



What's New in Avaya Aura[®] Release 8.1.x

Release 8.1.x
Issue 16
October 2022

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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](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 INC., 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 INC. 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](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](http://www.mpegla.com).

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction	7
Purpose.....	7
Avaya Aura® Release 8.1.3 components.....	7
Product compatibility.....	8
Technical Assistance.....	8
Change history.....	8
Chapter 2: Avaya Aura® overview	12
Avaya Aura® applications deployment offers.....	12
Avaya Aura® Virtualized Appliance overview.....	13
Virtualized Environment overview.....	15
Overview of Infrastructure as a Service environment.....	17
Software-only environment overview.....	20
Solution Deployment Manager overview.....	21
Solution Deployment Manager Client.....	23
Solution Deployment Manager.....	24
Avaya Aura® applications upgrade.....	26
Support for VMware components.....	26
Supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura® application OVAs.....	27
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.....	31
Supported browsers.....	31
Chapter 3: What's new in Appliance Virtualization Platform	33
New in this Release.....	33
New in Appliance Virtualization Platform Release 8.1.3.....	33
New in Appliance Virtualization Platform Release 8.1.2.....	33
New in Appliance Virtualization Platform Release 8.1.1.....	34
New in Appliance Virtualization Platform Release 8.1.....	34
Appliance Virtualization Platform feature matrix.....	35
Chapter 4: What's new in AVP Utilities	37
New in this release.....	37
New in AVP Utilities Release 8.1.3.....	37
New in AVP Utilities Release 8.1.2.....	38
New in AVP Utilities Release 8.1.1.....	38
New in AVP Utilities Release 8.1.....	38
AVP Utilities feature matrix.....	38
Chapter 5: What's new in System Manager	40

New in this release.....	40
New in System Manager Release 8.1.3.6.....	40
New in System Manager Release 8.1.3.5.....	41
New in System Manager Release 8.1.3.3.....	41
New in System Manager Release 8.1.3.1.....	42
New in System Manager Release 8.1.3.....	42
New in System Manager Release 8.1.2.....	44
New in System Manager Release 8.1.1.....	45
New in System Manager Release 8.1.....	46
System Manager feature matrix.....	49
Chapter 6: What's new in WebLM.....	51
New in this release.....	51
New in WebLM Release 8.1.3.5.....	51
New in WebLM Release 8.1.3.....	51
New in WebLM Release 8.1.2.....	52
New in WebLM Release 8.1.1.....	52
New in WebLM Release 8.1.....	52
WebLM feature matrix.....	53
Chapter 7: What's new in Session Manager.....	54
New in this release.....	54
New in Session Manager Release 8.1.3.5.....	54
New in Session Manager Release 8.1.3.1.....	54
New in Session Manager Release 8.1.3.....	55
New in Session Manager Release 8.1.2.....	56
New in Session Manager Release 8.1.1.....	56
New in Session Manager Release 8.1.....	57
Session Manager feature matrix.....	58
Chapter 8: What's new in Communication Manager.....	60
New in this release.....	60
New in Communication Manager Release 8.1.3.5.....	60
New in Communication Manager Release 8.1.3.1.....	61
New in Communication Manager Release 8.1.3.....	61
New in Communication Manager Release 8.1.2.....	62
New in Communication Manager Release 8.1.1.....	63
New in Communication Manager Release 8.1.....	64
Communication Manager feature matrix.....	65
Chapter 9: What's new in Presence Services.....	68
New in Presence Services Release 8.1.4.....	68
New in Presence Services Release 8.1.3.....	69
New in Presence Services Release 8.1.2.....	69
New in Presence Services Release 8.1.....	70
Presence Services feature matrix.....	70
Chapter 10: What's new in Application Enablement Services.....	72

New in this release.....	72
New in Application Enablement Services Release 8.1.3.5.....	72
New in Application Enablement Services Release 8.1.3.1.....	73
New in Application Enablement Services Release 8.1.3.....	73
New in Application Enablement Services Release 8.1.2.1.....	74
New in Application Enablement Services Release 8.1.2.....	74
New in Application Enablement Services Release 8.1.1.....	75
New in Application Enablement Services Release 8.1.....	75
Application Enablement Services feature matrix.....	77
Chapter 11: What's new in Branch Gateway.....	79
New in Branch Gateway Release 8.1.3.....	79
New in Branch Gateway Release 8.1.2.....	79
New in Branch Gateway Release 8.1.....	80
Branch Gateway new features.....	81
Chapter 12: What's new in Call Center Elite.....	82
New in Call Center Elite Release 8.1.3.....	82
New in Call Center Elite Release 8.1.2.....	83
New in Call Center Elite Release 8.1.1.....	84
New in Call Center Elite Release 8.1.0.....	84
Chapter 13: What's new in Avaya Device Adapter.....	85
What's new in Avaya Device Adapter Release 8.1.4.....	85
What's new in Avaya Device Adapter Release 8.1.3.....	85
What's new in Avaya Device Adapter Release 8.1.2.....	86
What's new in Avaya Device Adapter Release 8.1.1.....	87
Avaya Device Adapter feature matrix.....	87
Chapter 14: Resources.....	94
Documentation.....	94
Finding documents on the Avaya Support website.....	97
Accessing the port matrix document.....	98
Avaya Documentation Center navigation.....	98
Training.....	99
Viewing Avaya Mentor videos.....	99
Support.....	100
Using the Avaya InSite Knowledge Base.....	100
Appendix A: PCN and PSN notifications.....	102
PCN and PSN notifications.....	102
Viewing PCNs and PSNs.....	102
Signing up for PCNs and PSNs.....	103

Chapter 1: Introduction

Purpose

This document provides an overview of the new and enhanced features of Avaya Aura® Release 8.1.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 8.1.3 components

Product component	Release version
Appliance Virtualization Platform	8.1.3
AVP Utilities	8.1.3
System Manager	8.1.3
WebLM	8.1.3
Session Manager	8.1.3
Communication Manager	8.1.3
Branch Gateway	8.1.3
Presence Services	8.1.4
Application Enablement Services	8.1.3

Table continues...

Product component	Release version
Call Center Elite	8.1.3
Device Adapter	8.1.4
Communication Manager Messaging	7.0
Media Server	8.0

Product compatibility

For the latest and most accurate compatibility information, go to <https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

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	October 2022	Added the section New in System Manager Release 8.1.3.6 on page 40.
15	August 2022	Updated the section New in Session Manager Release 8.1.3 on page 55.

Table continues...

Issue	Date	Summary of changes
14	June 2022	<p>For Release 8.1.3.5, added the following sections:</p> <ul style="list-style-type: none"> • New in System Manager Release 8.1.3.5 on page 41 • New in WebLM Release 8.1.3.5 on page 51 • New in Session Manager Release 8.1.3.5 on page 54 • New in Communication Manager Release 8.1.3.5 on page 60 • New in Application Enablement Services Release 8.1.3.5 on page 72 <p>For Release 8.1.3.5, updated the section: Supported browsers on page 31</p>
13	October 2021	<p>For Release 8.1.3.3, added the New in System Manager Release 8.1.3.3 on page 41 section.</p>
12	June 2021	<p>For Device Adapter Release 8.1.4, added the What's new in Avaya Device Adapter Release 8.1.4 on page 85 section.</p> <p>For Device Adapter Release 8.1.4, updated the Avaya Device Adapter feature matrix on page 87 section.</p>
11	April 2021	<p>For Presence Services Release 8.1.4, added the New in Presence Services Release 8.1.4 on page 68 section.</p>
10	February 2021	<p>For Release 8.1.3.1, added the following sections:</p> <ul style="list-style-type: none"> • New in System Manager Release 8.1.3.1 on page 42 • New in Session Manager Release 8.1.3.1 on page 54 • New in Communication Manager Release 8.1.3.1 on page 61 • New in Application Enablement Services Release 8.1.3.1 on page 73
9	November 2020	<p>Updated the following sections:</p> <ul style="list-style-type: none"> • Supported ESXi version on page 29 • New in System Manager Release 8.1.3 on page 42

Table continues...

Issue	Date	Summary of changes
8	October 2020	<p>For Release 8.1.3, added the following sections:</p> <ul style="list-style-type: none"> • New in Appliance Virtualization Platform Release 8.1.3 on page 33 • New in AVP Utilities Release 8.1.3 on page 37 • New in System Manager Release 8.1.3 on page 42 • New in WebLM Release 8.1.3 on page 51 • New in Session Manager Release 8.1.3 on page 55 • New in Communication Manager Release 8.1.3 on page 61 • New in Presence Services Release 8.1.3 on page 69 • New in Application Enablement Services Release 8.1.3 on page 73 • New in Branch Gateway Release 8.1.3 on page 79 • New in Call Center Elite Release 8.1.3 on page 82 • What's new in Avaya Device Adapter Release 8.1.3 on page 85 <p>For Release 8.1.3, updated the following sections:</p> <ul style="list-style-type: none"> • Support for VMware components on page 26 • Supported ESXi version on page 29
7	June 2020	<p>For Release 8.1.2.1, added the section: New in Application Enablement Services Release 8.1.2.1 on page 74</p>
6	March 2020	<p>For Release 8.1.2, added the following sections:</p> <ul style="list-style-type: none"> • New in Appliance Virtualization Platform Release 8.1.2 on page 33 • New in AVP Utilities Release 8.1.2 on page 38 • New in System Manager Release 8.1.2 on page 44 • New in WebLM Release 8.1.2 on page 52 • New in Session Manager Release 8.1.2 on page 56 • New in Communication Manager Release 8.1.2 on page 62 • New in Presence Services Release 8.1.2 on page 69 • New in Application Enablement Services Release 8.1.2 on page 74 • New in Branch Gateway Release 8.1.2 on page 79 • What's new in Avaya Device Adapter Release 8.1.2 on page 86
5	January 2020	<p>Updated the section: New in Communication Manager Release 8.1.1 on page 63</p>

Table continues...

Issue	Date	Summary of changes
4	December 2019	<p>Updated the following sections:</p> <ul style="list-style-type: none"> • Supported applications in Virtualized Environment on page 15 • Supported applications in Infrastructure as a Service Environment on page 20
3	October 2019	<p>For Release 8.1.1, added the following sections:</p> <ul style="list-style-type: none"> • New in Appliance Virtualization Platform Release 8.1.1 on page 34 • New in AVP Utilities Release 8.1.1 on page 38 • New in System Manager Release 8.1.1 on page 45 • New in Session Manager Release 8.1.1 on page 56 • New in WebLM Release 8.1.1 on page 52 • New in Communication Manager Release 8.1.1 on page 63 • New in Application Enablement Services Release 8.1.1 on page 75 • New in Call Center Elite Release 8.1.1 on page 84 • What's new in Avaya Device Adapter Release 8.1.1 on page 87
2	June 2019	<p>Added the Accessing the port matrix document on page 98 section.</p> <p>Updated the following sections:</p> <ul style="list-style-type: none"> • Avaya Aura overview on page 12 • Supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura application OVAs on page 27 • Supported Red Hat Enterprise Linux operating system versions for Software-only Environment on page 28 • Supported servers for Avaya Aura applications on page 30 • New in Application Enablement Services Release 8.1 on page 75
1	June 2019	Release 8.1 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 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 single authentication

Avaya Aura[®] applications deployment offers

Avaya Aura[®] supports the following deployment offers:

- Avaya Aura[®] Virtualized Appliance (VA): Avaya-provided server, Avaya Aura[®] Appliance Virtualization Platform, based on the customized OEM version of VMware[®] ESXi 6.5.
- Avaya Aura[®] Virtualized Environment (VE): Customer-provided VMware infrastructure and Kernel-based Virtual Machine (KVM).
- Avaya Aura[®] on Infrastructure as a Service: Amazon Web Services, Microsoft Azure, Google Cloud Platform, and IBM Bluemix.
- Software-only environment: Deployment on the Red Hat Enterprise Linux operating system.

Avaya Aura® Virtualized Appliance overview

Avaya Aura® Virtualized Appliance is a turnkey solution. Avaya provides the hardware, all the software including the VMware hypervisor, and also offers the customer support of the setup.

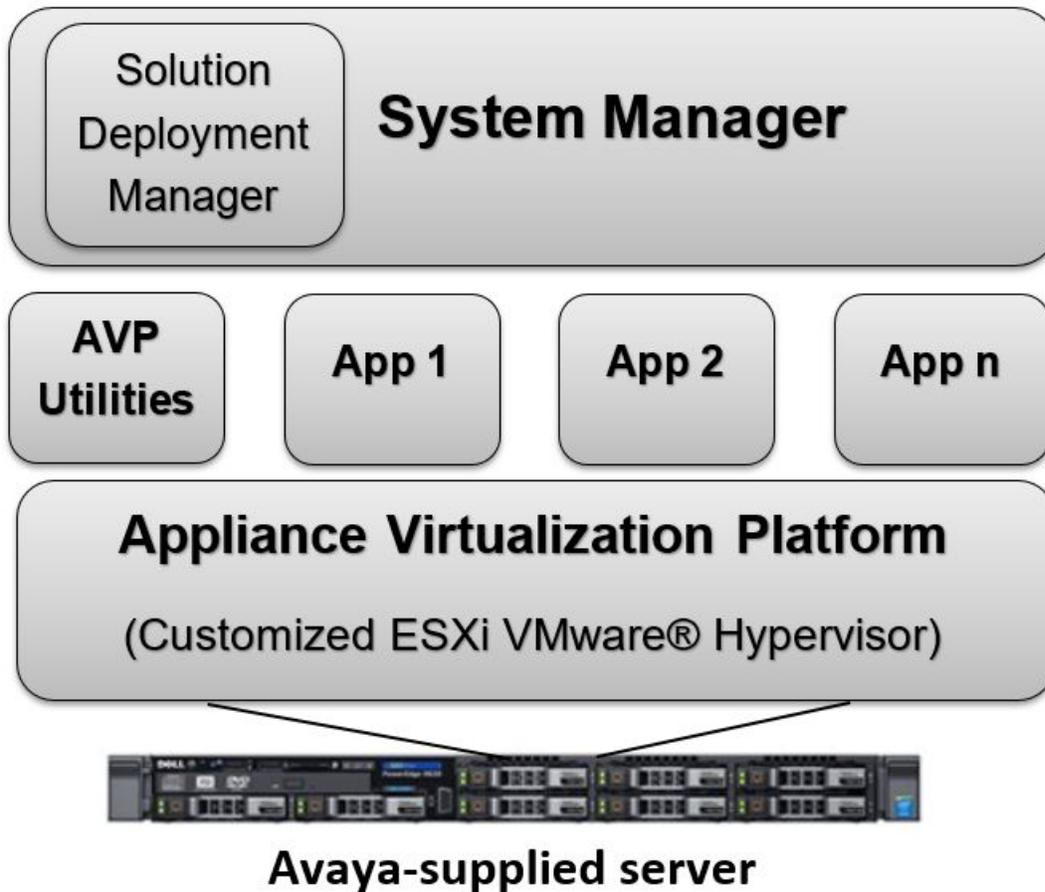
The Virtualized Appliance offer is different from Avaya Aura® Virtualized Environment, where Avaya provides the Avaya Aura® application software and the customer provides and supports the VMware hypervisor and the hardware on which the hypervisor runs.

Deployment on the Appliance Virtualization Platform server is performed using the System Manager Solution Deployment Manager or the Solution Deployment Manager client.

Appliance Virtualization Platform overview

From Avaya Aura® Release 7.0 and later, Avaya provides the VMware®-based Avaya Aura® Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications. The Appliance Virtualization Platform replaces the System Platform.

Avaya Aura® Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 6.5. With Avaya Aura® Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Avaya Aura® Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.



Avaya Aura® Virtualized Appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360p G8, and HP ProLiant DL360 G9
- Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640
- Avaya S8300E

*** Note:**

- With WebLM Release 7.x and later, you cannot deploy WebLM on S8300E Server running on Avaya Aura® Appliance Virtualization Platform.
- Common Servers using ESXi 6.0 or 6.5 can require more memory than System Platform or ESXi 5.5. For information about Avaya Aura® Appliance Virtualization Platform memory requirements and memory validation process, see PSN027060u and the Avaya Aura® Release Notes on the Avaya Support website.

You can deploy the following applications on Appliance Virtualization Platform:

- AVP Utilities 8.1.3
- System Manager 8.1.3
- Session Manager 8.1.3
- Branch Session Manager 8.1.3
- Communication Manager 8.1.3
- Application Enablement Services 8.1.3
- WebLM 8.1.3
- Communication Manager Messaging 7.0

*** Note:**

Communication Manager Messaging 7.0 is available for upgrades only.

For information about other Avaya product compatibility information, go to <https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

*** Note:**

For deploying Avaya Aura® applications on Appliance Virtualization Platform only use Solution Deployment Manager.

! Important:

Due to Avaya enhanced customizations, Appliance Virtualization Platform (aka Avaya Solutions Platform120) does not support administration on vCenter. For the Appliance Virtualization Platform administration, System Manager and Solution Deployment Manager are the only management platform supported by Avaya.

Besides not being a supported configuration, if vCenter is connected to any appliance running the Appliance Virtualization Platform, the Avaya hypervisor customization and specific data (such as, logins, Datastore and VM information among others) will be overwritten and corrupted. This can result in making the situation unrecoverable and requires complete fresh re-installation of Appliance Virtualization Platform on the appliance.

Virtual Appliance components

Software component	Description
ESXi Host	The physical machine running the ESXi Hypervisor software.
Appliance Virtualization Platform	Avaya-provided virtualization turnkey solution that includes the hardware and all the software including the VMware hypervisor.
Solution Deployment Manager	Centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.

Virtualized Environment overview

You can deploy the Avaya Aura® applications in one of the following Virtualized Environment:

- VMware in customer-provided Virtualized Environment

Avaya Solutions Platform 130 Appliance (Dell PowerEdge R640) is a single host server with ESXi 6.5 preinstalled.

- Kernel-based Virtual Machine Virtualized Environment

Avaya Aura® Virtualized Environment overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® and Kernel-based Virtual Machine (KVM).

Kernel-based Virtual Machine overview

Kernel-based Virtual Machine (KVM) is a virtualization infrastructure for the Linux kernel that turns the Linux kernel into a hypervisor. You can remotely access the hypervisor to deploy applications on the KVM host.

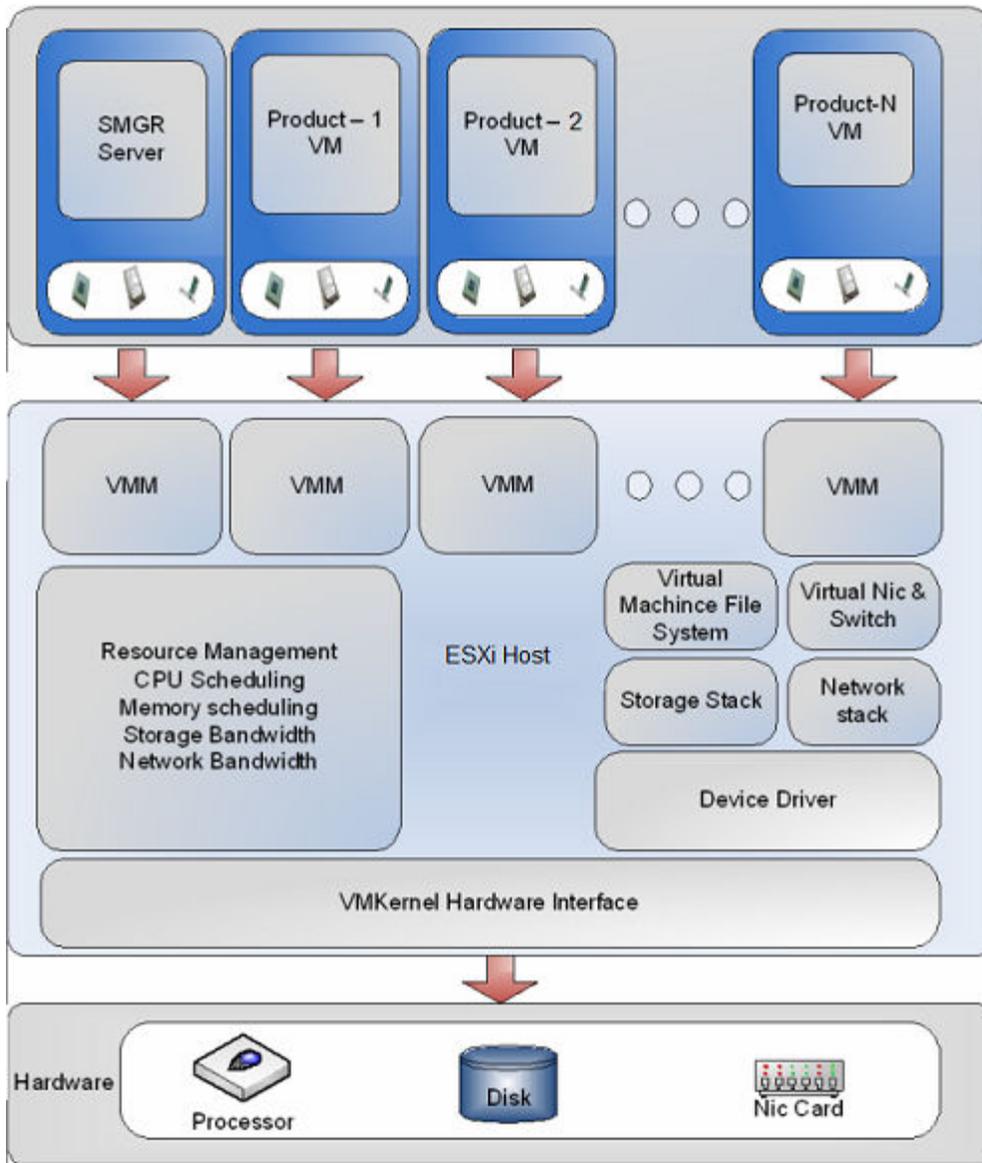
Supported applications in Virtualized Environment

Application	Release	VMware	KVM
Avaya Aura® System Manager	Release 8.1.3	Y	Y
Avaya WebLM	Release 8.1.3	Y	Y
Avaya Aura® Session Manager	Release 8.1.3	Y	Y
Avaya Aura® Communication Manager	Release 8.1.3	Y	Y
Avaya Aura® AVP Utilities	Release 8.1.3	—	—
Avaya Aura® Application Enablement Services	Release 8.1.3	Y	Y
Avaya Aura® Media Server (Software only)	Release 8.0	Y	Y

For information about other Avaya product compatibility information, go to <https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

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.
VMware	
ESXi Host	The physical machine running the ESXi Hypervisor software.

Table continues...

Virtualized component	Description
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Web Client	Using a Web browser, vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.
vSphere Client (HTML5)	vSphere Client (HTML5) is available from vSphere 6.5 and later. Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. This is the only vSphere client administration tool after the next vSphere release.
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.
KVM	
KVM hypervisor	A platform that runs multiple operating systems on a host computer at the same time.

Overview of Infrastructure as a Service environment

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
- Microsoft Azure
- Google Cloud Platform
- IBM Bluemix (IBM Cloud)

For information about Bluemix, see IBM Bluemix product documentation.

The Infrastructure as a Service environment supports the following offers:

Offer	Supported environments
OVA	Amazon Web Services
ISO	Simplex <ul style="list-style-type: none"> • Amazon Web Services • Microsoft Azure • Google Cloud Platform Duplex <ul style="list-style-type: none"> • Amazon Web Services • Microsoft Azure

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® Conferencing Release 8.0 and later
- 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), Kernel Service Packs (KSP), and Linux Security Update (LSU) are built for customers who do not use the software-only distribution. Software-only installation is in the control of the operating system and is responsible for applying the relevant security patches from Red Hat.

Avaya Communication Manager Security Service Packs (SSP) and Kernel Service Packs (KSP) 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 and get more control on the system. For the list of supported third-party software applications in Release 8.0 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 Bluemix overview

IBM Bluemix is a suite of public cloud computing services offered by IBM.

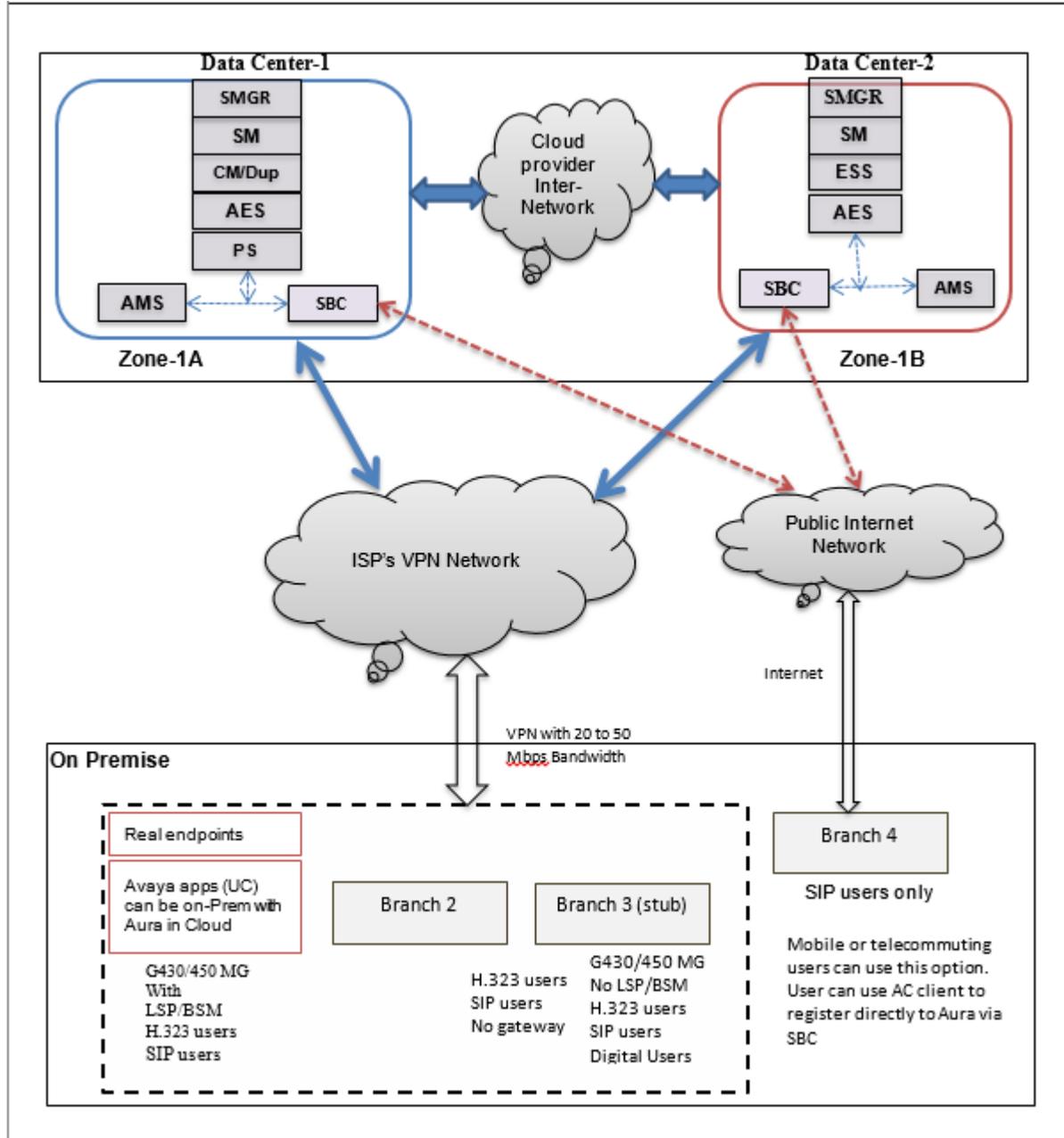
For information about IBM Bluemix, see IBM product documentation website.

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 8.1.3	Y	Y	Y
Avaya WebLM	Release 8.1.3	Y	Y	Y
Avaya Aura® Session Manager	Release 8.1.3	Y	Y	Y
Avaya Aura® Communication Manager	Release 8.1.3	Y	Y	Y
Presence Services using Avaya Breeze® platform	Release 8.1.3	Y	—	—
Avaya Aura® Application Enablement Services (Software only)	Release 8.1.3	Y	Y	Y
Avaya Aura® Media Server (Software only)	Release 8.0	Y	Y	Y

For information about other Avaya product compatibility information, go to <https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

Software-only environment overview

Avaya Aura® Release 8.0 and later supports software-only installation. 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 must procure a server that meets the recommended hardware requirements and the appropriate version of Linux® Operating System.

Software security updates

Avaya Security Service Packs (SSP), Kernel Service Packs (KSP), and Linux Security Update (LSU) are built for customers who do not use the software-only distribution. Software-only installation is in the control of the operating system and is responsible for applying the relevant security patches from Red Hat.

Avaya Communication Manager Security Service Packs (SSP) and Kernel Service Packs (KSP) 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 and get more control on the system. For the list of supported third-party software applications in Release 8.0 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 *PSN020361u* that Avaya publishes periodically. PSN is available at [Avaya Support website](#).

*** Note:**

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

Supported platforms

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

- VMware
- Kernel-based Virtual Machine (KVM)
- Hyper-V

*** Note:**

Starting with the Release 8.0.1, Avaya Aura® applications support Hyper-V.

- Nutanix
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

*** 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
- Avaya WebLM
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Application Enablement Services
- Avaya Aura® Media Server

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 provides the combined capabilities that Software Management, Avaya Virtual Application Manager, and System Platform provided in earlier releases.

From Release 7.1 and later, Solution Deployment Manager supports migration of Virtualized Environment-based 6.x, 7.0.x, and 7.1.x applications to Release 8.x and later in the customer's Virtualized Environment. For migrating to Release 8.x, you must use Solution Deployment Manager Release 8.x.

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:

- Avaya Aura® Virtualized Appliance: Contains a server, Appliance Virtualization Platform, and Avaya Aura® application OVA. Appliance Virtualization Platform includes a VMware ESXi 6.5 hypervisor.
- 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 and Avaya Aura® Virtualized Appliance 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
 - Avaya Aura® Appliance Virtualization Platform, 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 8.1.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

Related links

[Solution Deployment Manager Client](#) on page 23

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 System Platform-based System Manager.
- Upgrade VMware-based System Manager from Release 6.x, 7.x, or 8.0.x to Release 8.1 and later.
- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.
- Create the Appliance Virtualization Platform 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.
- You must use Solution Deployment Manager Client 7.1 and later to create the kickstart file for initial Appliance Virtualization Platform installation or recovery.

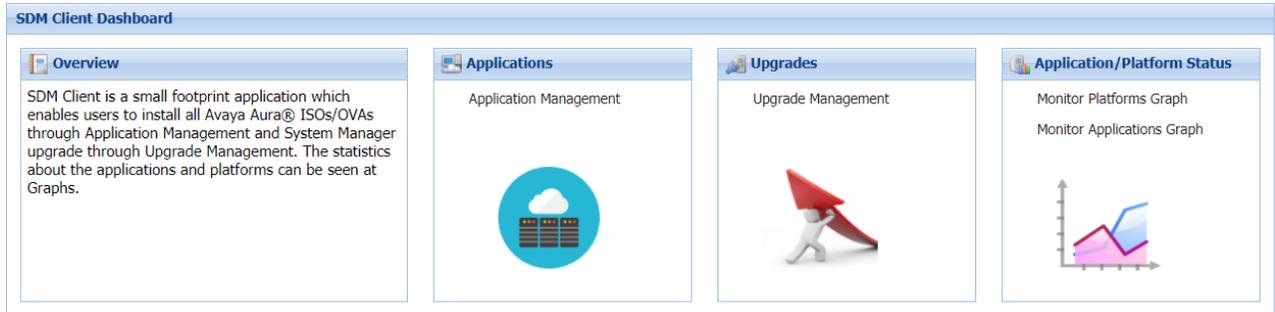


Figure 1: Solution Deployment Manager Client dashboard

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:

- AVP Utilities 8.1.3
- System Manager 8.1.3
- Session Manager 8.1.3
- Branch Session Manager 8.1.3
- Communication Manager 8.1.3
- Application Enablement Services 8.1.3
- WebLM 8.1.3
- Communication Manager Messaging 7.0

For information about other Avaya product compatibility information, go to <https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

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

*** 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 8.1.3. The process reduces the upgrade time and error rate.

Solution Deployment Manager dashboard

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

App Management : To deploy OVA files for supported Avaya Aura® applications. Also, to define the physical location, ESXi host, and discover virtual machines required for application deployments and virtual machine life cycle management.[\[„More\]](#)

Upgrade Management : To upgrade supported Avaya Aura® applications to Release 7.0.x. Also, to refresh applications, analyze software, and perform preupgrade checks required for upgrades.[\[„More\]](#)

Download Management : To download the software releases that the customer is entitled from Avaya PLDS or from an alternate source.[\[„More\]](#)

Software Library Management : To set a location where you can store the software and firmware files that you downloaded.[\[„More\]](#)

User Settings : To configure the location from where System Manager displays information about the latest software and firmware releases.[\[„More\]](#)

Application/Platform Status : Monitor the CPU and memory usage of platforms and applications.[\[„More\]](#)

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 8.1.3 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 Kickstart file.

- **Upgrade Management:** To upgrade Avaya Aura® applications to Release 8.1.3.
- **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 8.1.3:

- Communication Manager
- Session Manager
- Branch Session Manager
- AVP Utilities
- WebLM

 **Note:**

You must upgrade System Manager to Release 8.1.3 by using the Solution Deployment Manager client before you upgrade the Avaya Aura® applications to Release 8.1.3.

Support for VMware components

Avaya Aura® Release 8.1.3 supports deployment and upgrades on the following VMware components in Virtualized Environment.

- VMware® vSphere ESXi 6.0
- VMware® vSphere ESXi 6.5
- VMware® vSphere ESXi 6.7
- VMware® vSphere ESXi 7.0
- VMware® vCenter Server 6.0
- VMware® vCenter Server 6.5
- VMware® vCenter Server 6.7

- VMware® vCenter Server 7.0

*** Note:**

- Avaya Aura® Release 8.0 and later does not support vSphere ESXi 5.0 and 5.5.
- VMware vSphere ESXi 6.0 and 6.5 supports vSphere Client for Windows as well as vSphere Web Client. However, with VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.

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
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
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

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
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.	

Table continues...

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

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
ESXi 5.0	Y			
ESXi 5.1	Y			
ESXi 5.5	Y	Y		
ESXi 6.0		Y	Y	Y
ESXi 6.5		Y	Y	Y
ESXi 6.7			Y	Y
ESXi 7.0				Starting from Release 8.1.3: Y

Table continues...

ESXi version	Avaya Aura® Release			
	7.0.x	7.1.x	8.0.x	8.1.x
<p>* Note:</p> <ul style="list-style-type: none"> VMware vSphere ESXi 6.0 and 6.5 supports vSphere Client for Windows as well as vSphere Web Client. However, with VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported. Avaya Aura® applications support the ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 6.7 can be VMware ESXi 6.7 Update 3. Only the Encrypted Core Session Manager (8.1E OVA) is supported on VMware ESXi 7.0. Application Enablement Services Release 8.1.1 and 8.1.2 OVAs are supported on VMware 7.0. Device Adapter and Presence Services are deployed on the Avaya Breeze® platform, which supports VMware 6.5 and 6.7. 				

Supported servers for Avaya Aura® applications

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

Supported servers	Avaya Aura® Release			
	7.0.x	7.1.x	8.0.x	8.1.x
S8300D	Y	Y		
S8300E	Y	Y	Y	Y
HP ProLiant DL360 G7	Y	Y		
HP ProLiant DL360p G8	Y	Y	Y	Y
HP ProLiant DL360 G9	Y	Y	Y	Y
Dell™ PowerEdge™ R610	Y	Y		
Dell™ PowerEdge™ R620	Y	Y	Y	Y
Dell™ PowerEdge™ R630	Y	Y	Y	Y
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 *			Y	Y
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 **			Y	Y

*Avaya Solutions Platform 120 Appliance supports virtualization using Appliance Virtualization Platform.

**Avaya Solutions Platform 130 Appliance supports virtualization using VMware vSphere ESXi Standard License.

*** Note:**

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
G250 Branch Gateway	Y	Y			
G350 Branch Gateway	Y	Y			
G430 Branch Gateway	Y	Y	Y	Y	Y
G450 Branch Gateway	Y	Y	Y	Y	Y
G650 Media Gateway	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 8.1.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	Session Manager	AE Services	Communication Manager
8.1.3.5	<ul style="list-style-type: none"> • Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93 	<ul style="list-style-type: none"> • Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93 	<ul style="list-style-type: none"> • Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93 	<ul style="list-style-type: none"> • Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93 	<ul style="list-style-type: none"> • Mozilla Firefox Release 93 • Google Chrome Release 91 • Microsoft Edge Release 93
8.1.x	<ul style="list-style-type: none"> • Internet Explorer 11.x and later • Mozilla Firefox Release 65, 66, and 67 	<ul style="list-style-type: none"> • Internet Explorer 11.x and later • Mozilla Firefox Release 65, 66, and 67 	<ul style="list-style-type: none"> • Internet Explorer 11.x and later • Mozilla Firefox Release 65, 66, and 67 	<ul style="list-style-type: none"> • Internet Explorer 11.x and later • Mozilla Firefox Release 65, 66, and 67 	<ul style="list-style-type: none"> • Internet Explorer 11.x and later • Mozilla Firefox Release 65, 66, and 67

*** 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 8.1.3.5 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

Chapter 3: What's new in Appliance Virtualization Platform

This chapter provides an overview of the new and enhanced features of Appliance Virtualization Platform Release 8.1.x.

For more information about these features and administration, see:

- *Deploying Avaya Aura® Appliance Virtualization Platform*
- *Upgrading Avaya Aura® Appliance Virtualization Platform*

New in this Release

New in Appliance Virtualization Platform Release 8.1.3

Appliance Virtualization Platform Release 8.1.3 supports the following new features and enhancements:

Support for configuring the certificate validity duration

With Appliance Virtualization Platform Release 8.1.3, you can configure the number of days for the Appliance Virtualization Platform certificate validation. The maximum limit for certificate validation is 825 days. You can configure the certificate validation days by:

- Generating the Appliance Virtualization Platform Kickstart file during a fresh installation.
- By using the **More Actions** > **Generate/Accept Certificate** option on the **Platforms** tab.

The generated certificate is valid for the number of days configured in the **Validity in Days** field.

Support for certificate expiry alarm

With Release 8.1.3, Appliance Virtualization Platform supports the `CERT_FAULT` alarm to notify customers about a certificate expiry.

New in Appliance Virtualization Platform Release 8.1.2

Appliance Virtualization Platform Release 8.1.2 supports the following new features and enhancements:

Supports Log Rotation

Appliance Virtualization Platform can rotate and delete the older system log files when the newly generated log files reaches to the configured file size limit to avoid the out of disk space situation.

Customization of the Appliance Virtualization Platform banner through CLI

You can customize the login banner of the Appliance Virtualization Platform host and Direct Console User Interface (DCUI) of an ESXi host.

Support for Snapshot retention period

With Release 8.1.2, you can configure the snapshot retention period. Appliance Virtualization Platform retains the application snapshot for the configured period. Once the number of configured days expires, Appliance Virtualization Platform automatically deletes the expired snapshot.

New in Appliance Virtualization Platform Release 8.1.1

Appliance Virtualization Platform Release 8.1.1 supports the following new features and enhancements:

NIC teaming alarms

With Release 8.1.1, the following alarms can be generated when NIC teaming is configured.

Alarm ID	Severity	Description
NIC_TEAM_DEGRADED	Minor	This alarm is generated when NIC teaming is configured and link is lost on one of the NICs in the team goes down.
NIC_TEAM_FAULT	Critical	This alarm is generated when NIC teaming is configured and links of both the NICs in the team go down.
NIC_TEAM_CLEAR	Cleared	This alarm is generated when NIC teaming is configured and links of both the NICs in the team come up.

To enable the NIC teaming alarms, you can use the `/opt/avaya/common_services/set_linkmonitor enable` command.

To disable the NIC teaming alarms, you can use the `/opt/avaya/common_services/set_linkmonitor disable` command.

New in Appliance Virtualization Platform Release 8.1

Appliance Virtualization Platform Release 8.1 supports the following new features and enhancements:

Appliance Virtualization Platform Hypervisor

With Release 8.1, Appliance Virtualization Platform is based on the customized OEM version of VMware® ESXi 6.5.

Support of Windows Server 2016 for installing the Solution Deployment Manager client

With Release 8.1, you can install the Solution Deployment Manager client on the Windows Server 2016, 64-bit operating system.

Appliance Virtualization Platform enhancements

On the **Solution Deployment Manager > Application Management > Platforms** tab, a new:

- **More Actions > AVP Firewall Rules** option is added to view Appliance Virtualization Platform firewall rules.
- **Advanced Configuration** tab is added on the **Change Network params > Change Network Settings > Host Network/IP Settings** page from where you can delete unused Port Groups that are not associated with any virtual machine.

Supported browsers

Following are the minimum supported versions of the supported browsers:

- Internet Explorer 11
- Mozilla Firefox 65, 66, and 67

* 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.

Support for Red Hat Enterprise Linux operating system 7.6

With Release 8.1, you can deploy and upgrade Avaya Aura® applications on the Red Hat Enterprise Linux operating system 7.6.

Appliance Virtualization Platform feature matrix

The following table lists the feature matrix of Appliance Virtualization Platform.

* Note:

The features listed in the following table are not a comprehensive feature list. It only covers the new features.

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x
OVA signing	Y	Y	Y
IPv6 support	Y	Y	Y
Enhanced Access Security Gateway (EASG)	Y	Y	Y
Compliance with DISA security STIGs	Y	Y	Y
Extended Security Hardening	Y	Y	Y
Support for TLS 1.2	Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance		Y	Y

Table continues...

What's new in Appliance Virtualization Platform

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x
Supports Log Rotation			Y
Support for configuring the certificate validity duration			Y
Support for certificate expiry alarm			Y

Chapter 4: What's new in AVP Utilities

This chapter provides an overview of the new and enhanced features of AVP Utilities Release 8.1.x. For more information about these features and administration, see *Administering Avaya Aura® AVP Utilities*.

New in this release

New in AVP Utilities Release 8.1.3

AVP Utilities Release 8.1.3 supports the following new features and enhancements:

AVP Utilities certificate management on System Manager

With Release 8.1.3, you can manage AVP Utilities certificates using System Manager. You need administrator access to do the following:

- Add, replace and remove identity certificates using System Manager Element Manager.
- Generate certificate signing request (CSR).

Security Enhancements

With Release 8.1.3, AVP Utilities has stronger password policy. You can configure the passwords for better complexity, aging and authentication failure.

Support for alarms in AVP Utilities

With Release 8.1.3, AVP Utilities supports alarming infrastructure and following new alarms:

- **TEST_ALARM**: Administrator can test the alarming infrastructure.
- **AUTH_FAULT**: This alarm triggers when there are repeated login failure attempts made on AVP Utilities.
- **ACCESS_FAULT**: The alarm triggers when an unauthorized user attempts to execute a root command.
- **AUDIT_FAULT**: This alarm triggers when the mandatory audit service is either disabled or failed due to some reason.
- **CERTIFICATE_REVOCATION_FAULT**: This alarm triggers when a certificate on the system is revoked.

New in AVP Utilities Release 8.1.2

AVP Utilities Release 8.1.2 supports the following new features and enhancements:

Data Encryption

With Release 8.1.2, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized environments. Once you deploy the application with data encryption, you cannot disable data encryption after deployment and vice-versa.

Support to retain logs

With Release 8.1.2, you can retain the log files that contain privacy-related data for the following log categories:

- Application Command History
- CM Logs/MST Trace
- Linux OS Messages

New in AVP Utilities Release 8.1.1

AVP Utilities Release 8.1.1 supports the following new features and enhancements:

VMware console for applications

With Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab for the application that reside on Appliance Virtualization Platform Release 7.1.2 and later.

Based on the role of the user, you can assign the permissions for accessing the console.

New in AVP Utilities Release 8.1

AVP Utilities Release 8.1 supports the following new features and enhancements:

Support to forward syslog messages

With AVP Utilities Release 8.1, you can configure up to five remote syslog servers using AVP Utilities CLI and two remote syslog servers using System Manager Solution Deployment Manager.

Support for encrypted backup

With AVP Utilities Release 8.1, you can encrypt the backup files and restore the encrypted backup files.

AVP Utilities feature matrix

The following table lists the feature matrix of AVP Utilities.

Feature	Release 7.x (Applicable for Utility Services)	Release 8.0.x	Release 8.1.x
Services port access	Y	Y	Y
Appliance Virtualization Platform alarming	Y	Y	Y
Enabling SSH access	Y	Y	Y
Extended security hardening	Y	Y	Y
Enhanced Access Security Gateway	Y	Y	Y
Out of Band Management	Y	Y	Y
Enterprise System Directory	Y		
File Server	Y		
MyPhone Admin	Y		
Support for Avaya Solutions Platform 120 Appliance		Y	Y
Support for Avaya Solutions Platform 130 Appliance		Y	Y
Encrypted backup			Y
Encrypted Rsyslog			Y
Encryption (Supported for 8.1E OVA)			Y
Log Retention			Y

Chapter 5: What's new in System Manager

This chapter provides an overview of the new and enhanced features of System Manager Release 8.1.x.

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

New in this release

New in System Manager Release 8.1.3.6

Avaya Aura® System Manager Release 8.1.3.6 supports the following new feature and enhancement:

Support for configuring the DH Key size value

On the System Manager Release 8.1.x system, by default, the DH Key size value is 1024.

On the System Manager Release 8.1.3.6 system, you can use the `configureDHKeySize` command to configure the DH Key size value to 2048. At any point you can also reset the value to 1024.

The root user and the user created during deployment can run the `configureDHKeySize` command.

Enhancement to the Remove options

From System Manager Release 8.1.3.6, 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 8.1.3.5

Avaya Aura® System Manager Release 8.1.3.5 supports the following new feature and enhancement:

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Mozilla Firefox Release 93
- Google Chrome Release 91
- Microsoft Edge Release 93

* Note:

- From Avaya Aura® Release 8.1.3.5 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

Certificate renewal command

From System Manager Release 8.1.3.5, 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 enabling or disabling the display of help text on the Communication Manager Element Cut-Through page

From System Manager Release 8.1.3.5, 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 8.1.3.5, logging framework has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.

* Note:

For Release 10.1.x, the changes corresponding to Log4j 2.x will be available during the GA of Release 10.1.0.2.

New in System Manager Release 8.1.3.3

Avaya Aura® System Manager Release 8.1.3.3 supports the following new feature and enhancement:

Support for the configureSyslog command

With Release 8.1.3.3, configuration of syslog by attaching SYSLOG appenders through the Log Settings screen is no longer available. Alternately, to configure, list, and delete the remote syslog server, use the `configureSyslog` command.

New in System Manager Release 8.1.3.1

Avaya Aura® System Manager Release 8.1.3.1 supports the following new feature and enhancements:

Support for Active Directory 2019

With Release 8.1.3.1, System Manager supports Active Directory 2019.

Removal of the System Manager message pop-up with last login details

From Release 8.1.3.1, System Manager does not display the message pop-up window at login.

The last login information is now displayed in the **Notifications** widget on the System Manager dashboard.

Enhancements to the System Manager Alert messages at login

From Release 8.1.3.1, System Manager does not display the Session Manager emergency Dial Pattern routes notification message for Emergency Location Management Solution in an Alert Message pop-up window.

The emergency Dial Pattern routes notification message is now displayed in the **Notifications** widget on the System Manager dashboard.

Enhancements to the Notifications widget

From Release 8.1.3.1, the **Notifications** widget on the System Manager dashboard also displays the user login information and emergency Dial Pattern routes notification message for Emergency Location Management Solution.

From System Manager Release 8.1.3.1 and later, you cannot close the **Notifications** widget.

New in System Manager Release 8.1.3

Avaya Aura® System Manager Release 8.1.3 supports the following new features and enhancements:

Migration of 96x1 endpoints to J-Series phone

With Release 8.1.3, System Manager supports the migration of 96x1 endpoints to the J-Series phone. For migration of endpoints, System Manager and Session Manager must be on Release 8.1.3 or later.

Service observe support for J-Series endpoints

With Release 8.1.3, Communication Manager and System Manager supports the **sip-sobsrv** button for the following J-Series endpoints: J169 and J179.

Support of apostrophe character for Login Name

With Release 8.1.3, the **Login Name** field on the **Users > User Management > Manage Users** page, supports login names with an apostrophe ('). This helps import a user that has a login name with an apostrophe.

Support of 256-character password length for LDAP Server credentials

With Release 8.1.3, System Manager supports a 256-character password. Configure the password in one of the following ways:

- On the **Users > Administrators > User Services > External Authentication** page in the **Password for Root Binding** field.
- On the **Users > Directory Synchronization > Sync Users > User Synchronization** page, in the **Synchronization Datasources** tab when performing a New or Edit operation. On the New/Edit User Synchronization Datasource page in the **Password** field.

Simple Certificate Enrollment Protocol enhancement to improve Certificate Management for endpoints

With System Manager Release 8.1.3 and later, supports the following:

- Endpoints that have certificates issued by System Manager can use entity classes to send certificate enrollment or renewal requests to System Manager. You can add, edit, and delete entity classes using the **Services > Security > Certificates > Manage Entity Classes** page.

You can manage the password for entity classes on the View Profile: SMGR page in the Password Policy for Programmatic Accounts section.

- You can add, list, view, and delete subject names for the provided entity class using the **manageEntityClassWhitelist** command. You can add and delete bulk entries of subject names for an entity class. You can also check the status of the subject name validation for the entity class.
- You can use the **Number of days after which system deletes expired certificates** field on the **Services > Configurations > Settings > SMGR > Trust Management** page to set the number of days to delete the expired certificates from the system.

Support for outbound connection logging

With Release 8.1.3, you can log all outgoing connections from System Manager, using the **outboundConnectionLogging** utility.

Support for configuring the outbound firewall rule

With Release 8.1.3, you can configure System Manager outbound firewall rule by using the **configureOutboundFirewall** utility. You can add, list, view status, disable, remove, and overwrite the IP addresses and FQDN in the whitelist for establishing the outbound connection from System Manager.

Support of new CLI command for managing the password policies

With Release 8.1.3, System Manager supports the **setSecurityPolicy** command for managing 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 at the time of deployment.

Enhancement to password policies

With Release 8.1.3, the Communication Profile Password Policy and the Password strength policy are enhanced with the following:

- **Minimum total length** supports the default value of 14 characters as the minimum number of characters that you must use in a password.
- **Previous passwords blocked** supports the default value of 10 for the number of latest passwords that the system maintains in its history.
- Supports the addition of the new **Maximum repeated consecutive characters** field.
- Supports the addition of the new **Maximum consecutive characters from same character type** field.

Support for VMware ESXi 7.0

With Release 8.1.3, Avaya Aura® applications support the VMware® vSphere ESXi 7.0 and VMware® vCenter Server 7.0 in the VMware virtualized environment.

System Manager Welcome message

From System Manager Release 8.1.3, after your first successful login, when you log in to the System Manager web console or the System Manager command line interface again, System Manager displays the Welcome <SystemManager_UserName> pop-up window at your each subsequent login.

Enhancements to the System Manager alert messages at login

With Release 8.1.3, for the Emergency Location Management Solution, System Manager displays the Session Manager emergency Dial Pattern routes notification warning message in an Alert Messages pop-up window, if the Routing Locations, Routing Policies, and Dial Patterns are not configured on Session Manager according to the emergency calling guideline.

Centralized subscription licensing

With Release 8.1.3, WebLM supports the Centralized subscription licensing feature for solution licenses.

Enhancement to the number of IP Office branches support

With Release 8.1.3, System Manager supports up to:

- 2000 IP Office branches with System Manager Profile 3.
- 3500 IP Office branches with System Manager Profile 4.

New in System Manager Release 8.1.2

Avaya Aura® System Manager Release 8.1.2 supports the following new features and enhancements:

Data Encryption

With Release 8.1.2, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized environments. Once you deploy the application with data encryption, you cannot disable data encryption after deployment and vice-versa.

Support for encrypted backup and restore

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

Support for log file retention period management

With Release 8.1.2, you can configure the automated purging rule for log files based on the retention period configured on the Data Retention page of System Manager web console. Default value for number of days to retain log files are 30 days.

Support for the Avaya Subscription license

With Release 8.1.2, WebLM supports the Avaya Subscription license. You can view the license usage of the Avaya Subscription license as **Metered**.

New in System Manager Release 8.1.1

Avaya Aura® System Manager Release 8.1.1 supports the following new features and enhancements:

VMware console for applications

With Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab for the application that reside on Appliance Virtualization Platform Release 7.1.2 and later.

Based on the role of the user, you can assign the permissions for accessing the console.

Support for deploying Avaya SBCE using Solution Deployment Manager

With Release 8.1.1, you can:

- Download the Avaya Session Border Controller for Enterprise (Avaya SBCE) OVA from the Download Management page.
- Deploy the Avaya SBCE OVA.

To support this System Manager must be deployed on Profile 3 and higher systems.

Busy indicator support for J-Series endpoints

With Release 8.1.1, System Manager supports the **busy-ind** button for the following J-Series endpoints: J169, J169CC, J179, J179CC.

Support for the IP Phone Group Id field for SIP endpoints

With Release 8.1.1, System Manager supports the **IP Phone Group Id** field on the **Feature Options** tab for SIP endpoints.

On Communication Manager, this field is available on the page 3 of the **add station** or **change station** command. With Release 8.1.1, **IP Phone Group Id** also supports SIP endpoints.

For information about configuring the **IP Phone Group Id** field, see *Administering Avaya Aura® System Manager*.

Support for read only phone view layout for SIP Endpoints

With Release 8.1.1, you can view the Read only phone view layout for SIP Endpoints.

Support for common parameter across endpoint template

With Release 8.1.1, when you create a SIP endpoint, the system retains the common parameter information so that when you login SIP endpoints of that same type or of another type, all your SIP Endpoints are able to retrieve and update any of the common parameters they utilize.

The common parameters are on the **Elements > Communication Manager > Endpoints > Manage Endpoints** page on the **Profile Settings** and **Button Assignment** tabs.

Bulk import and export of Holiday Table and Service Hours Tables

Bulk import and export of **Holiday Table** and **Service Hours Tables** using System Manager web console. For adding, deleting and updating Holiday Table and Service Hours Tables in bulk, you can download a pre-loaded excel <Excel template file name>.xlsx file from **More Actions > Download Excel Template** on the following pages:

- **Elements > Communication Manager > Call Center > Holiday Table**
- **Elements > Communication Manager > Call Center > Service Hours Tables**

Multiple audio files upload in single click for broadcasting announcement

With Release 8.1.1, you can upload more than one audio files (.wav) in single click by using the **Browse** option of the **Select Announcement File** field.

New in System Manager Release 8.1

Avaya Aura® System Manager Release 8.1 supports the following new features and enhancements:

Support for System Manager Profile 4

With Release 8.1, System Manager supports a new Profile 4. The Profile 4 supports 35000 to 300000 users with up to 5000 Branch Session Manager instances and 28 Session Manager instances with a single System Manager system in an Avaya Aura® deployment.

System Manager Profile 1 not supported

From Release 8.0 and later, System Manager Profile 1 is not supported. If System Manager is on a pre Release 8.0 and using the Profile 1, ensure that the server has the required resources to configure Profile 2 on Release 8.0 and later.

Appliance Virtualization Platform Hypervisor

With Release 8.1, Appliance Virtualization Platform is based on the customized OEM version of VMware® ESXi 6.5.

Support for Red Hat Enterprise Linux operating system 7.6

With Release 8.1, you can deploy and upgrade Avaya Aura® applications on the Red Hat Enterprise Linux operating system 7.6.

Support of Windows Server 2016 for installing the Solution Deployment Manager client

With Release 8.1, you can install the Solution Deployment Manager client on the Windows Server 2016, 64-bit operating system.

Solution Deployment Manager enhancements

- Increased capacity for **Refresh, Analyze, Update/Upgrade** operations on multiple elements at the same time for System Manager:
 - Profile 2: 20 elements
 - Profile 3: 30 elements
 - Profile 4: 50 elements
- The `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet on the **Solution Deployment Manager > Upgrade Management > Download > Bulk Import Spreadsheet** page supports bulk upgrade of Branch Session Managers.
- During OVA deployment, the Network Parameters page is revamped to display wider UI elements to enhance user experience.

Appliance Virtualization Platform enhancements

On the **Solution Deployment Manager > Application Management > Platforms** tab, a new:

- **More Actions > AVP Firewall Rules** option is added to view Appliance Virtualization Platform firewall rules.
- **Advanced Configuration** tab is added on the **Change Network params > Change Network Settings > Host Network/IP Settings** page from where you can delete unused Port Groups that are not associated with any virtual machine.

Support for bulk upgrade of Branch Session Manager instances

With Release 8.1, you can perform bulk upgrade of Branch Session Manager instances by using the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet on the **Solution Deployment Manager > Upgrade Management > Download > Bulk Import Spreadsheet** page.

Remote Syslog profile enhancement

With Release 8.1, the Add Syslog Receiver page provides the following TLS authentication options when the **tcp** protocol is selected.

- **Server certificate authentication**
- **Mutual TLS authentication**

Support for managing Syslog receiver certificates for Remote Syslog receiver

With Release 8.1, you can:

- Add trusted certificates for Remote Syslog receiver by selecting the **SYSLOG** store type on System Manager.
- Create identity certificate to use with Remote Syslog receiver by selecting the **syslog** service name on System Manager.

Administration and Serviceability enhancements

- Serviceability Agents management supports background execution job for pushing SNMP Target/User Profiles to multiple Serviceability Agents.
- Manage Elements displays a progress bar indication of background notification operations for Geographic Redundancy state change operations.

- API based management operations off-loaded from Port 443 to new Port 10443.
- Data Replication Service supports 250 node repairs at a time for System Manager Profile 4.
- Typeahead support is provided for the:
 - **Host Name** field on **Services > Events > Log Harvester > Create New Profile**.
 - **Survivability Server** field on **Users > User Provisioning Rule > Communication Profile > Session Manager Profile**.
- Advanced Search feature is added on the following pages:
 - **Inventory > Manage Elements**
 - **Inventory > Manage Serviceability Agents > Serviceability Agent**
 - **Replication > Replica Groups > Replica Nodes**
- Automated purging rule is added in Data Retention for Aged Scheduler Completed Jobs.
- Adding certificates for more than one element of same type and same version creates background job for execution. You can view this on the Certificate Management Jobs page using **Inventory > Manage Elements > More Actions > View Certificate Add Status** on System Manager.

Crisis Alert support for SIP endpoints

With Release 8.1, Crisis Alert (**crss-alert**) button support is added for SIP phones. When an emergency call is initiated by an enterprise user, then the crisis-alert watcher's endpoint displays an alert including information about emergency call.

No Hold Conference for SIP endpoints

With Release 8.1, No hold conference (no-hld-cnf) button support is added for SIP phones. No Hold Conference is the ability to add a party in conference without putting existing users on Hold.

EC500 button support for SIP endpoints

With Release 8.1, System Manager supports the **EC500** button for the following endpoints: 9608SIPCC, 9611SIPCC, 9621SIPCC, 9641SIPCC, J169CC, J179CC, CS1K-IPCC (Avaya Device Adapter).

Call appearance and Bridged appearance with per button ring control for SIP endpoints

With Release 8.1, System Manager supports Call appearance (Abbreviated/Delayed ringing) and Bridged appearance with per button ring control for the following endpoints: 9608SIPCC, 9611SIPCC, 9621SIPCC, 9641SIPCC, J169CC, J179CC, CS1K-IPCC (Avaya Device Adapter).

Enhancements to the 16-digit extension

With Release 8.1, Avaya Aura® applications extend support for configuration of 16-digit extension to the following Communication Manager objects.

- hunt groups

 **Note:**

Administration of hunt group with 16-digit group extension and group members.

- coverage answer groups

- ELIN
- abbr dial buttons
- Listed Directory Number

Supported browsers

Following are the minimum supported versions of the supported browsers:

- Internet Explorer 11
- Mozilla Firefox 65, 66, and 67

* 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.

IP Office integration with System Manager

From Release 8.1, you can add and administer the IP Office element from the System Manager web console.

System Manager feature matrix

The following table lists the feature matrix of System Manager.

* Note:

The features listed in the following table are not a comprehensive feature list. It only covers the new features.

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x
OVA signing	Y	Y	Y
IPv6 support	Y	Y	Y
Enhanced Access Security Gateway (EASG)	Y	Y	Y
Compliance with DISA security STIGs	Y	Y	Y
Extended Security Hardening	Y	Y	Y
Support for TLS 1.2	Y	Y	Y
Customer Root Access		Y	Y
Preserve security hardening modes on upgrade		Y	Y
Extended host name validation		Y	Y
Support for 16-digit extension		Y	Y
Product Initiated Registration		Y	Y

Table continues...

What's new in System Manager

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1.x
Support for Software-only deployment		Y	Y
Support for deployment on Cloud Services	Y	Y	Y
Support for Geographic Redundancy in mixed deployment environment		Y	Y
Support for Avaya Solutions Platform 120 Appliance		Y	Y
Support for Avaya Solutions Platform 130 Appliance		Y	Y
Support for Data Encryption			Y
Support for encrypted backup and restore			Y
Support for log file retention period management			Y
Support for the Avaya Subscription license			Y
Support for VMware ESXi 7.0			Y
Support for J-Series phone migration			Y
SCEP Enrollment Enhancement to improve Certificate Management for endpoints			Y
Emergency Location Management Solution			Y

Chapter 6: What's new in WebLM

This chapter provides an overview of the new and enhanced features of WebLM Release 8.1.x.

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

New in this release

New in WebLM Release 8.1.3.5

WebLM Release 8.1.3.5 supports the following new feature:

Toggle WebLM Cipher Suites

From WebLM Release 8.1.3.5, you can toggle between the following cipher suites:

- Relaxed cipher suites
- Strict cipher suites

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

From Release 8.1.3.5, logging framework has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Mozilla Firefox Release 93
- Google Chrome Release 91
- Microsoft Edge Release 93

Note:

- From Avaya Aura® Release 8.1.3.5 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

New in WebLM Release 8.1.3

WebLM Release 8.1.3 supports the following new features and enhancements:

Centralized subscription licensing

With Release 8.1.3, WebLM supports the Centralized subscription licensing feature for solution licenses.

Support for VMware ESXi 7.0

With Release 8.1.3, Avaya Aura® applications support the VMware® vSphere ESXi 7.0 and VMware® vCenter Server 7.0 in the VMware virtualized environment.

New in WebLM Release 8.1.2

WebLM Release 8.1.2 supports the following new features and enhancements:

Support for the Avaya Subscription license

With Release 8.1.2, WebLM supports the Avaya Subscription license. You can view the license usage of the Avaya Subscription license as **Metered**.

Support of Metering Collector configuration

With Release 8.1.2, you can manage the Avaya Subscription license on the WebLM server when metering collector is registered with WebLM. The metering collector configuration is applicable only for the Avaya Subscription license. The Solution-Avaya Subscription license contains more than one application.

Using the metering collector configuration, the WebLM server tracks the license usage information from the deployed applications.

New in WebLM Release 8.1.1

WebLM Release 8.1.1 supports the following new features and enhancements:

VMware console for applications

With Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab for the application that reside on Appliance Virtualization Platform Release 7.1.2 and later.

Based on the role of the user, you can assign the permissions for accessing the console.

New in WebLM Release 8.1

WebLM Release 8.1 supports the following new features and enhancements:

Appliance Virtualization Platform Hypervisor

With Release 8.1, Appliance Virtualization Platform is based on the customized OEM version of VMware® ESXi 6.5.

Supported browsers

Following are the minimum supported versions of the supported browsers:

- Internet Explorer 11
- Mozilla Firefox 65, 66, and 67

*** 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.

Support for Red Hat Enterprise Linux operating system 7.6

With Release 8.1, you can deploy and upgrade Avaya Aura® applications on the Red Hat Enterprise Linux operating system 7.6.

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
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	Y
Extended Security Hardening	Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y
Customer Root Access			Y	Y
Support for Software-only deployment			Y	Y
Support for deployment on Cloud Services		Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance			Y	Y
Support for Avaya Solutions Platform 130 Appliance			Y	Y
Centralized subscription licensing				Y
Support for VMware ESXi 7.0				Y
Support for the Avaya Subscription license				Y
Support of Metering Collector configuration				Y

Chapter 7: What's new in Session Manager

This chapter provides an overview of the new and enhanced features of Session Manager Release 8.1.x.

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

New in this release

New in Session Manager Release 8.1.3.5

Session Manager Release 8.1.3.5 supports the following new features and enhancements:

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Mozilla Firefox Release 93
- Google Chrome Release 91
- Microsoft Edge Release 93

Note:

- From Avaya Aura® Release 8.1.3.5 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

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

From Release 8.1.3.5, logging framework has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.

Note:

For Release 10.1.x, the changes corresponding to Log4j 2.x will be available during the GA of Release 10.1.0.2.

New in Session Manager Release 8.1.3.1

Session Manager Release 8.1.3.1 supports the following new features and enhancements:

Support for Apple Push Notification activation maintenance

With Release 8.1.3.1, Session Manager will provide real-time activation status of push notifications that a user subscribes. A newly introduced Push Notification Activations status page will display activation status, last notification time, and status information per user or device. From a maintenance point of view, you can deactivate push notification subscriptions from the status page.

New in Session Manager Release 8.1.3

Session Manager Release 8.1.3 supports the following new features and enhancements:

Support for Branch Visiting User survivability

With Release 8.1.3, Session Manager supports the Branch Visiting User survivability feature that automatically assigns a visiting user to the Branch Session Manager of the visiting location. With this feature, you do not need to manually administer or change the Branch Session Manager with the local Branch Session Manager for the visiting users in the SIP controller list.

To configure the feature, select the **Enable Branch Visiting User** field on the Global Settings page.

Note:

Branch Visiting User is only supported on the survivability servers of Branch Session Manager. IP Office survivable branches (formerly known as B5800) do not support the Branch Visiting User feature.

Support for Apple Push Notification Services

With Release 8.1.3, Session Manager provides telephony push notifications events through Apple Push Notification service (APNs) to Client SDK based iOS applications, such as Avaya Workplace Client for iOS. Session Manager provides push notifications for incoming calls and voice messaging status updates. Avaya Workplace Client for iOS must be on Release 3.14 or later to receive push notification services.

Currently, Avaya Aura® Web Gateway (AAWG) supports push notification events towards iOS application, and you can choose to utilize push notification service from AAWG or Session Manager. You can select a group of users and update their client configuration through Avaya Aura® Device Services to point towards AAWG or Session Manager as their Push Notification provider.

To configure the feature, select 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.

Support for VMware ESXi 7.0

With Release 8.1.3, Avaya Aura® applications support the VMware® vSphere ESXi 7.0 and VMware® vCenter Server 7.0 in the VMware virtualized environment.

Enhancements to the System Manager alert messages at login

With Release 8.1.3, for the Emergency Location Management Solution, System Manager displays the Session Manager emergency Dial Pattern routes notification warning message in an Alert Messages pop-up window, if the Routing Locations, Routing Policies, and Dial Patterns are not configured on Session Manager according to the emergency calling guideline.

New in Session Manager Release 8.1.2

Session Manager Release 8.1.2 supports the following new features and enhancements:

Data Encryption

With Release 8.1.2, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized environments. Once you deploy the application with data encryption, you cannot disable data encryption after deployment and vice-versa.

Administrable Endpoint Adaptation

With Release 8.1.2, Session Manager supports administrable endpoint adaptation, allowing an administrator to apply sequences of adaptations to groups of endpoints (based on device type) and/or users (based on membership in an origination dial-pattern set). This feature is an extension of the adaptation capability made available to SIP entities in Session Manager Release 8.0.1.

Support for Log Retention

With Release 8.1.2, Session Manager supports **Log Retention** to specify the number of days for which logs will be retained. Default value for number of days to retain log files are 30 days. You can set the number of days between 1 — 180.

Support for Centralized Call History Retention (days)

With Release 8.1.2, Session Manager supports **Centralized Call History Retention (days)** to specify the number of days for which centralized call history will be retained. Default number of days is 90. You can set the number of days between 1 — 180.

Support for encrypted backup and restore

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

New in Session Manager Release 8.1.1

Session Manager Release 8.1.1 supports the following new features and enhancements:

Enhanced support for Matching Pattern

Session Manager extends the support for Matching Pattern. With Release 8.1.1, Matching Pattern ranges can be entered in the form of [start of range]:[end of range]. For example, 600000:600009.

Support for Regex Debugger

With Release 8.1.1, Session Manager supports a new tool called Regular Expression debugger which allows checking, validating and backtracking regular expressions.

Support for SIP headers and Attachment fields for Call Routing Test

With Release 8.1.1, you can use zero or more **SIP headers** to insert into the SIP INVITE request created by the call routing test.

With Release 8.1.1, you can use Content-type and content of an attachment to insert into the SIP INVITE request created by the call routing test.

Support for new Log Action for Regular-expression adaptations

With Release 8.1.1, a new Log action can be added to the regular-expression adaptations. This action will not modify a SIP message, but will instead log an event indicating that conditions were met for the action to execute.

VMware console for applications

With Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab for the application that reside on Appliance Virtualization Platform Release 7.1.2 and later.

Based on the role of the user, you can assign the permissions for accessing the console.

New in Session Manager Release 8.1

Session Manager Release 8.1 supports the following new features and enhancements:

Support for Session Manager Profile 6

With Release 8.1, Session Manager supports a new Profile 6. The Profile 6 supports 66.7K SIP devices. Using the Session Manager Profile 6, an Avaya Aura[®] deployment can support up to 1 million SIP devices.

Support for 5000 SIP branches

Earlier to Release 8.1, you can configure only 500 Branch Session Manager instances. From Release 8.1, you can configure 5000 Branch Session Manager instances with a single System Manager system in an Avaya Aura[®] deployment.

Appliance Virtualization Platform Hypervisor

With Release 8.1, Appliance Virtualization Platform is based on the customized OEM version of VMware[®] ESXi 6.5.

Syslog server configuration for Session Manager

With Session Manager Release 8.1, you can configure one or more syslog server for the Session Manager logging and SIP tracer for single Session Manager.

Enhancement for SIP tracing

With Session Manager Release 8.1, you can:

- View tracer configuration for the single Session Manager security module.
- Modify the tracer configuration for the single Session Manager security module, if required.
- Send traces to Syslog Server that is configured for Session Manager.

Support for managing Syslog receiver certificates for Remote Syslog receiver

With Release 8.1, you can:

- Add trusted certificates for Remote Syslog receiver by selecting the *SYSLOG* store type on System Manager.
- Create identity certificate to use with Remote Syslog receiver by selecting the *syslog* service name on System Manager.

Enhancement for origination dial pattern sets

With Session Manager Release 8.1, you can create origination dial pattern for origination dial pattern sets.

Enhancement for SIP Entity Reference Report

With Session Manager Release 8.1, you can view the outbound proxy, application, and failover group that correspond to the SIP entity.

Support for bulk upgrade of Branch Session Manager instances

With Release 8.1, you can perform bulk upgrade of Branch Session Manager instances by using the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet on the **Solution Deployment Manager > Upgrade Management > Download > Bulk Import Spreadsheet** page.

Supported browsers

Following are the minimum supported versions of the supported browsers:

- Internet Explorer 11
- Mozilla Firefox 65, 66, and 67

*** 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.

Support for Red Hat Enterprise Linux operating system 7.6

With Release 8.1, you can deploy and upgrade Avaya Aura® applications on the Red Hat Enterprise Linux operating system 7.6.

Session Manager feature matrix

The following table lists the feature matrix of Session Manager.

*** Note:**

The features listed in the following table are not a comprehensive feature list. It only covers the new features.

Feature name	Release 7.0.x	Release 7.1.x	Release 8.0.x	Release 8.1.x
OVA signing		Y	Y	Y
IPv6 support		Y	Y	Y
Enhanced Access Security Gateway (EASG)		Y	Y	Y

Table continues...

Feature name	Release 7.0.x	Release 7.1.x	Release 8.0.x	Release 8.1.x
Compliance with DISA security STIGs		Y	Y	Y
Extended Security Hardening		Y	Y	Y
Conference factory URI		Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y
Customer Root Access			Y	Y
Preserve security hardening modes on upgrade			Y	Y
SIP Resiliency			Y	Y
Extended host name validation			Y	Y
Cassandra clustering		Y	Y	Y
Support for Software-only deployment			Y	Y
Support for 16 digit dial plan			Y	Y
Support for Hyper-V in Software-Only environment			Y	Y
Support for Regular Expression based adaptation module			Y	Y
Support for Call Journaling Server High Availability			Y	Y
Cassandra security hardening			Y	Y
Support for multiple customer accounts			Y	Y
Support for role-based access control			Y	Y
Support for Avaya Solutions Platform 120 Appliance			Y	Y
Support for Avaya Solutions Platform 130 Appliance			Y	Y
Syslog server configuration				Y
Data Encryption				Y
Branch Visiting User				Y
Push notification				Y
Support for VMware ESXi 7.0				Y

Chapter 8: What's new in Communication Manager

This chapter provides an overview of the new and enhanced features of Communication Manager Release 8.1.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 8.1.3.5

Avaya Aura® Communication Manager Release 8.1.3.5 supports the following enhancement:

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Mozilla Firefox Release 93
- Google Chrome Release 91
- Microsoft Edge Release 93

*** Note:**

- From Avaya Aura® Release 8.1.3.5 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

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

From Release 8.1.3.5, logging framework has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.

*** Note:**

For Release 10.1.x, the changes corresponding to Log4j 2.x will be available during the GA of Release 10.1.0.2.

New in Communication Manager Release 8.1.3.1

Communication Manager Release 8.1.3.1 supports the following enhancement:

Enhancement to Site Data screen

With Release 8.1.3.1 onwards, the Site Data screen displays 14 pages of building strings that can hold 1000 entries, instead of two pages containing 150 entries.

New in Communication Manager Release 8.1.3

Communication Manager Release 8.1.3 supports the following enhancements:

Resending display update message

With Release 8.1.3, Communication Manager can resend display updated messages to Session Manager on receiving a 481 response from Session Manager.

Alarm when memory usage approaches the reserved capacity

With Release 8.1.3, Communication Manager raises an alarm when the memory usage approaches the reserved capacity.

Support to integrate with Emergency Location Management Solution

With Release 8.1.3, Communication Manager can send SNMP inform messages to the Emergency Location Management Solution when a DCP or H.323 endpoint comes into service or when a non-SIP endpoint places an emergency call.

Integration with Emergency Location Management Solution helps you to comply with Kari's Law and Ray Baum's Act by notifying the emergency service about the physical location of the user placing the emergency call.

Allowing emergency calls despite bandwidth limit exhaustion

With Release 8.1.3, for the Communication Manager managed bandwidth and the Session Manager managed bandwidth, emergency calls always connect despite administered bandwidth limit exhaustion.

SA9143 - Enhancement to Hold/Unhold notification field

When you upgrade to Communication Manager Release 8.1.3, the **Hold/Unhold notifications** field on the Trunk Group screen is not visible for all SIP trunks. You must enable the **Hold/Unhold Notifications for SIP Trunks** field on the system-parameters special-applications screen. When you enable the **Hold/Unhold Notifications for SIP Trunks** field on the system-parameters special-applications screen, the **Hold/Unhold notifications** field appears on the Trunk Group screen.

SA9142 - Enhancement to SIP station display details

With Release 8.1.3, if you enable the **Redirected Display for SIP Hunt Group Members** field on the system-parameters special-applications screen, SIP station displays the caller name and the hunt group name when a call is received on that SIP station.

SA9095 - Hunt-group enhancements

With Release 8.1.3, if you enable the **Hunt Group Modifications** field on the system-parameters special-applications screen, and the hunt-group algorithm is set to **circ** but there are no members

in the hunt group, **Re-hunt on no answer** is configured but no coverage path is assigned to hunt, then the caller must hear a busy tone.

Service observe support for J-Series endpoints

With Release 8.1.3, Communication Manager and System Manager supports the **sip-sobsrv** button for the following J-Series endpoints: J169 and J179.

Third-party call control support for service observe

From AE Services Release 8.1.3 and Communication Manager Release 8.1.3 onwards, a new third-party call control support is added for the activation and deactivation of service observe, service observe connection mode change, query service observe status, and monitor service observe the state change, on a hard phone. Service observer state change events are only sent on station monitors if the ASAI version is 12 or later.

Controlling the port from an un-named IP address

With Release 8.1.3, Communication Manager controls the sharing of the x-ported station, when a request comes from an unnamed IP address.

Sharing EC500Delay state to Workplace Clients

The **EC500Delay Deactivation State** field controls the sharing of the EC500Delay state to Workplace Clients.

Support for VMware ESXi 7.0

With Release 8.1.3, Avaya Aura® applications support the VMware® vSphere ESXi 7.0 and VMware® vCenter Server 7.0 in the VMware virtualized environment.

New in Communication Manager Release 8.1.2

Communication Manager Release 8.1.2 supports the following enhancements:

Support to specify the number of days to retain CDR logs

With Release 8.1.2, Communication Manager supports you to specify the number of days for which you want to retain the CDR logs. You can use the **CDR Retention (Days)** field to specify the number of days to retain the CDR logs.

On Communication Manager SAT interface, the **CDR Retention (Days)** field is available on page 1 of the CDR SYSTEM PARAMETERS screen. You can access the CDR SYSTEM PARAMETERS screen using the **change system-parameters cdr** command.

Support to retain logs

With Release 8.1.2, you can retain the log files that contain privacy-related data for the following log categories:

- Application Command History
- CM Logs/MST Trace
- Linux OS Messages

Data Encryption

With Release 8.1.2, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform

and VMware Virtualized environments. Once you deploy the application with data encryption, you cannot disable data encryption after deployment and vice-versa.

Support to connect Communication Manager with Call Management System using TLS

With Release 8.1.2, you can connect Communication Manager with Call Management System using the TLS protocol. To connect Communication Manager with Call Management System using the TLS protocol, you must enter `R19.1+ (secured)` in the **CMS (appl mis)** field.

On Communication Manager SAT interface, the **CMS (appl mis)** field is available on page 12 of the Feature-Related System Parameters screen. You can access the Feature-Related System Parameters screen page using the `change system-parameters features` command.

Encrypting CDR data using TLS

With Release 8.1.2, a new column **TLS Encryption** is added in the IP Services page of the Communication Manager SAT interface. Entering `Y` for **TLS Encryption** encrypts the CDR data for primary and secondary CDR devices using the TLS protocol.

On Communication Manager SAT interface, the **TLS Encryption** field is available on page 1 of the IP SERVICES screen. You can access the IP Services screen using the `change ip-services` command. This is applicable to **Service Type** for CDR1 and CDR2 options.

Support for 12-party conference

With Release 8.1.2, Communication Manager supports 12 participants for ad-hoc and meet-me conferences.

In page 7 of `change system-parameters features` screen, **12-party Conferences** field is added.

In page 2 of `change VDN` screen, the valid entry for **Conference Type** field is changed from `6-party` to `local`.

Busy/Reorder/Intercept Tone Timeout (Seconds)

With Release 8.1.2, Communication Manager allows you to configure the time to play busy, reorder, or intercept tone. This field is not applicable for SIP endpoints.

This field is available on page 16 of the `change feature-related system parameters` screen.

New in Communication Manager Release 8.1.1

Communication Manager Release 8.1.1 supports the following enhancements:

Support for the IP Phone Group Id field for SIP endpoints

With Release 8.1.1, System Manager supports the **IP Phone Group Id** field on the **Feature Options** tab for SIP endpoints.

On Communication Manager, this field is available on the page 3 of the `add station` or `change station` command. With Release 8.1.1, **IP Phone Group Id** also supports SIP endpoints.

For information about configuring the **IP Phone Group Id** field, see *Administering Avaya Aura® System Manager*.

Busy indicator support for J-Series endpoints

With Release 8.1.1, System Manager supports the **busy-ind** button for the following J-Series endpoints: J169, J169CC, J179, J179CC.

VMware console for applications

With Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab for the application that reside on Appliance Virtualization Platform Release 7.1.2 and later.

Based on the role of the user, you can assign the permissions for accessing the console.

Support for IP phone firmware

The firmware download functionality for IP phones in Utility Services is migrated to Avaya Aura[®] Device Services (AADS). However, in small branches in which communication infrastructure is hosted on a S8300E card, local firmware download functionality is absent.

Release 8.1.1 provides the option to enable a simple HTTP/HTTPS file server on the Communication Manager server in an S8300E only. This can be done by using the new **fileserver** command on Communication Manager Command Line Interface (CLI). For more details on using the **fileserver** command, see *Maintenance Commands for Avaya Aura[®] Communication Manager, Branch Gateways and Servers*.

To allow a user to manage certificates for IP phone HTTPS connections, a new certificate repository type is added to the Communication Manager System Management Interface (SMI) for Communication Manager running on an S8300; **F** for **File Server**.

The following SMI pages are added with **F** type:

- **Administration > Server (Maintenance) > Security > Trusted Certificates**
- **Administration > Server (Maintenance) > Security > Server/Application Certificates**

The new certificates are stored under: `/etc/opt/ecs/certs/web411`

Phone firmware packages will be moved to the Communication Manager through the SMI: **Administration > Server (Maintenance) > Download Files**.

The **fileserver** command options are then utilized to unpack, activate, and manage the firmware on the server. Only the firmware download capability and simple management of those files are provided with the new **fileserver** command on the S8300E.

No other IP Phone firmware support that was available on Utility Services 7.x is provided:

- No User Interface (UI) support to unpack, activate, deactivate the phone firmware. Available from the CLI only.
- No UI or tools to modify the Phone settings and configuration file.
- No scheduling of IP Phone firmware downloads.
- No IP Phone backup and restore.
- No MyPhone support.

New in Communication Manager Release 8.1

Communication Manager Release 8.1 supports the following new features and enhancements:

Supported browsers

Following are the minimum supported versions of the supported browsers:

- Internet Explorer 11
- Mozilla Firefox 65, 66, and 67

* 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.

Crisis Alert support for SIP endpoints

With Release 8.1, Crisis Alert (**crss-alert**) button support is added for SIP phones. When an emergency call is initiated by an enterprise user, then the crisis-alert watcher's endpoint displays an alert including information about emergency call.

No Hold Conference for SIP endpoints

With Release 8.1, No hold conference (no-hld-cnf) button support is added for SIP phones. No Hold Conference is the ability to add a party in conference without putting existing users on Hold.

Syslog server supports additional transport methods

With Communication Manager Release 8.1, syslog server supports the following transport methods to send the logs to an external syslog server:

- TCP
- TLS

Communication Manager feature matrix

The following table lists the feature matrix of Communication Manager.

* Note:

The features listed in the following table are not a comprehensive feature list. It only covers the new features.

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
OVA signing	Y	Y	Y	Y	Y
IPv6 support	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
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y	Y
Compliance with DISA security STIGs	Y	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
Preserve security hardening modes on upgrade			Y	Y	Y
SIP trunk optimization			Y	Y	Y
Automatic Call Distribution	Y	Y	Y	Y	Y
Emergency Calling Services	Y	Y	Y	Y	Y
Alphanumeric URI dialing		Y	Y	Y	Y
Extended security hardening		Y	Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance			Y	Y	Y
Support for Avaya Solutions Platform 130 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
Support for J-Series phone migration					Y
Support for VMware ESXi 7.0					Y
Emergency Location Management Solution					Y

Chapter 9: What's new in Presence Services

This chapter provides an overview of the new and enhanced features of Presence Services Release 8.1.x.

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

New in Presence Services Release 8.1.4

Presence Services Release 8.1.4 supports the following new features and enhancements:

Select same site mode

With Release 8.1.4, Presence Services enables you to define the same site modes.

Delete old messages

With Release 8.1.4, Presence Services allows you to delete the old messages from the conversation history.

Message archiving

With Release 8.1.4, Presence Services lets you upload the attachments associated with the IMs to the SFTP server.

Maximum threshold

With Presence Services Release 8.1.4, when the message capacity reaches the maximum threshold of 95%, system deletes the oldest messages until the lower threshold for message capacity is reached. The lower threshold for message capacity is 92%.

Message storage capacity

With Release 8.1.4, Presence Services displays the message storage capacity parameters for the system and the current count of messages in the cluster.

New in Presence Services Release 8.1.3

Presence Services Release 8.1.3 supports the following new features and enhancements:

OAuth support for Office 365

With Presence Services Release 8.1.3, Exchange Collector provides the ability to use OAuth for authentication with Office 365.

Messaging Security Enhancement

With Release 8.1.3, Presence Services encrypts the messages and attachments that you share with others to make them more secured. The encrypted messages and attachments are secured with a passphrase and only the recipient has the special key to unlock and read them.

Multiple Front End Pools of Skype for Business Servers

With Release 8.1.3, Presence Services supports multiple Front End pools of Skype for Business servers for presence federation.

Microsoft Active Directory 2019

With Release 8.1.3, Presence Services supports Microsoft Active Directory 2019.

Font and Color support within text messages for Windows

With Presence Services Release 8.1.3, font and color support within text messages is added for Windows the same way in which it is already supported for Mac and IOS Android.

Supported upgrade paths

The supported upgrade paths for Presence Services Release 8.1.3 are:

Release	Requirement
8.1.2	Direct upgrade to 8.1.3
8.1.1	Direct upgrade to 8.1.3
8.1	Direct upgrade to 8.1.3
8.0.x	Direct upgrade to 8.1.3
7.1.x	Direct upgrade to 8.1.3

New in Presence Services Release 8.1.2

Presence Services Release 8.1.2 supports the following new features and enhancements:

Manual presence state expiration time

Presence Services Release 8.1.2 lets you define the expiration period of presence state that is set manually.

Support for devices that do not support registration events

The **Default On-Hook State** attribute allows you to configure the on-hook state of devices that are not supporting the registration events.

Support for Office 365

Presence Services Release 8.1.2 supports Microsoft Office 365.

Supported upgrade paths

The supported upgrade paths for Presence Services Release 8.1.2 are:

Release	Requirement
8.1.1	Direct upgrade to 8.1.2
8.1	Direct upgrade to 8.1.2
8.0.x	Direct upgrade to 8.1.2
7.1.x	Direct upgrade to 8.1.2

New in Presence Services Release 8.1

Presence Services Release 8.1 supports the following new features and enhancements:

Enhancements to Avaya Workplace Client authentication

Avaya Workplace Client clients uses OAuth2 (JWT) authentication mechanism to authenticate with Presence Services to use the services provided by Presence Services.

Support to share multimedia attachments

In Presence Services Release 8.1, Inter-PS federated Avaya Workplace Client users can share multimedia attachments.

Support to archive Multimedia Messaging conversations

The SMTP Archiving Service archives Multimedia Messaging conversations to an SMTP server.

Supported upgrade paths

The supported upgrade paths for Presence Services Release 8.1 are:

Release	Requirement
8.0.x	Direct upgrade to 8.1.
7.1.x	Direct upgrade to 8.1.
7.0.1.x	Direct upgrade to 8.1.
7.0.0.x	Direct upgrade to 8.1.

Presence Services feature matrix

The following table lists the feature matrix of Presence Services.

*** Note:**

The features listed in the following table are not a comprehensive feature list. It only covers the new features.

Feature	Release 7.1.x	Release 8.0.x	R 8.1.x
Apple Push Notification service (APNs)	N	Y	Y
Access control lists	Y	Y	Y
AES collector	Y	Y	Y
Exchange collector	Y	Y	Y
Domino collector	Y	Y	Y
Microsoft Real Time Communication federation	Y	Y	Y
Inter-PS federation	Y	Y	Y
XMPP federation	Y	Y	Y
Spaces federation	Y	Y	Y
Simple authentication and security layer	Y	Y	Y
IM blocking in Do Not Disturb state	Y	Y	Y
Instant message broadcast	Y	Y	Y
Interoperability with Avaya Multimedia Messaging	Y	N	N
Inter-domain presence	Y	Y	Y
Inter-tenant communication control	Y	Y	Y
Multi-tenancy	Y	Y	Y
Message archiver	Y	Y	Y
Offline IM storage	Y	Y	Y
Avaya Solutions Platform servers	Y	Y	Y
KVM	Y	Y	Y
IPv6	Y	Y	Y
Extended hostname validation		Y	Y
Microsoft Office 365			Y
Message Security			Y
Multiple Front End pools			Y
Microsoft Active Directory 2019			Y

Chapter 10: What's new in Application Enablement Services

This chapter provides an overview of the new and enhanced features of Application Enablement Services Release 8.1.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 a Software-Only Environment*
- *Deploying Avaya Aura® Application Enablement Services in Infrastructure as a Service Environment*
- *Deploying Avaya Aura® Application Enablement Services in Virtual Appliance*
- *Upgrading Avaya Aura® Application Enablement Services*

New in this release

New in Application Enablement Services Release 8.1.3.5

Application Enablement Services Release 8.1.3.5 supports the following new feature and enhancement:

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Mozilla Firefox Release 93
- Google Chrome Release 91
- Microsoft Edge Release 93

Note:

- From Avaya Aura® Release 8.1.3.5 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

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

From Release 8.1.3.5, logging framework has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.

* Note:

For Release 10.1.x, the changes corresponding to Log4j 2.x will be available during the GA of Release 10.1.0.2.

New in Application Enablement Services Release 8.1.3.1

Support for Active Directory version 2016 and 2019

With the existing support of Microsoft Windows Server Active Directory 2012, from Release 8.1.3.1, Application Enablement Services also supports integration with the following Microsoft Active Directory (AD) server versions:

- Microsoft Windows Server Active Directory 2016
- Microsoft Windows Server Active Directory 2019

New in Application Enablement Services Release 8.1.3

Application Enablement Services Release 8.1.3 supports the following new features and enhancements:

Third-party call control support for service observe

From AE Services Release 8.1.3 onwards, new APIs have been added for third-party call control support for activation and deactivation of service observe, service observe connection mode change, query service observe status and monitor service observe state change on phone. Third-party call control for service observe will work with Avaya Aura® Communication Manager Release 8.1.3 and later. Service observer state change events are sent to the station monitors only if the ASAI version is 12 and above. This feature works with private data version 17 and above for TSAPI and JTAPI applications.

Support for changing the default password for single user mode login

From AE Services Release 8.1.3 onwards, you can set or change the password when logged in as a root user for a single user mode.

Support for VMware 7.0

From AE Services Release 8.1.3 onwards, customer provided virtualized environment supports the following software versions:

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

* Note:

AE Services Release 8.1.1 OVA is supported on VMware® vSphere ESXi 7.0.

Support for TSAPI 64-bit client for Windows and SDK

From AE Services Release 8.1.3 onwards, 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.

Effect of TLS Certificate Hostname Validation on AE Services Release 8.1.3 upgrade

If you are upgrading to Release 8.1.3, then certificate hostname validation will be enabled automatically for an external WebLM server and for all Communication Manager connections.

If the certificate identity in the **Subject Common Name (CN)** or **Subject Alternate Name (SAN)** matches with the FQDN/IP address of the WebLM server or with Communication Manager, then the connection is established, otherwise the connection is dropped.

For more information, see the *Upgrading Avaya Aura® Application Enablement Services*.

New in Application Enablement Services Release 8.1.2.1

From Release 8.1.2.1, Application Enablement Services is a part of Avaya OneCloud™ Subscription offer.

For more information about Avaya OneCloud™ Subscription offer, see Avaya Support website at <http://support.avaya.com>.

New in Application Enablement Services Release 8.1.2

Application Enablement Services Release 8.1.2 supports the following new features and enhancements:

Data Privacy

- **Data Encryption:** You can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized environments. Once you deploy the application with data encryption, you cannot disable data encryption after deployment and vice-versa.
- **Support for Log and Trace Retention:** You can set the retention period for retaining logs and traces from 0 to 180 days. The saved log and trace files are deleted after the retention period is reached. You can set the retention period via OAM and CLI.
- **Support for Clearing Logs and Traces:** You can clear the logs and traces for a certain period or you can choose to clear all the logs and traces irrespective of the number of days. You can set the clearing period via OAM and CLI.
- **Support for Auto Log and Trace Delete:** When logs disk reaches 90% occupancy, AE Services will automatically delete the oldest logs and traces till the time when the occupancy reaches 75%.

Support for 12-Party Conferencing

With Release 8.1.2, AE Services supports 12 participants for conference.

New in Application Enablement Services Release 8.1.1

Support for Location Parameter

With Release 8.1.1, the Locations model in the System Management Service (SMS) supports setting and retrieving the Locations Parameter value. You can set the area code for each location and administer different location information for each location. With this feature, you can administer multiple location specifications. Otherwise, information for Location 1 applies to all locations.

The Location Parameter (Loc_Param) is supported with the SMS Software Development Kit (SDK). For more information, see the Model documentation on the SMS test page.

VMware console for applications

With Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab for the application that reside on Appliance Virtualization Platform Release 7.1.2 and later.

Based on the role of the user, you can assign the permissions for accessing the console.

New in Application Enablement Services Release 8.1

Application Enablement Services Release 8.1 supports the following new features and enhancements:

Appliance Virtualization Platform Hypervisor

With Release 8.1, Appliance Virtualization Platform is based on the customized OEM version of VMware® ESXi 6.5.

Support of Clear Alarm for License Normal mode

With Release 8.1, AE Services sends a `clear` alarm notification that clears temporary license error alarms, when the license state returns to a *Normal* state from the license grace period state. This distinguishes license errors generated between transient state and network fluctuations.

Prior to Release 8.1, the license grace period alarms were generated but not cleared when the license state returned to normal mode. With this enhancement, AE Services sends the license clear alarm to notify the system administrator of the normal state of license mode.

Support for a videoCall private data parameter

With AE Services Release 8.1, a new private data parameter `videoCall` is added in CSTA Service Make call, Answer call, Consultation call and Single step transfer call requests, if CTI application requests endpoints to send and/or receive video stream.

Supported values for `videoCall` parameter are:

- **DISABLED**: No Video support required. This is the default value.
- **INCOMING**: Application requests endpoint to only receive video from far-end.
- **TWOWAY**: Application requests endpoint to send/receive video to/from far-end.

AE Services Release 8.1 also supports Channel Type in CSTA Originated event to identify an incoming SIP trunk calls as either Voice or Video via CTI.

Support for G.722 codec

With AE Services Release 8.1, call recording supports G.722 codec for DMCC applications in Client media mode. This enables DMCC applications to record end-to-end High Definition Media Stream.

Support for command line utilities for configuring AE Services using CLI

With Release 8.1, you can seamlessly configure AE Services in an automated manner through the command line interface. To facilitate this, the following command line utilities are provided:

- Switch Connection and CTI link
- Licensing
- Security Database
- Networking Configuration
- Certificate Management
- User Management
- SNMP configuration

Enhancements to the 16-digit extension

With Release 8.1, Avaya Aura[®] applications extend support for configuration of 16-digit extension to the following Communication Manager objects.

- hunt groups

 **Note:**

Administration of hunt group with 16-digit group extension and group members.

- coverage answer groups
- ELIN
- abbr dial buttons
- Listed Directory Number

Supported browsers

Following are the minimum supported versions of the supported browsers:

- Internet Explorer 11
- Mozilla Firefox 65, 66, and 67

 **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.

Support for Red Hat Enterprise Linux operating system 7.6

With Release 8.1, you can deploy and upgrade Avaya Aura[®] applications on the Red Hat Enterprise Linux operating system 7.6.

Application Enablement Services feature matrix

The following table lists the feature matrix of Application Enablement Services.

*** Note:**

The features listed in the following table are not a comprehensive feature list. It only covers the new features.

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
Third-party call control support for service observe					Y
VMware 7.0					Y
TSAPI 64-bit client for Windows and SDK					Y ^{***}
OVA signing	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
Multi factor authentication	Y	Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y	Y
Customer Root Access		Y	Y	Y	Y
Preserve security hardening modes on upgrade		Y	Y	Y	Y
Support for 16-digit dial plan		Y	Y	Y	Y
Support for KVM	Y	Y	Y		
Support for Software-only deployment	Y	Y	Y		Y ^{**}
Support for Hyper-V in Software-Only environment		Y	Y		Y ^{**}
Support for third-party software in Software-Only environment		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
Support of Held Call ID on auto dial request by Application Enablement Services		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
Support for G.722 codec			Y	Y	Y
Support for 12-Party Conferencing			Y	Y	Y

* - OVA is available for VMware and not for KVM.

** - 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

*** - 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.

Chapter 11: What's new in Branch Gateway

This chapter provides an overview of the new and enhanced features of Branch Gateway Release 8.1.x.

For more information about these features and administration, see:

New in Branch Gateway Release 8.1.3

The following sections describe new features and enhancements that are available in Branch Gateway 8.1.3.

Support of DC power supply for G450 Branch Gateway

With Release 8.1.3, DC power supply is available with only G450 Branch Gateway.

Commands updated for displaying the DC power supply

The following commands are enhanced to display the DC power supply:

- `Show System`
- `Show Voltage`
- `Show Platform power`

New in Branch Gateway Release 8.1.2

The following section describes new features and enhancements that are available in Branch Gateway 8.1.2.

Log retention

The following commands are added for log retention:

- `set logging file retention {retention_days}`
- `show logging file retention`

Support for G450v4

With Release 8.1.2, G450 Branch Gateway supports the G450v4 with the firmware versions 7.1.3.5, 8.1.1, or later.

G450v4 supports only the MP 160 DSP module. You can have a maximum of two MP 160 DSP modules. Each MP 160 DSP module supports 160 channels.

New in Branch Gateway Release 8.1

The following sections describes new features and enhancements that are available in Branch Gateway in Release 8.1 and later:

Syslog over TLS

Branch Gateway supports the syslog application directory for the TLS certificates.

The following commands are updated to add TLS for syslog:

- `set link-encryption syslog <all | tls | tls1.2 | tls1.1 | tls1.0> <yes | no>`
- `set logging server <ip-addr> tls [port]`
- `show logging server condition`

The following `certificate-options` commands are added and updated:

- `certificate-options syslog`
 - `set validate-alternate-name`
 - `set validate-common-name`
 - `set validate-expiration`
- `show certificate-options`
- `show certificate-options syslog`

Enhancements to the certificate management commands

The following certificate management commands are updated to include the syslog application:

- `copy scp root-ca syslog <filename> <ip>`
- `copy usb root-ca syslog <source-usb-device> <source-filename>`
- `erase root-ca syslog <index>`
- `show root-ca syslog [index]`
- `copy scp gw-identity syslog <filename> <ip>`
- `copy usb gw-identity syslog <source-usb-device> <source-filename>`
- `erase gw-identity syslog`
- `show gw-identity syslog`

Removed support of HTTP access

The HTTP access to Branch Gateway and the Gxxx Manager is not supported. The following commands are updated:

- `show protocol`
- `dir`

The following commands are removed:

- `set snmp timeout`
- `show snmp timeout`
- `set snmp retries`
- `show snmp retries`
- `ip http`
- `no ip http`
- `copy ftp EW_archive`
- `copy scp EW_archive`
- `copy tftp EW_archive`
- `copy usb EW_archive`
- `set web aux-files-url`
- `show web aux-files-url`

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
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y
16-digit dial plan extension	N	N	Y	Y
Login authentication password complexity	N	N	Y	Y
Syslog over TLS	N	N	N	Y

Chapter 12: What's new in Call Center Elite

This chapter provides an overview of the new and enhanced features of Call Center Elite Release 8.1.x.

New in Call Center Elite Release 8.1.3

Call Center Elite Release 8.1.3 supports the following new features:

- Support for Service Observing with users on AES CTI clients
- Support for sending 96 byte UUI data to Avaya one-X[®] Agent H.323 soft clients using the Adjunct Switch Application Interface (ASAI) feature
- Support failover from a Call Center Elite SIP agent softphone to a physical hardphone (Special Application SA9141)

Support for Service Observing with users on AES CTI clients

This feature allows users on AES CTI clients to access the Service Observing feature. When the AES CTI client activates Service Observing, only specific supported devices (listed below) will function properly and recognize Service Observing activation. Only the listed devices will receive notification that Service Observing is activated by the AES CTI client. This supported SIP device must have the “sip-sobsrv” button administered.

The SIP devices that support this feature include:

- J169CC
- J179CC
- Avaya Device Adapter Snap-in UNISTim phones
- AES CTI devices

Note:

When using the “sip-sobsrv” feature button, coaching is only available from these SIP devices when the user is logged on as an agent.

For more information, see *Avaya Aura[®] Call Center Elite Feature Reference* and *Administering Avaya Aura[®] Call Center Elite*.

Support for sending 96 byte UUI data to Avaya one-X® Agent H.323 soft clients using the ASAI feature

Prior to Call Center Elite Release 8.1.3, the system sent 32 byte ASAI UUI data to Avaya one-X® Agent H.323 soft clients. With Release 8.1.3, the system now sends 96 byte ASAI UUI data. The UUI data can be viewed by using the “UUI Info” button.

* Note:

The 96 byte UUI data is supported by Avaya one-X® Agent Release 2.5.13 and newer. When using an older version of Avaya one-X® Agent, only up to 73 bytes of UUI data can be displayed using the “UUI Info” button. Customers must upgrade to Avaya one-X® Agent Release 2.5.13 (or newer) to see the full 96 byte UUI data.

For Avaya one-X® Agent H.323 soft clients configured in Desk Phone mode (formerly known as Shared Controlled Mode), the system will only send 32 Byte ASAI UUI data.

There are no changes to Call Center Elite or Avaya one-X® Agent documentation for this enhancement.

Support failover from a Call Center Elite SIP agent softphone to a physical hardphone (Special Application SA9141)

! Important:

This special application was specifically developed for use in emergency call centers. Special applications are expected to be used for the purpose intended and Avaya cannot guarantee seamless operation with all other product features.

Prior to Call Center Elite Release 8.1.3 and SA9141, when an agent using a SIP device on a call, other SIP agent Multiple Device Access (MDA) devices display a **Bridge** button. However, when the agent presses the **Bridge** button, the bridging attempt fails because bridging is not allowed for SIP agents.

With Call Center Elite Release 8.1.3 and SA9141 enabled, when an agent presses the **Bridge** button, bridging is allowed and the agent can continue the call on another MDA-enabled device. This is an important safety feature that allows an agent on an emergency call to bridge the call to a physical SIP telephone in case there is a softphone failure. The call with the customer is not lost.

To use this special application, you must enable the feature on the Special Applications form.

For more information about special applications, see *Avaya Aura® Communication Manager Special Application Features* or contact your Avaya sales representative or Avaya Business Partner for a more detailed description of this feature.

New in Call Center Elite Release 8.1.2

There were no new features in Call Center Elite Release 8.1.2.

New in Call Center Elite Release 8.1.1

Call Center Elite Release 8.1.1 supports the new feature “Whisper Coaching Allowed on Invisible ASAI Single Step Conference (SSC) Calls”.

Supervisors must always be observing a call before trying to coach a call. For conference calls, prior to Release 8.1.1, coaching on a conference call was blocked. With Release 8.1.1, if the **Coach on SSC** option is enabled, supervisors can coach agents using the Service Observing Coach functionality even while the call is being recorded by recording applications that use the invisible ASAI SSC option to record calls. Prior to this option being available, supervisors could not coach agents on any call that was being recorded. If the **Coach on SSC** option is disabled, agent coaching continues to be blocked on any other conference call. Note that if the call is an invisible ASAI SSC call, the phone displays for the other parties on the call do not say “Conference”.

For more information, see *Avaya Aura® Call Center Elite Feature Reference* and *Administering Avaya Aura® Call Center Elite*.

New in Call Center Elite Release 8.1.0

Call Center Elite Release 8.1.0 supports the new feature “Multi-Device Access (MDA) Support for SIPCC Endpoints”.

MDA Support for SIPCC Endpoints has the following restrictions:

- The SIP agent must be registered and logged into only one physical endpoint.
- Soft clients using Third Party Call Control (3PCC) must operate in shared control mode. For example, if Avaya Workplace Client is used, Avaya Workplace Client must be configured to operate in “My Desk Phone” mode.

Registering two endpoints to the same extension is permissive use and will cause functional interactions during feature operation. The following examples are the most likely interactions:

- Service Observing will not start when more than one physical endpoint is registered with the same extension.
- Supervisor Assist fails when more than one physical endpoint is registered with the same extension.

Other feature interactions can occur when more than one endpoint is registered to the same extension.

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

Chapter 13: What's new in Avaya Device Adapter

This chapter provides an overview of the new and enhanced features of Avaya Device Adapter Release 8.1.x.

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

What's new in Avaya Device Adapter Release 8.1.4

Device Adapter Release 8.1.4 provides the following new capabilities:

- Allows use of AADS service account to access the Device Adapter Corporate Directory.
- Enables mapping of local IP addresses to public IP addresses to support static NAT services configuration.
- Supports fax and modem calls in pass-through mode.
- Supports Hebrew language using the Called Party Name Display (CPND) feature.
- Supports handsfree voice call on Hotline Intercom auto-answer, which is an enhancement to the Hotline Intercom feature.
- Enables Device Adapter Element Manager to access Avaya Device Adapter Snap-in installed in cloud deployment.

What's new in Avaya Device Adapter Release 8.1.3

Device Adapter Release 8.1.3 provides the following new capabilities:

- Supports additional Idle time interval range for DVLA phones before automatic virtual office logout functionality in the **Virtual Office/Emergency Calls** section.
- Supports Avaya SBCE setup with Device Adapter end users by implementing the **Remote Cluster** feature thereby overriding user defined Session Manager addresses for all Device Adapter endpoints.

- Supports activation and deactivation of the **LimitInCalls** feature key on the CS 1000 phones for the Limit Number of Concurrent Calls (LNCC) feature.
- With Release 8.1.3, you can use Device Adapter to manage phones migrated from the CS 2100 product.

What's new in Avaya Device Adapter Release 8.1.2

Device Adapter Release 8.1.2 provides the following new capabilities:

- Supports Call Center Elite features and capabilities on a limited subset of Device Adapter phones.
Call Center Elite agents and supervisors can use these phones to perform both UC and call center-specific operations.
- Supports Avaya Workspaces CTI application with Call Center Elite.
- Supports Avaya Workspaces and Avaya Aura[®] Agent Desktop CTI applications with Avaya Aura[®] Contact Center.
- Allows phones to be CTI controlled in a call center environment.
- Supports IPv6 between Device Adapter and the Avaya Aura[®] components.
- Supports the Private Line Service (PVR/PVN) feature.
- Supports the `ada-report` command, which provides the Device Adapter and Avaya Breeze[®] platform logs in one .zip file.
- Supports the `tnInfo` command, which displays a list of TNs of the Device Adapter endpoints that are configured in System Manager.
- Supports multiple node IDs and System IDs on one Avaya Breeze[®] platform cluster during migration of endpoints from CS 1000 to Avaya Aura[®].
- Stores Personal Directory data in the PPM instead of the Cluster database of Avaya Breeze[®] platform for Data Privacy.
- Avaya Breeze[®] platform restart is not required if you modify any of the Avaya Breeze[®] platform trusted certificates after Device Adapter is installed.
- Supports NT1R20 off-premise station analog line cards.
- Supports the Group Paging feature.
- Supports the Auto-Answer feature.
- Supports context-sensitive soft keys for voice mail on UNISlim IP desk phones and 3900 series digital desk phones.

What's new in Avaya Device Adapter Release 8.1.1

Device Adapter Release 8.1.1 provides the following new capabilities:

- Supports the Communication Manager operation of managing Call Forward All Calls (CFW) from a user extension on behalf of another user extension.
A user can use the CFW feature along with the Busy Indicator feature to manage CFW on behalf of another user extension.
- Supports the Virtual Office (VO) feature that allows a user to log in at a guest station by using VO credentials.
- Allows a VO user to make an emergency call irrespective of whether the VO user is logged in or logged out of the phone.
- Supports the following CS 1000 pcap commands to monitor network packets that are sent and received by the network interfaces of the Avaya Breeze[®] platform: `pcapHelp`, `pcapStart`, `pcapStop`, `pcapStatus`, `pcapRestart`, `pcapConfigShow`, and `pcapConfig`.
- Allows all Device Adapter UNISlim, analog, and digital endpoints to be used as CTI controlled SIP endpoints for Avaya Aura[®] Contact Center.
- Supports the `daHelp` command that displays a list of Device Adapter-specific maintenance and troubleshooting commands at the Avaya Breeze[®] platform CLI interface.
- Supports filtering of the DSA log components.
- The `mgcShow` command now also shows the type of the registered controllers; for example, MGC or MG-XPEC, and the number of voice gateways; that is, DSP resources that can be allocated to the TDM stations.

Avaya Device Adapter feature matrix

The following table lists the feature matrix of Avaya Device Adapter.

 **Note:**

The feature list is not a comprehensive feature list.

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 8.1.4
Ad hoc conference	UNISlim	UNISlim, Digital, Analog					

Table continues...

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 8.1.4
Autodial	UNISstim	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital
Busy Indicator	Not supported	Not supported	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital
Call Forward All Calls (CFW) along with the Busy Indicator feature to manage CFW on behalf of another extension	Not supported	Not supported	Not supported	UNISstim ¹ , Digital ¹ This feature is not supported on 2001 and 3901 endpoints.	UNISstim ¹ , Digital ¹ This feature is not supported on 2001 and 3901 endpoints.	UNISstim ¹ , Digital ¹ This feature is not supported on 2001 and 3901 endpoints.	UNISstim ¹ , Digital ¹ This feature is not supported on 2001 and 3901 endpoints.
Call Forward - all calls / busy / no answer	UNISstim	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog
Caller List / Redial List / Personal Directory	UNISstim	UNISstim, Digital ¹	UNISstim, Digital ¹	UNISstim, Digital ¹	UNISstim, Digital ¹	UNISstim, Digital ¹	UNISstim, Digital ¹
Call Pickup (Directed / Group / Ringing Number)	UNISstim	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog
Call Park and Call Pickup	UNISstim	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog	UNISstim, Digital, Analog
Call Waiting	UNISstim	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital	UNISstim, Digital
Corporate Directory	Not supported	UNISstim ¹ , Digital ¹	UNISstim ¹ , Digital ¹	UNISstim ¹ , Digital ¹	UNISstim ¹ , Digital ¹	UNISstim ¹ , Digital ¹	UNISstim ¹ , Digital ¹
Context-sensitive key access - idle / offhook / dialed / ringing / active call state	UNISstim	UNISstim, Digital ¹	UNISstim, Digital ¹	UNISstim, Digital ¹	UNISstim, Digital ¹	UNISstim, Digital ¹	UNISstim, Digital ¹

Table continues...

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 8.1.4
End-to-end signaling (DTMF)	UNISlim	UNISlim, Digital, Analog					
Fixed feature key access	UNISlim	UNISlim, Digital					
Hold / retrieve	UNISlim	UNISlim, Digital, Analog					
Hot Line - multiple types on CS 1000	UNISlim	UNISlim, Digital, Analog					
Last Number Redial	UNISlim	UNISlim, Digital, Analog					
Making, answering, and releasing a basic call	UNISlim	UNISlim, Digital, Analog					
Make Set Busy	UNISlim	UNISlim, Digital, Analog					
Malicious Call Trace	Not supported	Not supported	UNISlim, Digital	UNISlim, Digital	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog
Message Waiting Indication (including audio)	UNISlim	UNISlim, Digital, Analog					
Message Waiting Key and Lamp for voice mail	UNISlim	UNISlim, Digital, Analog ¹					
Multiple Appearance Directory Numbers (MADN)	UNISlim	UNISlim, Digital, Analog ²					

Table continues...

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 8.1.4
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 should be a Device Adapter UNISim endpoint.	Not supported	Not supported	UNISim	UNISim	UNISim	UNISim	UNISim
Release key - disconnect a call	UNISim	UNISim, Digital, Analog					
Ring Again	UNISim	UNISim, Digital	UNISim, Digital, Analog				
Set Display - calling / called / redirecting name and number.	UNISim	UNISim, Digital, Analog					
Set Display - time and date, call timer, and so on.	UNISim	UNISim, Digital, Analog ¹					

Table continues...

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 8.1.4
Speed Dial	UNISlim	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog
Sequential Registration: Allows registration of only one endpoint at one time.	UNISlim ³	UNISlim ³ , Digital ³ , Analog ³	UNISlim ⁴ , Digital ³ , Analog ³	UNISlim ⁴ , Digital ³ , Analog ³	UNISlim ⁴ , Digital ³ , Analog ³	UNISlim ⁴ , Digital ³ , Analog ³	UNISlim ⁴ , Digital ³ , Analog ³
Support for 50 Avaya Breeze [®] platform nodes and 2,00,000 endpoints.	Support for 35 Avaya Breeze [®] platform nodes.	50 Avaya Breeze [®] platform nodes retroactively supported.	Yes	Yes	Yes	Yes	Yes
SMGR IU for Device Adapter	No	Yes	Yes	Yes	Yes	Yes	Yes
SMGR IU for Media Gateway	No	Yes	Yes	Yes	Yes	Yes	Yes
Transfer - blind as well as consultative	UNISlim	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog
Privacy Release	UNISlim	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog	UNISlim, Digital, Analog
Presence Service Notification: Provides presence status indication to non-Device Adapter endpoints	Not supported	Not supported	UNISlim, Digital, Analog				

Table continues...

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 8.1.4
Virtual Office (VO)	Not supported	Not supported	Not supported	UNISlim with soft keys The endpoint must support Home and Virtual soft keys.	UNISlim with soft keys The endpoint must support Home and Virtual soft keys	UNISlim with soft keys The endpoint must support Home and Virtual soft keys	UNISlim with soft keys The endpoint must support Home and Virtual soft keys
Virtual Office Emergency dialing	Not supported	Not supported	Not supported	UNISlim with soft keys The endpoint must support Emergency soft key.	UNISlim with soft keys The endpoint must support Emergency soft key	UNISlim with soft keys	UNISlim with soft keys
Virtual Office DVLA Timer	Not supported	Not supported	Not supported	Not supported	Not supported	UNISlim with soft keys	UNISlim with soft keys
Remote Cluster	Not supported	Not supported	Not supported	Not supported	Not supported	UNISlim	UNISlim
Limit Number of Concurrent Calls (LNCC)	Not supported	Not supported	Not supported	Not supported	Not supported	UNISlim	UNISlim
CS2100	Not supported	Not supported	Not supported	Not supported	Not supported	UNISlim, Digital, Analog	UNISlim, Digital, Analog
Uses AADS service account to access the Device Adapter Corporate Directory	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	UNISlim
Server side NAT	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	UNISlim

Table continues...

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 8.1.4
Fax and modem calls in pass-through mode	Not supported	Analog					
Hebrew support using CPND	Not supported	UNISstim					
Handsfree Voice call	Not supported	UNISstim, Digital					
ADA EM access in cloud deployment	Not supported	UNISstim, Digital, Analog					

¹ Applies to a subset of the set types. For example, Digital¹ 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 UNISstim 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 UNISstim endpoints.

Chapter 14: Resources

Documentation

The following table lists the documents related to the components of Avaya Aura® Release 8.1.3. Download the documents from the Avaya Support website at <https://support.avaya.com>.

Title	Description	Audience
Implementation		
<i>Deploying Avaya Aura® System Manager in Virtualized Environment</i>	Deploy the Avaya Aura® System Manager application in a virtualized environment.	Implementation personnel
<i>Deploying Avaya Aura® System Manager in Virtual Appliance</i>	Deploy the Avaya Aura® System Manager application in a virtual appliance environment.	Implementation personnel
<i>Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment</i>	Deploy the Avaya Aura® System Manager application on cloud services.	Implementation personnel
<i>Deploying Avaya Aura® System Manager in Software-Only Environment</i>	Deploy the Avaya Aura® System Manager application in a software only environment.	Implementation personnel
<i>Upgrading Avaya Aura® System Manager</i>	Upgrade the Avaya Aura® System Manager application to Release 8.1.x.	System administrators and IT personnel
<i>Deploying Avaya Aura® Communication Manager in Virtualized Environment</i>	Describes the implementation instructions while deploying Communication Manager on VMware and Kernel-based Virtual Machine (KVM).	Implementation personnel
<i>Deploying Avaya Aura® Communication Manager in Virtual Appliance</i>	Describes the implementation instructions while deploying Communication Manager on Appliance Virtualization Platform.	Implementation personnel
<i>Deploying Avaya Aura® Communication Manager in Infrastructure as a Service Environment</i>	Describes the implementation instructions while deploying Communication Manager on Amazon Web Services, Microsoft Azure, Google Cloud Network.	Implementation personnel

Table continues...

Title	Description	Audience
<i>Deploying Avaya Aura® Communication Manager in Software-Only Environment</i>	Describes the implementation instructions while deploying Communication Manager on a software-only environment.	Implementation personnel
<i>Upgrading Avaya Aura® Communication Manager</i>	Describes instructions while upgrading Communication Manager.	System administrators and IT personnel
<i>Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment</i>	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Implementation personnel
<i>Deploying Avaya Aura® Session Manager in Infrastructure as a Service Environment</i>	Describes how to deploy the Session Manager in the Infrastructure as a Service (IaaS) environment.	Implementation personnel
<i>Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Software-Only Environment</i>	Describes how to deploy the Session Manager in the Software-Only environment.	Implementation personnel
<i>Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtual Appliance</i>	Describes how to deploy the Session Manager in Virtual Appliance.	Implementation personnel
<i>Upgrading Avaya Aura® Session Manager</i>	Provides common administration scenarios.	System administrators and IT personnel
<i>Deploying Avaya Aura® Application Enablement Services in Virtual Appliance</i>	Deploy Application Enablement Services applications in Virtual Appliance	Implementation personnel
<i>Deploying Avaya Aura® Application Enablement Services in Virtualized Environment</i>	Deploy Application Enablement Services applications in Virtualized Environment	Implementation personnel
<i>Deploying Avaya Aura® Application Enablement Services in Infrastructure as a Service Environment</i>	Deploy Application Enablement Services applications in Infrastructure as a Service Environment	Implementation personnel
<i>Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment</i>	Deploy Application Enablement Services applications in Software-Only Environment	Implementation personnel
<i>Upgrading Avaya Aura® Application Enablement Services</i>	Upgrading Application Enablement Services applications.	System administrators and IT personnel
<i>Deploying standalone Avaya WebLM in Virtual Appliance</i>	Deploy the application in virtual appliance environment by using Solution Deployment Manager	Implementation personnel
<i>Deploying standalone Avaya WebLM in Virtualized Environment</i>	Deploy the application in virtualized environment.	Implementation personnel

Table continues...

Title	Description	Audience
<i>Deploying standalone Avaya WebLM in Infrastructure as a Service Environment</i>	Deploy the application on cloud services.	Implementation personnel
<i>Deploying standalone Avaya WebLM in Software-Only Environment</i>	Deploy the application in software-only environment.	Implementation personnel
<i>Upgrading standalone Avaya WebLM</i>	Upgrade the application.	System administrators and IT personnel
Administration		
<i>Administering Network Connectivity on Avaya Aura® Communication Manager</i>	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
<i>Administering Avaya Aura® Communication Manager</i>	Describes the procedures and screens used for administering Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
<i>Administering Avaya Aura® System Manager</i>	Describes the procedures for configuring System Manager Release 8.1.3 and the Avaya Aura® applications and systems managed by System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
<i>Avaya Aura® Presence Services Snap-in Reference</i>	Describes the steps to deploy and configure Presence Services.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Using		
<i>Using the Solution Deployment Manager client</i>	Deploy and install patches on Avaya Aura® applications.	System administrators
Understanding		
<i>Avaya Aura® Communication Manager Feature Description and Implementation</i>	Describes the features that you can administer using Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
<i>Avaya Aura® Communication Manager Screen Reference</i>	Describes the screen and detailed field descriptions of Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Table continues...

Title	Description	Audience
<i>Administering Avaya Aura® Session Manager</i>	Describes how to administer Session Manager by using System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
<i>Avaya Aura® Communication Manager Hardware Description and Reference</i>	Describes the hardware devices that can be incorporated in a Communication Manager telephony configuration.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
<i>Planning for Deploying Avaya Aura® applications</i>	Provides planning information for deploying Avaya Aura® applications on supported platforms.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
<i>Planning for Upgrading Avaya Aura® applications to Release 8.1.x</i>	Provides planning information for upgrading Avaya Aura® applications on supported platforms.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Maintenance and Troubleshooting		
<i>Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers</i>	Provides commands to monitor, test, and maintain hardware components of Avaya servers and gateways.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.
The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.
For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Accessing the port matrix document

Procedure

1. Go to <https://support.avaya.com>.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support by Product > Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or both the following categories:
 - **Application & Technical Notes**
 - **Design, Development & System Mgt**The list displays the product-specific Port Matrix document.
7. Click **Enter**.

Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at <https://documentation.avaya.com>.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites > Support** on the top menu to open <https://support.avaya.com>.

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
 - Click **Filters** to select a product and then type key words in **Search**.
 - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** (🌐) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

Navigate to the **Manage Content > My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
- Add topics from various documents to a collection.

- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon ().

Navigate to the **Manage Content > Watchlist** menu, and do the following:

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

 **Note:**

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

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® Release 8.1
71200V	Integrating Avaya Aura® Core Components
72200V	Supporting Avaya Aura® Core Components
20130V	Administering Avaya Aura® System Manager Release 8.1
21450V	Administering Avaya Aura® Communication Manager Release 8.1

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 on to the Avaya 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>.
If the Avaya Support website displays the login page, enter your SSO login credentials.
2. On the top of the page, click **DOCUMENTS**.
3. On the Documents page, in the **Enter Your Product Here** field, type the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. 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 services packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to <http://support.avaya.com> and search for “Avaya Support Web Tips and Troubleshooting: E-Notifications Management”.

Under the Results section, click Avaya Support Web Tips and Troubleshooting: E-Notifications Management.

2. Set up e-notifications.

For detailed information, see the **How to set up your E-Notifications** procedure.

Index

A

accessing port matrix	98
Appliance Virtualization Platform	13
feature matrix	35
what's new	33
Appliance Virtualization Platform 8.1 new in release	34
Appliance Virtualization Platform 8.1.1 new in release	34
Appliance Virtualization Platform 8.1.2 new in release	33
Appliance Virtualization Platform 8.1.3 new in release	33
Appliance Virtualization Platform components	15
Appliance Virtualization Platform overview	13
Application Enablement Services feature matrix	77
new in release	75
new in release 8.1.1	75
new in release 8.1.2	74
new in release 8.1.2.1	74
new in release 8.1.3	73
new in release 8.1.3.1	73
new in release 8.1.3.5	72
what's new	72
Avaya Aura application upgrade	26
Avaya Aura components Release 8.1.x	7
Avaya Aura Virtualized Appliance offer	13
Avaya Aura® overview	12
Avaya Aura® application browsers	31
ESXi version	29
supported gateways	31
supported servers	30
Avaya Aura® application OVAs Linux operating system version	27
Avaya Aura® offers	12
Avaya Device Adapter feature matrix	87
what's new	85
Avaya Device Adapter 8.1.1 what's new	87
Avaya Device Adapter 8.1.2 what's new	86
Avaya Device Adapter 8.1.4 What's new	85
Avaya Device Adapter Release 8.1.3 What's new	85
Avaya support website	100
Avaya virtualization platform	13

AVP Utilities

feature matrix	38
new in release 8.1	38
new in release 8.1.1	38
new in release 8.1.2	38
new in release 8.1.3	37

B

Branch Gateway new features	81
new in release	80
what's new	79
browsers Avaya Aura® application	31

C

Call Center Elite what's new	82
client Solution Deployment Manager	21
collection delete	98
edit name	98
generating PDF	98
sharing content	98
Communication Manager feature matrix	65
new in release 8.1	64
new in release 8.1.1	63
new in release 8.1.2	62
new in release 8.1.3	61
new in release 8.1.3.1	61
new in release 8.1.3.5	60
what's new	60
components Appliance Virtualization Platform	15
virtualized environment	16
content publishing PDF output	98
searching	98
sharing	98
sort by last updated	98
watching for updates	98
customer VMware	15

D

document changes	8
documentation center	98
finding content	98
navigation	98

documentation portal	98	new in release	
finding content	98	Appliance Virtualization Platform 8.1	34
navigation	98	Appliance Virtualization Platform 8.1.1	34
E		Appliance Virtualization Platform 8.1.2	33
ESXi version		Appliance Virtualization Platform 8.1.3	33
Avaya Aura® application	29	Application Enablement Services	75
F		Branch Gateway	80
feature matrix		Presence Services	70
Appliance Virtualization Platform	35	Session Manager	54-57
Application Enablement Services	77	System Manager 8.1	46
Avaya Device Adapter	87	WebLM 8.1	52
AVP Utilities	38	new in release 8.1	
Branch Gateway	81	AVP Utilities	38
Communication Manager	65	Communication Manager	64
Presence Services	70	new in Release 8.1.0	84
Session Manager	58	new in release 8.1.1	
System Manager	49	Application Enablement Services	75
WebLM	53	AVP Utilities	38
finding content on documentation center	98	Communication Manager	63
finding port matrix	98	System Manager	45
I		WebLM	52
iaaS		new in Release 8.1.1	84
overview	17	new in release 8.1.2	
Infrastructure as a Service		Application Enablement Services	74
overview	17	AVP Utilities	38
InSite Knowledge Base	100	Communication Manager	62
K		Presence Services	69
Kernel-based Virtual Machine		System Manager	44
overview	15	WebLM	52
L		new in Release 8.1.2	83
Linux operating system version		new in release 8.1.2.1	
Avaya Aura® application OVAs	27	Application Enablement Services	74
Avaya Aura® application Software-only Environment	28	new in release 8.1.3	
M		Application Enablement Services	73
My Docs	98	AVP Utilities	37
N		Communication Manager	61
new features in 8.1.2	79	Presence Services	69
new features in 8.1.3 release	79	System Manager	42
new in 8.1.2	79	WebLM	51
new in 8.1.3	79	new in Release 8.1.3	82
new in 8.1.3 release	79	new in release 8.1.3.1	
		Application Enablement Services	73
		Communication Manager	61
		System Manager	42
		new in release 8.1.3.3	
		System Manager	41
		new in release 8.1.3.5	
		Application Enablement Services	72
		Communication Manager	60
		System Manager	41
		WebLM	51
		new in release 8.1.3.6	
		System Manager	40
		new in release 8.1.4	
		Presence Services	68

O

offer

Avaya virtualized appliance	12
Infrastructure as a Service	12
Software-only environment	12
Virtualized Environment	12

overview

Amazon Web Services (AWS)	18
Google Cloud Platform	18
IBM Bluemix	18
Microsoft Azure	18

P

PCN notification	102
------------------------	---------------------

port matrix	98
-------------------	--------------------

Presence Services

feature matrix	70
new in release	70
new in release 8.1.2	69
new in release 8.1.3	69
new in release 8.1.4	68
what's new	68

Product compatibility	8
-----------------------------	-------------------

PSN notification	102
------------------------	---------------------

R

related documentation	94
-----------------------------	--------------------

Release 8.1.0	84
---------------------	--------------------

Release 8.1.1	84
---------------------	--------------------

Release 8.1.3	82
---------------------	--------------------

S

SDM Client	23
------------------	--------------------

searching for content	98
-----------------------------	--------------------

Session Manager

feature matrix	58
new in release	54–57
what's new	54

sharing content	98
-----------------------	--------------------

signing up

PCNs and PSNs	103
---------------------	---------------------

software-only	20
---------------------	--------------------

Solution Deployment Manager	21
-----------------------------------	--------------------

supported applications	24
------------------------------	--------------------

Solution Deployment Manager client	21
--	--------------------

Solution Deployment Manager Client	23
--	--------------------

sort documents by last updated	98
--------------------------------------	--------------------

support	100
---------------	---------------------

supported applications

Infrastructure as a Service	20
VMware and KVM	15

supported gateways

supported gateways (*continued*)

Avaya Aura® application	31
-------------------------------	--------------------

supported servers

Avaya Aura® application	30
-------------------------------	--------------------

System Manager

feature matrix	49
----------------------	--------------------

new in release 8.1.1	45
----------------------------	--------------------

new in release 8.1.2	44
----------------------------	--------------------

new in release 8.1.3	42
----------------------------	--------------------

new in release 8.1.3.1	42
------------------------------	--------------------

new in release 8.1.3.3	41
------------------------------	--------------------

new in release 8.1.3.5	41
------------------------------	--------------------

new in release 8.1.3.6	40
------------------------------	--------------------

what's new	40
------------------	--------------------

System Manager 8.1

new in release	46
----------------------	--------------------

T

technical assistance	8
----------------------------	-------------------

topology

Avaya applications on Infrastructure as a Service platform	19
---	--------------------

System Manager	16
----------------------	--------------------

training	99
----------------	--------------------

U

upgrade

Branch Session Manager	26
------------------------------	--------------------

Communication Manager	26
-----------------------------	--------------------

Session Manager	26
-----------------------	--------------------

V

videos	99
--------------	--------------------

viewing

PCNs	102
------------	---------------------

PSNs	102
------------	---------------------

Virtualized Appliance	13
-----------------------------	--------------------

virtualized environment	15
-------------------------------	--------------------

Virtualized Environment	13, 15
-------------------------------	------------------------

VMware components

Release 8.x	26
-------------------	--------------------

W

watch list	98
------------------	--------------------

WebLM

feature matrix	53
----------------------	--------------------

new in release 8.1.1	52
----------------------------	--------------------

new in release 8.1.2	52
----------------------------	--------------------

new in release 8.1.3	51
----------------------------	--------------------

new in release 8.1.3.5	51
------------------------------	--------------------

what's new	51
------------------	--------------------

WebLM 8.1

WebLM 8.1 (*continued*)

- new in release [52](#)
- What's new
 - Avaya Device Adapter Release 8.1.3 [85](#)
 - Avaya Device Adapter Release 8.1.4 [85](#)
- what's new [82](#), [84](#)
 - Appliance Virtualization Platform [33](#)
 - Application Enablement Services [72](#)
 - Avaya Device Adapter [85](#)
 - Avaya Device Adapter 8.1.1 [87](#)
 - Avaya Device Adapter 8.1.2 [86](#)
 - Branch Gateway [79](#)
 - Call Center Elite [82](#)
 - Communication Manager> [60](#)
 - Presence Services [68](#)
 - Session Manager [54](#)
 - System Manager [40](#)
 - WebLM [51](#)
- What's new [37](#)