Virtual IP support on AE Services Geo Redundant High Availability (GRHA) on Azure platform

From Release 10.1.2, AE Services GRHA supports Virtual IP (VIP) configuration on Azure platform.

Configuring a Virtual IP on the Azure platform enables recovery of the DMCC stations and monitors during a failover.

Real Time Agent Events

Starting from Release 10.1.2, AE Services will provide an event feed for real-time agent events. Business partners and customers can use this real-time information for various purposes, such as making accurate business decisions, creating custom or AI applications, and integrating with third-party customer experience (CX) solutions for both on-premises and cloud services.

What makes it different from today?

Avaya provides agent state change events, such as login/logout, as part of its SDK and CTI APIs. However, customers have requested additional events that have previously been restricted to Avaya applications (Trusted Applications). Third-party applications currently "poll" the agent state change information, making it near real-time but also resource-intensive. With the new event feed, any third-party app can avail the capability of receiving the agent state change events in real-time.

Starting from Release 10.1.2, AE Services introduces a new license type called Advance Agents. With this license, CTI applications receive real-time updates of the following agent events:

- Ready (Auto-in, Manual -in)
- Not Ready (Aux)
- Work Not ready (ACW)

Note:

To access this capability, the integration partner (CTI app developer) must work with Avaya to obtain the new SDK. The customer needs to purchase the Advance Agents license for the required quantity. Create Technical Support Ticket on DevConnect (@ https://www.avaya.com/devconnect) for more details.

AE Services REST APIs (Web Telephony interface)

The introduction of the WTI service in Release 10.1.2 offers existing AE Services CTI interfaces as REST APIs, enabling cloud services and on-premises CTI applications to access CTI capabilities through these REST APIs to meet specific business requirements.

The WTI service is being introduced gradually and aims to include all existing APIs across subsequent 10.x releases. The first set of APIs is available in AE Services 10.1.2 and is aimed at customers who use older TWS (Telephony Web Services) APIs. This set of APIs enables these customers to transition to REST APIs before TWS reaches its end of support.

Note:

A separate license is not required to use WTI. The WTI service consumes TSAPI and DMCC licenses in AE Services 10.1.2.

New in Application Enablement Services Release 10.1.0.2

Avaya Aura® Application Enablement Services Release 10.1.0.2 supports the following new features and enhancements:

Support for Call Work Code and Stroke Count

From Release 10.1.0.2 onwards, AE Services and Avaya Aura® Communication Manager support two new APIs, Call Work Code (CWC) and Stroke Count (SC). These third-party call control support APIs send CWC and SC to Avaya Aura® Communication Manager.

These APIs work if the ASAI version is 12 and above and the private data version is 18 and above for TSAPI and JTAPI applications. These APIs are exposed over JTAPI, TSAPI, DMCC, and CVLAN services on the AE Services server.

Log4j upgrade from version 1.x to version 2.x

From Release 10.1.0.2, logging framework has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.

New in Application Enablement Services Release 10.1

Avaya Aura® Application Enablement Services Release 10.1 supports the following new features and enhancements:

Support for Microsoft Windows Server Active Directory 2022

From Release 10.1, AE Services supports Microsoft Windows Server Active Directory 2022.

Support of Microsoft Windows 11 and Microsoft Windows Server 2022 (64-bits)

From Release 10.1, you can install AE Services Clients and SDK on the following Microsoft Windows operating systems:

- Microsoft Windows 11 Professional Edition (64-bits)
- Microsoft Windows Server 2022 Standard Edition (64-bits)

Support for TLS 1.3

From Release 10.1, AE Services supports the TLS version 1.3.

Enhancement to SMS Web service

From Release 10.1, AE Services enhances support for additional attributes in SMS. With this enhancement, you can view or edit the newly introduced Communication Manager fields, Hunt Group and Vector Directory Number.

Support of Remote backup utility

From Release 10.1, AE Services supports remote backup utility. You can take a periodic scheduled backup of AE Services database on a remote machine that has a Linux OS.

Support of Software-Only prerequisite check utility

From Release 10.1, AE Services supports Software-Only prerequisite check utility. It provides an overview of the RHEL host to ensure that the RHEL host satisfies all the conditions to install AE Services software-only.

Support of Red Hat Enterprise Linux 8.4

With Release 10.1, AE Services supports Red Hat Enterprise Linux 8.4.

Supported browsers

With Release 10.1, the following are the supported versions of the supported browsers:

- Microsoft Chromium Edge Release 93 and later
- Google Chrome Release 91 and later
- Mozilla Firefox Release 93 and later

Note:

From Release 10.1 and later, Microsoft Internet Explorer is no longer supported.

Enhancement to Log management

From Release 10.1, AE Services enhances support for getlogs utility to provide better diagnostics. You can now customize the period to collect the relevant logs using the getlogs utility.

Planned phase out of Telephony Web Service (TWS) of AE Services

In Release 10.1, AE Services supports TWS, but it will eventually be replaced with a RESTful web service. Greenfield customers can easily consume the upcoming REST APIs without the need for SDK. For more information, see the Avaya Product Support Notice at PSN020533u.

End-of-support of Microsoft Lync Server 2010

With Release 10.1, AE Services do not support Microsoft Lync Server 2010.

End-of-support of Appliance Virtualization Platform

From Release 10.1, Appliance Virtualization Platform is no longer available for deploying or upgrading the Avaya Aura® applications.

- To deploy the Avaya Aura® applications on Avaya-Supplied ESXi, use Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.x.
- To upgrade the Avaya Aura® applications, migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.x before upgrading the application.

End-of-support of AVP Utilities

With Release 10.1, Avaya Aura® applications do not support AVP Utilities.

Unsupported Avaya-provided servers

With Release 10.1, the following Avaya-provided servers are not supported:

- HP ProLiant DL360p G8
- HP ProLiant DL360 G9
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630
- Avaya Solutions Platform 120 offers

  Avaya Solutions Platform 120 and 130 have the same Dell PowerEdge R640 hardware configuration. Only Avaya Solutions Platform 120 is supported for migrating to Avaya Solutions Platform 130 Release 5.x.

Discontinued the AWS and KVM OVAs

From Release 10.1, Avaya Aura® applications will no longer have the Amazon Web Services (AWS) and Kernel-based Virtual Machine (KVM) OVAs. Alternately, you can continue to deploy the application by using the software-only offer.

For information about deploying, see the product-specific Software-only and Infrastructure as a Service Environments deployment guide.

For information about upgrading to Software-only, see the product-specific Upgrading guides.

Application Enablement Services feature matrix

The following table lists the feature matrix of Application Enablement Services from Release 7.x to Release 10.1.x. The features listed in the table cover the key features only.

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1 and Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 10.1.x
Third-party call control support for service observe					Y	Y
VMware 7.0					Y	Y
TSAPI 64-bit client for Windows and SDK					Y[c]	Y[c]
OVA signing	Y	Y	Y	Y[a]		Y[a]
IPv6 support	Y	Y	Y	Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1 and Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 10.1.x
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y	Y	Y
Compliance with DISA security STIGs	Y				Y	
Multi factor authentication	Y	Y	Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y	Y	Y
Support for TLS 1.3						Y
Red Hat Enterprise Linux (RHEL) 8.4						Y
Customer Root Access		Y	Y	Y	Y	Y
Preserve security hardening modes on upgrade		Y	Y	Y	Y	N[d]
Support for 16-digit dial plan		Y	Y	Y	Y	Y
Software-only support for KVM	Y	Y	Y			Y
Support for Software-only deployment	Y	Y	Y		Y[b]	Y[b]
Support for Hyper-V in Software-Only environment		Y	Y		Y[b]	Y[b]
Support for third-party software in Software-Only environment		Y	Y	Y	Y[b]	Y[b]
Support of Held Call ID on auto dial request by Application Enablement Services		Y	Y	Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance		Y	Y	Y	Y	
Support for Avaya Solutions Platform 130 Appliance		Y	Y	Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1 and Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 10.1.x
Support for G.722 codec			Y	Y	Y	Y
Support for 12–Party Conferencing			Y	Y	Y	Y
Real Time Agent Events						Y
REST APIs (Web Telephony Interface)						Y

[a] - OVA is available for VMware and not for KVM.

[b]- To install Application Enablement Services Release 8.1.3 FP in software-only environment, you must follow the following steps:

1. Install Release 8.1 or Release 8.1.1 ISO
2. Upgrade to Release 8.1.2.x FP
3. Upgrade to Release 8.1.3 FP

[c] - TSAPI client and SDK supports 64-bit architecture for Windows and Linux platforms which is backward compatible with AE Services Release 8.1.x server.

[d]- AE Services does not take any status backup of SELinux and Kernel FIPS mode during database backup. If the status of SELinux and Kernel FIPS mode is enabled on the current version, after upgrading to Release 10.1, you must enable the status manually.

Chapter 9: What's new in Branch Gateway

This chapter provides an overview of the new and enhanced features of Branch Gateway Release 10.1.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 10.1

The following section describes new features and enhancements that are available in Branch Gateway 10.1.

Minimum Password Length

The default value for minimum password length was changed from 8 to 14 characters. At first install the root user can override the new limit once. In addition, the minimum password length can be set using the **`login authentication min-password-length`** command.

DHCP status

With Release 10.1, DHCP is enabled by default on vlan 1.

At first install, the user will be asked if DHCP should be disabled so that a static address can be configured.

T.38 fax Transport over RTP/SRTP

The present T.38 Fax relay feature employs the use of UDPTL transport. This does not provide any encryption support. From Release 10.1, page 2 of the IP Codec-Set screen on the Communication Manager SAT interface allows to administer SRTP transport for T-38 fax. This feature will provide the same encryption technique and strength as Avaya supports for voice and video transport.

Note:

This feature is not supported in gateways that include MP80, MP20, and MP10 modules and gateways with 20 or 25 channel on-board DSPs. Only MP120, MP160 modules, or the 40 channel on-board DSPs are supported.

Support for Edge Gateway mode

With Release 10.1, Gateway introduces an Edge Mode - Internet Friendly Gateway which allows to deploy gateways in a remote location without the need for an Enterprise connection (VPN, MPLS links). With the Edge Gateway feature, endpoints and gateways can operate in local NAT address domains at the branch office sites, while the Avaya server products remain in the data centers. The data centers operate in a private address space as well. The Avaya Session Border Controller (ASBCE) is the conversion element that supports end-to-end communication from the data centers to public service provider networks and the branch office sites. The solution also supports T.38 secure fax transport over RTP.

Note:

This feature is not supported in gateways that include MP80, MP20, and MP10 modules and gateways with 20 or 25 channel on-board DSPs. Only MP120, MP160 modules, or the 40 channel on-board DSPs are supported.

Announcement Files

The following commands are added for announcement files:

- **`copy announcement-file https <URL> [transfer-type]`**
- **`copyedge announcement-file scp <file directory path> <file server IP address>`**
- **`copy https announcement-file <file-url> [transfer-type] [<destination-filename>]`**
- **`copyedge scp announcement-file <file directory path> <file server IP address>`**

Configuration Files

The following commands are added for configuration files:

- **`copy startup-config https <URL> [transfer-type]`**
- **`copyedge startup-config scp <file directory path> <file server IP address>`**
- **`copy https startup-config <URL> [transfer-type]`**
- **`copyedge scp startup-config <file directory path> <file server IP address>`**

DHCP binding file

The following commands are added for configuration files:

- **`copy dhcp-binding https <URL> [transfer-type]`**
- **`copy dhcp-binding scp <file directory path> <file server IP address>`**

DHCP Client

The following commands were updated to support VLAN interface for DHCP client:

- **[no] ip address dhcp**
- **[no] ip dhcp client client-id {hex hex-string}**
- **[no] ip dhcp client hostnamehost-name**
- **[no] ip dhcp client lease days [hours [minutes]]**
- **[no] ip dhcp client request {domain-name | dns-nameserver | router }**
- **[no] ip dhcp client route tracktrack-index**

EASG authentication

The following commands are added for EASG authentication:

- **copy https easg <URL> [saf <SAF-value>][transfer type]**
- **copyedge scp easg <file directory path> <file server IP address>**

Enhancements to the firmware management commands

The following firmware management commands are added for file transfer operations with HTTPS:

- **copy https SW_imageA <URL> [transfer-type]**
- **copy https SW_imageB <URL> [transfer-type]**
- **copyedge scp SW_imageA <file directory path> <file server IP address>**
- **copyedge scp SW_imageB <file directory path> <file server IP address>**
- **copy https module <URL> <module_number> [transfer-type]**
- **copyedge scp module <file directory path> <file server IP address>**

The following command has been updated to display the trust anchor version in use:

- **dir {module_number | file-system [directory]}**

NAT Keep Alive packets

The following commands have been added to support the NAT TCP and NAT UDP keep alive messages:

- **- tcp keepalive [timer value]**

  - udp keepalive [timer value]

Enhancement to the MGC configuration commands

Updated the following MGC configuration commands in support of Edge Gateway mode:

- **set link-encryption h248reg {protocol} <yes | no>**
- **show mgc**

- **set mgc list <controller entry>**

Packet sniffing

The following packet sniffing commands are added for file transfer operations with HTTPS:

- **copy capture-file https <URL> [transfer-type]**
- **copyedge capture-file scp <file directory path> <file server IP address>**

Syslog files

The following commands are added for Syslog files:

- **copy syslog-file https <URL> [transfer-type]**
- **copyedge syslog-file scp <file directory path> <file server IP address>**

Enhancement to the Root-CA Certificate commands

Updated the following Root-CA certificate commands to support the Web trust store:

- **show root-ca <app>**
- **copy scp root-ca <app> <filename> <ip>**
- **copy usb root-ca <app> usbdevice0 <filename>**
- **erase root-ca <app> <index>**

The following commands are added for Root-CA certificates:

- **copy certificate root-ca <appA> <appB> <index>**
- **copy https root-ca <app> <URL> [transfer-type]**
- **copyedge scp root-ca <file directory path> <file server IP address>**

Enhancement to the Gateway Identity Certificate commands

Updated the following Gateway Identity certificate commands to support the Web trust store:

- **show gw-identity-cert <app>**
- **copy scp gw-identity-cert <app> <filename> <ip>**
- **copy usb gw-identity-cert <app> usbdevice0 <filename>**
- **erase gw-identity-cert <app>**

The following commands are added for Gateway Identity certificates:

- **copy certificate gw-identity-cert <appA> <appB>**
- **copy https gw-identity-cert <app> <URL> [transfer-type]**
- **copyedge scp gw-identity-cert <file directory path> <file server IP address>**

Trust Anchor

Added the following commands for Trust Anchors:

- **`set web trust-anchors [enable|disable]`**
- **`copy https trust-anchors <URL> <file directory path>`**
- **`copy usb trust-anchors <file directory path>`**
- **`copy scp trust-anchors <file directory path> <file server IP address>`**
- **`copyedge trust-anchors <file directory path> <file server IP address>`**
- **`show http`**
- **`show download trust-anchors status`**

Branch Gateway new features

The following table lists the new features of Branch Gateway supported in recent releases.

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

Chapter 10: What's new in Avaya Aura® Media Server

This chapter provides an overview of the new and enhanced features of Avaya Aura® Media Server Release 10.1.

For more information about these features and administration, see:

- *Avaya Aura® Media Server Overview and Specification*
- *Implementing and Administering Avaya Aura® Media Server*
- *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*
- *Deploying and Updating Avaya Aura® Media Server Appliance*

For latest information, see Avaya Aura® Media Server Release 10.1 Release Notes on the Avaya Support website at https://download.avaya.com/css/public/documents/101081316.

New in Avaya Aura® Media Server 10.1.0

- Support for Red Hat Enterprise Linux® Server 7.x is removed.
- Support for Red Hat Enterprise Linux® Server 8.x. is added.

Chapter 11: What's new in Avaya Experience Platform™ On-Prem

This chapter provides an overview of the new and enhanced features of Avaya Experience Platform™ On-Prem Release 10.1.x.

New in Avaya Experience Platform™ On-Prem Release 10.1.2

Avaya Experience Platform™ On-Prem Release 10.1.2 supports the following new feature:

Include Universal Call ID (UCID) details in Call Detail Recording (CDR)

Various third-party products use UCID in CDR. These third-party products track voice recordings and other features that help call center agents perform their jobs. Currently, a user must enable Special Application (SA) 8702 to get UCID details in the CDR records.

From Release 10.1.2, users can get UCID details in CDR records with the new field **Record UCID?** without enabling SA8702. The new field is available on page 1 of the CDR SYSTEM PARAMETERS form or can be accessed from **Element-cut through** on the System Manager web console. If the **Record UCID?** field is set to `y`, configure the customized CDR **Data Item** > **ucid** on page 2 of the CDR SYSTEM PARAMETERS form. Enabling this feature on the CDR System Parameters form does not impact other features of SA8702.

New in Avaya Experience Platform™ On-Prem Release 10.1.0.2

Avaya Experience Platform™ On-Prem Release 10.1.0.2 supports the following new feature:

Third-Party Call Control (3PCC) Support for Call Work Codes (CWC) and Stroke Counts (SC)

AE Services from Release 10.1.0.2 supports the Avaya Experience Platform™ On-Prem CWC and SC APIs. These 3PCC support APIs send CWC and SC to Communication Manager on Release 10.1.0.2.

These APIs work if the ASAI version is 12 and above and the private data version is 18 and above. These APIs are exposed over JTAPI, TSAPI, DMCC, and CVLAN services on AE Services server.

For more information on CWC and SC, see *Avaya Experience Platform™ On-Prem (formerly Avaya Aura® Call Center Elite) Feature Reference*.

New in Avaya Experience Platform™ On-Prem Release 10.1

Avaya Experience Platform™ On-Prem Release 10.1 supports the following new features:

- Support for Look-Ahead Interflow (LAI) over SIP
- Support for Unicode reason codes in Operations Support System Interface (OSSI)

Support for Look-Ahead Interflow (LAI) over SIP

With Release 10.1, a new header is added to SIP 182 and 183 messages in order to indicate acceptance of a LAI request. To enable the new behaviour both the Communication Managers involved in the LAI must be on Release 10.1. The LAI over SIP functionality is same as LAI over ISDN trunks. The trunk group receiving the LAI should set the setting **Convert 180 to 183 for Early Media?** to `n` unless you want the LAI to be accepted when Early Media is negotiated with SIP 183.

For more information, see *Avaya Experience Platform™ On-Prem (formerly Avaya Aura® Call Center Elite) Feature Reference* and *Administering Avaya Experience Platform™ On-Prem (formerly Avaya Aura® Call Center Elite)*.

Support for Unicode reason codes in Operations Support System Interface (OSSI)

With Release 10.1, Avaya Experience Platform™ On-Prem supports Unicode reason codes in OSSI. With this functionality, new native names of Logout and Aux Work reason code are added.

Chapter 12: What's new in Avaya Device Adapter

This chapter provides an overview of the new and enhanced features of Avaya Device Adapter Release 10.1.x.

For more information about these features and administration, see the *Avaya Device Adapter Snap-in Reference* guide.

New in this release

What's New in Avaya Device Adapter Release 10.1.2

Supports CSDK version update to enable registration with same pair of Session Managers

If a user has multiple devices in different geographic locations, from Release 10.1.2, Avaya Device Adapter supports CSDK version update, which enables an user to register devices with same pair of Session Managers regardless of the location of the devices.

What's new in Avaya Device Adapter Release 10.1

Enhancement to the Hotline Intercom feature

With Release 10.1, the Device Adapter provides a visual indication for an unconfirmed incoming Hotline Intercom call, if NAIA (No Answer Indication Allowed) mnemonic is configured in the Features field of the Avaya Aura® System Manager endpoint. The feature applies only for all Hotline Intercom keys configured on the Device Adapter Unistim and digital phones.

Supports configuration of the Session Manager registration timer

From Release 10.1, users can configure time in minutes using the **SM registration timeout** attribute or the Session Manager automatically unregisters user devices that fail to maintain registration. The configuration range is 5 to 60 minutes, and the default value is 60 minutes.

Supports Off-Hook alerts for Analog, Digital, IP/Unistim set types

Allows phones to automatically make calls to a pre-specified directory number (OHADN) after a pre-specified time interval (OHATimeout) and after the Dial Tone timeout has passed, that is, when a user goes off-hook. To access the off-hook alarms feature, you need to configure values for the **DN for Off Hook Alert** and **Off Hook Alert timeout** attributes in the **Off Hook Alert** section.

Supports Unistim firmware management for Avaya Device Adapter

From Release 10.1, Avaya Device Adapter supports firmware upgrades by incorporating CLI commands. To enable or disable firmware upgrades in the Unistim phones in the Avaya Device Adapter, users can navigate to **Elements** > **Avaya Breeze** > **Configuration** > **Attributes** > **Enable automatic firmware upgrades**.

Supports on-hook dialing feature

Enables users to call back numbers from their call log by sending full dialed numbers at a time. Numbers in the on-hook dialing state are dialed without the numbers matching against the dial plan.

Supports MGC Loadware Management from Avaya Device Adapter

From Release 10.1, Avaya Device Adapter supports MGC loadware management by introducing CLI commands such as **`umsFirmwareShow`** and **`umsSwitchFirmware <fw_version>`**.

Avaya Device Adapter feature matrix

The following table lists the feature matrix of Avaya Device Adapter from Release 8.x to Release 10.1.x. The features listed in the table covers the key features only.

Features	Release 8.0.x	Release 8.1.x	Release 10.1.x
Ad hoc conference	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Autodial	UNIStim, Digital **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital	UNIStim, Digital
Busy Indicator	Not supported	UNIStim, Digital	UNIStim, Digital

Table continues…

Features	Release 8.0.x	Release 8.1.x	Release 10.1.x
Call Forward All Calls (CFW) along with the Busy Indicator feature to manage CFW on behalf of another extension	Not supported	UNIStim1, Digital1 This feature is not supported on 2001 and 3901 endpoints. **Note:** Release 8.1 did not support this feature.	UNIStim1, Digital1
Call Forward - all calls / busy / no answer	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Caller List / Redial List / Personal Directory	UNIStim, Digital[1] **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital[1]	UNIStim, Digital[1]
Call Pickup (Directed / Group / Ringing Number)	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Call Park and Call Pickup	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Call Waiting	UNIStim, Digital **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital	UNIStim, Digital
Corporate Directory	UNIStim[1], Digital[1] **Note:** Release 8.0 did not support this feature.	UNIStim[1], Digital[1]	UNIStim[1], Digital[1]

Table continues…

Features	Release 8.0.x	Release 8.1.x	Release 10.1.x
Context-sensitive key access - idle / offhook / dialed / ringing / active call state	UNIStim, Digital[1] **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital[1]	UNIStim, Digital[1]
End-to-end signaling (DTMF)	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Fixed feature key access	UNIStim, Digital **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital	UNIStim, Digital
Hold / retrieve	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Hot Line - multiple types on CS 1000	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Last Number Redial	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Making, answering, and releasing a basic call	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog

Table continues…

Features	Release 8.0.x	Release 8.1.x	Release 10.1.x
Make Set Busy	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Malicious Call Trace	Not supported	UNIStim, Digital, Analog **Note:** Releases 8.1 and 8.1.1 did not support Analog.	UNIStim, Digital, Analog
Message Waiting Indication (including audio)	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Message Waiting Key and Lamp for voice mail	UNIStim, Digital, Analog[1] **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog[1]	UNIStim, Digital, Analog[1]
Multiple Appearance Directory Numbers (MADN)	UNIStim, Digital, Analog[2] **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog[2]	UNIStim, Digital, Analog[2]
Multiple Device Access: Allows concurrent registrations of a minimum of 2 up to a maximum of 10 SIP devices with the same extension. However, Avaya recommends that out of the 10 devices, only 1 device must be a Device Adapter UNIStim endpoint.	Not supported	UNIStim	UNIStim
Release key - disconnect a call	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog

Table continues…

Features	Release 8.0.x	Release 8.1.x	Release 10.1.x
Ring Again	UNIStim, Digital **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Set Display - calling / called / redirecting name and number.	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Set Display - time and date, call timer, and so on.	UNIStim, Digital, Analog[1] **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog[1]	UNIStim, Digital, Analog[1]
Speed Dial	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Sequential Registration: Allows registration of only one endpoint at one time.	UNIStim[3], Digital[3], Analog[3] **Note:** Release 8.0 supported only UNIStim[3].	UNIStim[4], Digital[3], Analog[3]	UNIStim[4], Digital[3], Analog[3]
Support for 50 Avaya Breeze® platform nodes and 2,00,000 endpoints.	50 Avaya Breeze® platform nodes retroactively supported. **Note:** Release 8.0 supported only 35 Avaya Breeze® platform nodes.	Yes	Yes
SMGR IU for Device Adapter	Yes **Note:** Release 8.0 did not support this feature.	Yes	Yes

Table continues…

Features	Release 8.0.x	Release 8.1.x	Release 10.1.x
SMGR IU for Media Gateway	Yes **Note:** Release 8.0 did not support this feature.	Yes	Yes
Transfer - blind as well as consultative	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Privacy Release	UNIStim, Digital, Analog **Note:** Release 8.0 supported only Unistim.	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Presence Service Notification: Provides presence status indication to non-Device Adapter endpoints	Not supported	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Virtual Office (VO)	Not supported	UNIStim with soft keys The endpoint must support Home and Virtual soft keys **Note:** Release 8.1 did not support this feature.	UNIStim with soft keys The endpoint must support Home and Virtual soft keys
Virtual Office Emergency dialing	Not supported	UNIStim with soft keys. In Releases 8.1.1 and 8.1.2, the endpoint also supported Emergency soft key. **Note:** Release 8.1 did not support this feature.	UNIStim with soft keys.

Table continues…

Features	Release 8.0.x	Release 8.1.x	Release 10.1.x
Virtual Office DVLA Timer	Not supported	UNIStim with soft keys **Note:** Releases 8.1, 8.1.1 and 8.1.2 did not support this feature.	UNIStim with soft keys.
Remote Cluster	Not supported	UNIStim **Note:** Releases 8.1, 8.1.1 and 8.1.2 did not support this feature.	UNIStim
Limit Number of Concurrent Calls (LNCC)	Not supported	UNIStim **Note:** Releases 8.1, 8.1.1 and 8.1.2 did not support this feature.	UNIStim
CS2100	Not supported	UNIStim, Digital, Analog **Note:** Releases 8.1, 8.1.1 and 8.1.2 did not support this feature.	UNIStim, Digital, Analog
Uses AADS service account to access the Device Adapter Corporate Directory	Not supported	UNIStim **Note:** This feature is supported only from Release 8.1.4	UNIStim
Server side NAT	Not supported	UNIStim **Note:** This feature is supported only from Release 8.1.4	UNIStim

Table continues…

Features	Release 8.0.x	Release 8.1.x	Release 10.1.x
Fax and modem calls in pass-through mode	Not supported	Analog **Note:** This feature is supported only from Release 8.1.4	Analog
Hebrew support using CPND	Not supported	UNIStim **Note:** This feature is supported only from Release 8.1.4	UNIStim
Handsfree Voice call	Not supported	UNIStim, Digital **Note:** This feature is supported only from Release 8.1.4	UNIStim, Digital
ADA EM access in cloud deployment	Not supported	UNIStim, Digital, Analog **Note:** This feature is supported only from Release 8.1.4	UNIStim, Digital, Analog
No Answer Indication for Hotline Intercom	Not supported	Not supported	Unistim, Digital
Session Manager registration timer	Not supported	Not supported	Unistim, Digital, Analog
Off-Hook Alarms implementation	Not supported	Not supported	Unistim, Digital, Analog
On-hook dialing feature	Not supported	Not supported	Unistim
MGC loadware management	Not supported	Not supported	Digital, Analog
Unistim firmware management	Not supported	Not supported	Unistim

[1] Applies to a subset of the set types. For example, Digital[1] may apply to the 39xx phones, that is, 3903, 3904, and so on.

[2] Analog stations may have a MADN assigned, but have only one available line appearance. Digital and UNIStim stations may have one or more line appearances for the directory number.

[3] Used for recovery in an event of a network failure.

[4] In addition to providing recovery in an event of a network failure, can also be used for switching between UNIStim endpoints.

Chapter 13: Resources

Documentation

The following table lists the documents related to the components of Avaya Aura® Release 10.1.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 to Release 10.1	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
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

Table continues…

Title	Description	Audience
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 10.1.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		
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

Table continues…

Title	Description	Audience
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 to Release 10.1.x	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
20970W	Introducing Avaya Device Adapter
20980W	What's New with Avaya Aura®

Table continues…

Course code	Course title
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager Release 10.1
61451V	Administering Avaya Aura® Communication Manager Release 10.1

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 **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **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 key word or key words 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 the topic. 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 http://www.avaya.com/support.
2. Log in to the Avaya support website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

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) when there is no update, service pack, or release fix, but the business unit or Avaya Services need 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

A

AE Services 10.1
new in release ... 64
AE Services 10.1.0.2
new in release ... 64
AE Services 10.1.2
new in release ... 63
AE Services 10.1.3
new in release ... 62
AE Services 10.1.3.1
new in release ... 62
Application Enablement Services
feature matrix ... 66
what's new ... 62
Avaya Aura application upgrade ... 26
Avaya Aura components
Release 10.1.x ... 8
Avaya Aura®
overview ... 13
Avaya Aura® application
browsers ... 32
ESXi version ... 29
JITC compliant ... 33
supported gateways ... 32
supported servers ... 30
Avaya Aura® application OVAs
Linux operating system version ... 26
Avaya Aura® offers ... 13
Avaya Device Adapter
feature matrix ... 78
what's new ... 77
Avaya Device Adapter 10.1 [What's new] ... 77
Avaya support website ... 90

B

Branch Gateway
new features ... 73
what's new ... 69
browsers
Avaya Aura® application ... 32

C

Call Center Elite
what's new ... 75
client Solution Deployment Manager ... 21
Communication Manager
feature matrix ... 56
new in release 10.1 ... 54
what's new ... 51
Communication Manager new in release 10.1.0.2 ... 53
Communication Manager new in release 10.1.2 ... 52
Communication Manager new in release 10.1.3 ... 51, 52
components
virtualized environment ... 15

D

document changes ... 9

E

ESXi version
Avaya Aura® application ... 29

F

feature matrix
Application Enablement Services ... 66
Avaya Device Adapter ... 78
Branch Gateway ... 73
Communication Manager ... 56
Presence Services ... 60
Session Manager ... 49
System Manager ... 40
WebLM ... 44

I

IaaS
overview ... 18
Infrastructure as a Service
overview ... 18
InSite Knowledge Base ... 91

J

JITC compliant
Avaya Aura® application ... 33

L

Linux operating system version
Avaya Aura® application OVAs ... 26
Avaya Aura® application Software-only Environment ... 28

M

Media Server
what's new ... 74

N

new features in 10.1 69
new in 10.1 69
new in media server 10.1.0 74
new in release
- Application Enablement Services 10.1 64
- Application Enablement Services 10.1.0.2 64
- Application Enablement Services 10.1.2 63
- Application Enablement Services 10.1.3 62
- Application Enablement Services 10.1.3.1 62
- Session Manager 45
- Session Manager 10.1 46
- Session Manager 10.1.0.1 46
- Session Manager 10.1.3.4 45
- System Manager 10.1 37
- System Manager 10.1.0.1 36
- System Manager 10.1.0.2 35
- System Manager 10.1.2 34
- System Manager 10.1.3.3 34
- WebLM 10.1.2 42

new in release 10.1
- Communication Manager 54
- Presence Services 59

new in Release 10.1 76
new in release 10.1.0 74
new in Release 10.1.0.2 75
new in release 10.1.0.2 Communication Manager 53
new in Release 10.1.2 75
new in release 10.1.2 Communication Manager 52
new in release 10.1.3 Communication Manager 52
new in release 10.1.3.6 Communication Manager 51

O

offer
- Avaya virtualized appliance 13
- Infrastructure as a Service 13
- Software-only environment 13
- Virtualized Environment 13

overview 16
- Amazon Web Services (AWS) 19
- Google Cloud Platform 19
- IBM Cloud for VMware Solutions 19
- Microsoft Azure 19

P

PCN notification 92
Presence Services
- feature matrix 60
- new in release 10.1 59
- what's new 59

Product compatibility 9
PSN notification 92

R

related documentation 87
Release 10.1 76
Release 10.1.0.2 75
Release 10.1.2 75

S

SDM Client 22
Session Manager
- feature matrix 49
- new in release 45
- new in release 10.1.0.2 46
- what's new 45

Session Manager 10.1
- new in release 46

Session Manager 10.1.0.1
- new in release 46

Session Manager 10.1.3.4
- new in release 45

signing up
- PCNs and PSNs 93

software-only 16
Solution Deployment Manager 21
- supported applications 23

Solution Deployment Manager client 21
Solution Deployment Manager Client 22
support 90
supported applications 17
- Infrastructure as a Service 20
- VMware and ASP 130 14

supported gateways
- Avaya Aura® application 32

supported servers
- Avaya Aura® application 30

System Manager
- feature matrix 40
- what's new 34

System Manager 10.1
- new in release 37

System Manager 10.1.0.1
- new in release 36

System Manager 10.1.0.2
- new in release 35

System Manager 10.1.2
- new in release 34

System Manager 10.1.3.3
- new in release 34

T

technical assistance 9
topology
- Avaya applications on Infrastructure as a Service platform 20
- System Manager 14

training 89

U

upgrade
Branch Session Manager 26
Communication Manager 26
Session Manager 26

V

videos 90
viewing
PCNs 92
PSNs 92
virtualized environment 14
VMware components
Release 10.1.x 16

W

WebLM
feature matrix 44
what's new 42
WebLM 10.1.2
new in release 42
what's new 74
What's new [Avaya Device Adapter Release 10.1] 77
What's New in ADA Release 10.1.2 77
what's new 75, 76
Application Enablement Services 62
Avaya Device Adapter 77
Branch Gateway 69
Call Center Elite 75
Communication Manager> 51
Media Server 74
Presence Services 59
Session Manager 45
System Manager 34
WebLM 42