# What's New in Avaya Aura® Release 7.1.3

Release 7.1.3
Issue 4
May 2018

**Notice**

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

**Documentation disclaimer**

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

**Link disclaimer**

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

**Warranty**

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

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

**Hosted Service**

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

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA 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. 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). You 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. “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). You 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").

**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. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

**Third Party Components**

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

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

**Service Provider**

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

**Compliance with Laws**

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

**Preventing Toll Fraud**

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

**Avaya Toll Fraud intervention**

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

**Security Vulnerabilities**

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

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

**Downloading Documentation**

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

**Contact Avaya Support**

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

**Trademarks**

# Contents

# Chapter 1: Introduction

## Purpose

This document provides an overview of the new and enhanced features of Avaya Aura® Release 7.1.3 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 7.1.3 components

| Product component | Release version |
|---|---|
| Appliance Virtualization Platform | 7.1.3 |
| Utility Services | 7.1.3 |
| System Manager | 7.1.3 |
| WebLM | 7.1.3 |
| Session Manager | 7.1.3 |
| Communication Manager | 7.1.3 |
| Branch Gateway | 7.1.3 |
| Presence Services | 7.1.3 |
| Application Enablement Services | 7.1.3 |

*Table continues…*

| Product component | Release version |
|---|---|
| Call Center Elite | 7.1 |
| Communication Manager Messaging | 7.0 |
| Media Server | 7.8 |

# Product compatibility

For the latest and most accurate compatibility information, go to http://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.

# Chapter 2: 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.

KVM virtualization solution is:

- Cost effective for the customers.
- Performance reliable and highly scalable.
- Secure as it uses the advanced security features of SELinux.
- Open source software that can be customized as per the changing business requirements of the customers.

# Chapter 3: Avaya Aura® on Amazon Web Services overview

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

Supporting the Avaya applications on the AWS Infrastructure as a service (IaaS) platform provides the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure. The customers can move from CAPEX to operational expense (OPEX).
- 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.

You can deploy the following Avaya Aura® applications on Amazon Web Services:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Utility Services
- Avaya WebLM
- Presence Services using Avaya Breeze™
- Avaya Session Border Controller for Enterprise
- Avaya Aura® Device Services
- Avaya Aura® Application Enablement Services (Software only)
- Avaya Aura® Media Server (Software only)
- Avaya Diagnostic Server (Software only)

The supported Avaya Aura® AWS applications can also be deployed on-premises.

You can connect the following applications to the Avaya Aura® AWS 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

# Topology

The following diagram depicts the architecture of the Avaya applications on the Amazon Web Services platform. This diagram is an example setup of possible configuration offered by Avaya. The setup must follow the AWS deployment guidelines, but does not need to include all the applications.

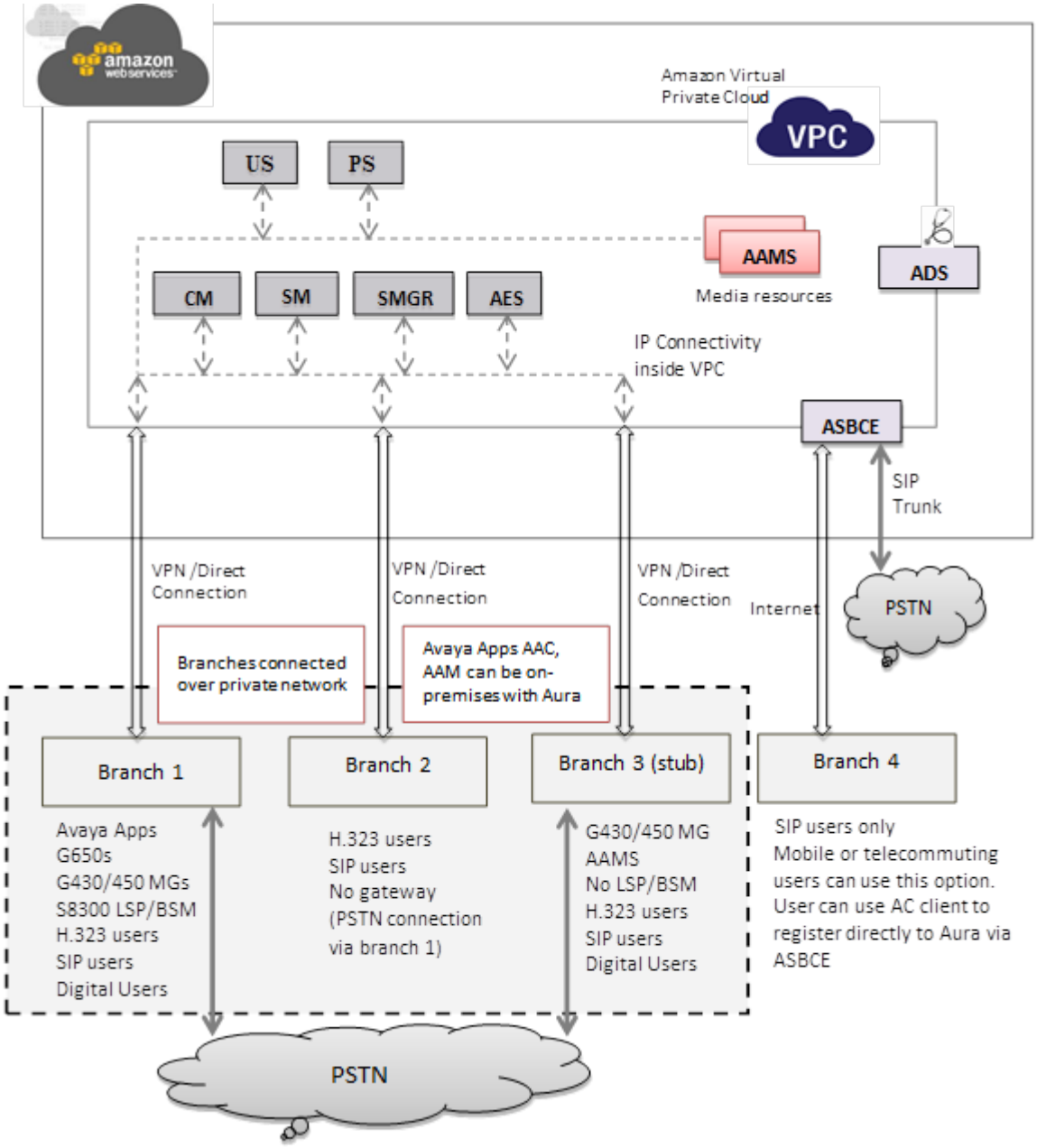



**Figure 1: Avaya Aura® applications on Amazon Web Services**

# Networking considerations for connecting Avaya applications

When you deploy an Avaya application at main location or at a branch location on AWS, ensure that you follow the networking requirements, such as, the WAN network topology, bandwidth and latency of the Avaya applications. You must adhere to the Avaya network recommendations and AWS networking rules.

AWS has some limitations for establishing public internet VPNs and direct connections into AWS. For more information about Amazon VPC Limits, see the AWS documentation at http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html.

**Important:**

Avaya recommends the use of direct connection in combination of a private WAN connection with Service Level Agreement (SLA) measures to ensure that the network quality is appropriate for signaling and voice traffic.

Avaya is not responsible for network connections between AWS and customer premises.

## Connection types

You can connect applications in a hybrid network on the Virtual Private Cloud (VPC) in the following ways:

| Connection type | Resource |
|---|---|
| VPN connection | For information about VPN connections, see http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html. |
| Direct connection | For information about AWS direct connections, see https://aws.amazon.com/directconnect/. |

# Chapter 4: Avaya Aura® Virtualized offers

Avaya Aura® Release 7.0 and later supports the following two Avaya virtualization offers based on VMware:

- Avaya Aura® Virtualized Appliance (VA): Avaya-provided server, Avaya Aura® Appliance Virtualization Platform, based on the customized OEM version of VMware® ESXi 6.0.
- Avaya Aura® Virtualized Environment (VE): Customer-provided VMware infrastructure

The virtualization offers provide the following benefits:

- Simplifies IT management using common software administration and maintenance.
- Requires fewer servers and racks which reduces the footprint.
- Lowers power consumption and cooling requirements.
- Enables capital equipment cost savings.
- Lowers operational expenses.
- Uses standard operating procedures for both Avaya and non-Avaya products.
- Deploys Avaya Aura® virtual products in a virtualized environment on Avaya provided servers or customer-specified servers and hardware.
- Business can scale rapidly to accommodate growth and to respond to changing business requirements.

## Appliance Virtualization Platform overview

From Release 7.0, Avaya uses the VMware®-based Avaya Aura® Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya Aura® Virtualized Appliance offer.

Avaya Aura® Virtualized Appliance offer includes:

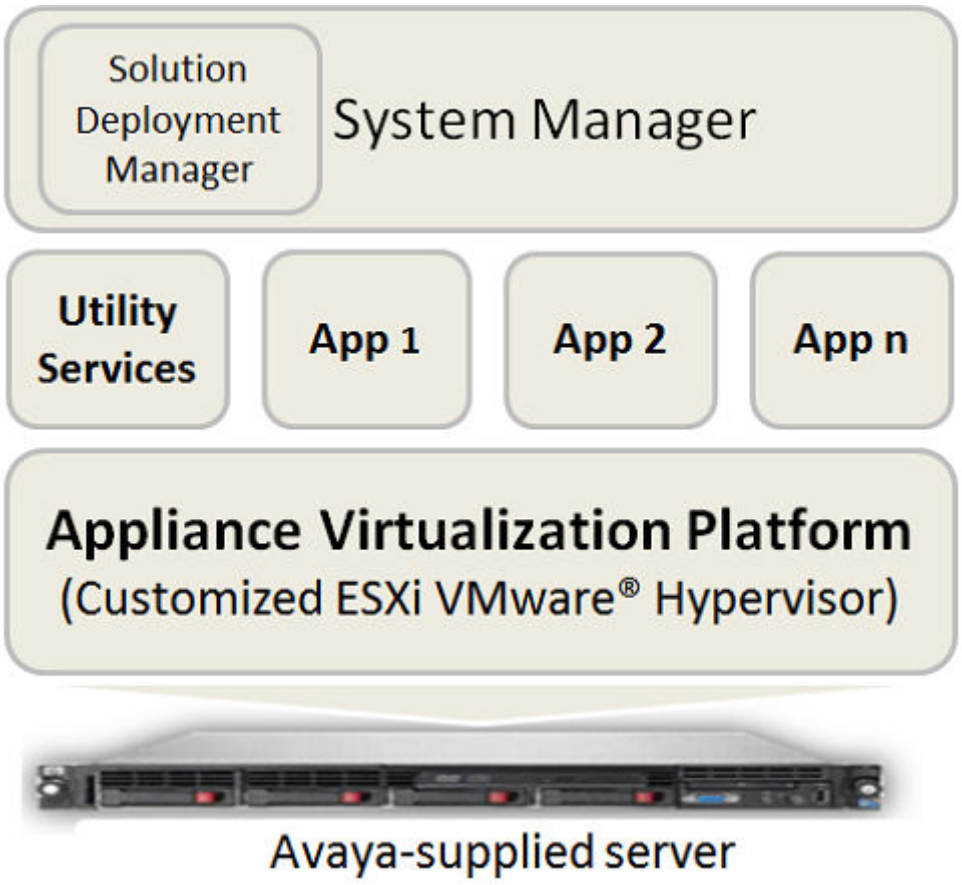
- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360 G7, HP ProLiant DL360p G8, and HP ProLiant DL360 G9
- S8300D and S8300E

**Note:**

With WebLM Release 7.x, you cannot deploy WebLM on S8300D Server or S8300E Server running on Appliance Virtualization Platform.

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 6.0. With Appliance Virtualization Platform, customers can run any combination of supported applications on

Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.




From Avaya Aura® Release 7.0 and later, Appliance Virtualization Platform replaces System Platform.

You can deploy the following applications on Appliance Virtualization Platform:

- Utility Services 7.1.3
- System Manager 7.1.3
- Session Manager 7.1.3
- Branch Session Manager 7.1.3
- Communication Manager 7.1.3
- Application Enablement Services 7.1.3
- WebLM 7.1.3
- Avaya Breeze™ 3.3.x with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0

- Avaya Aura® Device Services 7.1.2
- Avaya Aura® Media Server 7.8
- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

  For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

**Note:**

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

# Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® applications. Solution Deployment Manager supports the operations on customer Virtualized Environment and 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 and 7.0.x applications to Release 7.1 and later in customer Virtualized Environment.

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 is the primary management solution for Avaya Aura® Release 7.0 and later applications.

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 6.0 hypervisor.

  From Release 7.0 and later, Appliance Virtualization Platform replaces System Platform.
- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.

With Solution Deployment Manager, you can perform the following operations in Virtualized Environment and Avaya Aura® Virtualized Appliance models:

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

- 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
  - Utility Services
  - Appliance Virtualization Platform, the ESXi host that is running on the Avaya Aura® Virtualized Appliance.

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 7.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

**Related links**

Solution Deployment Manager client on page 19

# Solution Deployment Manager client

For the initial System Manager deployment or when System Manager is inaccessible, you can use the Solution Deployment Manager client. The client can reside on the computer of the technician. The Solution Deployment Manager client provides the functionality to install the OVAs on an Avaya-provided server or customer-provided Virtualized 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 and Virtualized Environment.
- Upgrade System Platform-based System Manager.
- Upgrade Virtualized Environment-based System Manager from Release 7.0.x to Release 7.1 and later.

- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.
- Create 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™.

**Note:**

You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.

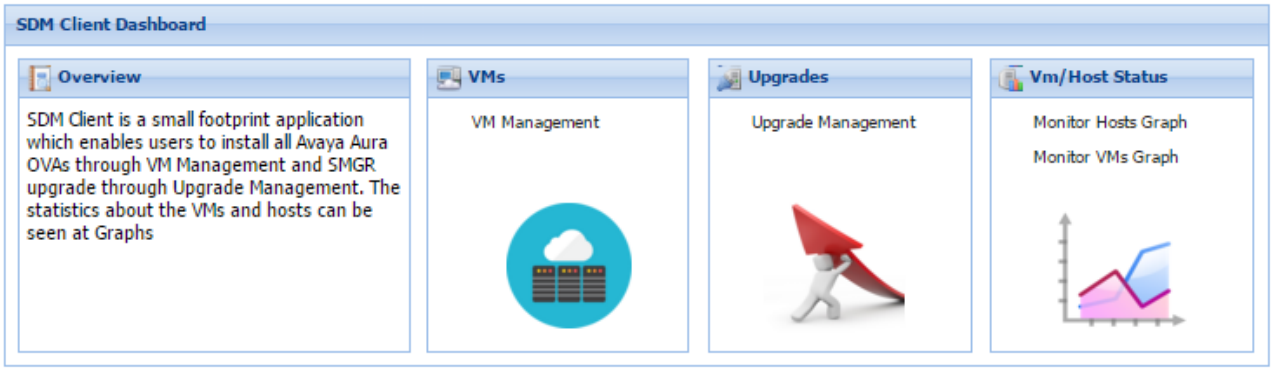



**Figure 2: Solution Deployment Manager client dashboard**

### Related links

Solution Deployment Manager overview on page 18

# Solution Deployment Manager

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

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

- Utility Services 7.1.3
- System Manager 7.1.3
- Session Manager 7.1.3
- Branch Session Manager 7.1.3
- Communication Manager 7.1.3
- Application Enablement Services 7.1.3

- WebLM 7.1.3
- Avaya Breeze™ 3.3.x with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0
- Avaya Aura® Device Services 7.1.2
- Avaya Aura® Media Server 7.8
- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

  For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

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

- Linux-based Communication Manager 5.x and the associated devices, such as Gateways, TN boards, and media modules.

  **Note:**

  In bare metal Linux-based deployments, the applications are directly installed on the server and not as a virtual machine.
- 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

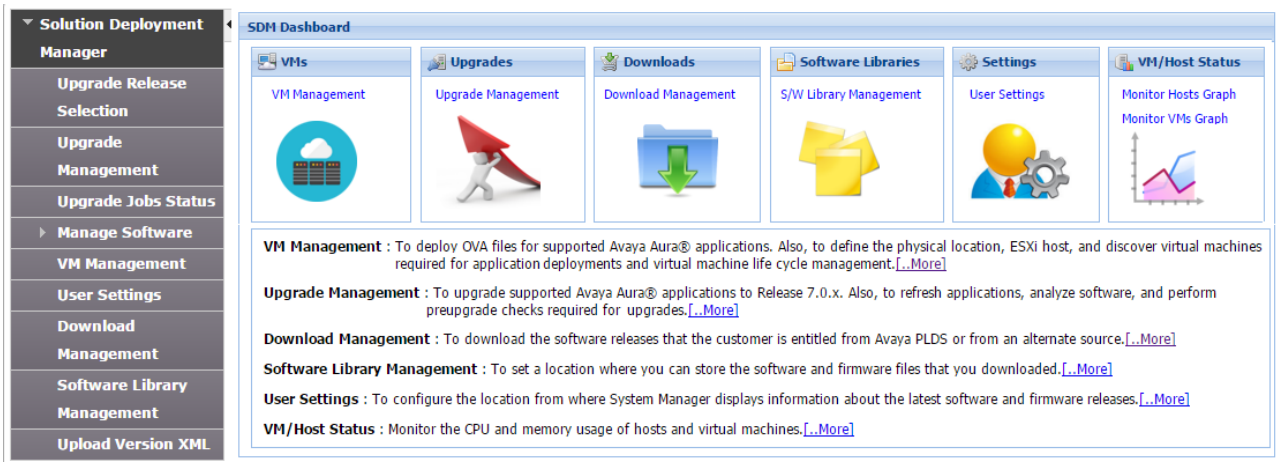
**Note:**

However, you must manually migrate Services virtual machine that is part of the template.

The centralized deployment and upgrade process provide better support to customers who want to upgrade their systems to Avaya Aura® Release 7.1.3. 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.




## 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 7.0** or **6.3.8** as the target upgrade. Release 7.1.3 is the default upgrade target.
- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module (UCM) and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **VM 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 Communication Manager that includes TN boards, media gateways and media modules, Session Manager, Communication Manager Messaging, Utility Services, Branch Session Manager, WebLM to Release 7.1.3.
- **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 `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 7.1.3:

- Communication Manager
- Session Manager
- Branch Session Manager
- Utility Services
- WebLM

**Note:**

You must upgrade System Manager to Release 7.1.3 by using the Solution Deployment Manager client before you upgrade the Avaya Aura® applications to Release 7.1.3.

# Support for VMware components

Avaya Aura® Release 7.1 and later supports deployment and upgrades on the following VMware components in Virtualized Environment.

- VMware® vSphere ESXi 5.5
- VMware® vSphere ESXi 6.0
- VMware® vSphere ESXi 6.5
- VMware® vSphere ESXi 6.7
- VMware® vCenter Server 5.5
- VMware® vCenter Server 6.0
- VMware® vCenter Server 6.5
- VMware® vCenter Server 6.7

**Note:**

- vSphere ESXi 6.7 is supported for Avaya Aura® Release 7.1 and later. Avaya Aura® Release 7.0.x and earlier does not support vSphere ESXi 6.7.
- vSphere ESXi 6.5 is supported for Avaya Aura® Release 7.1 and later. Avaya Aura® Release 7.0.x and earlier does not support vSphere ESXi 6.5.
- With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware® vSphere Client for ESXi and vCenter administration.
- Avaya Aura® Release 7.1 and later does not support vSphere ESXi 5.0 and 5.1.

# OVA signing

To ensure the integrity of the Avaya Aura® application OVAs, Avaya digitally signs the application OVAs. You can view the digital signature at the time of deploying and upgrading the application.

**Note:**

For Release 7.1 OVAs, Solution Deployment Manager and vCenter validates the certificate at the time of deployment. For 7.0 OVAs, you must manually check the md5sum values posted on the PLDS website against the downloaded images before the deployment.

# IPv6 support

Avaya Aura® Release 7.1 and later supports dual stack IP addressing. This enables you to provide IPv4 and IPv6 addresses at the time of:

- Deploying and upgrading the Avaya Aura® applications.
- Configuring the network settings.

# Support for TLS version

Avaya Aura® Release 7.1 and later supports the TLS version 1.2. By default, TLS versions 1.0 and 1.1 are disabled, but you can enable, if required.

# Enhanced Access Security Gateway (EASG)

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

# Supported Linux operating system version

Avaya Aura® Release 7.1 applications use the Red Hat Enterprise Linux operating system Release 7.2 with 64-bit.

**Note:**

Utility Services Release 7.1 uses the Red Hat Enterprise Linux operating system Release 7.3 with 64-bit.

# Compliance with DISA security STIGs

Following products are compliant with the security requirements stated in Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG).

- Appliance Virtualization Platform
- Utility Services
- System Manager
- Session Manager
- Communication Manager
- Presence Services
- Application Enablement Services
- Branch Gateway

# Chapter 5: What's new in Appliance Virtualization Platform

This chapter provides an overview of the new features and enhancements for Avaya Aura® Appliance Virtualization Platform Release 7.1 and later.

For more information about features and administration, see *Migrating and Installing Avaya Aura® Appliance Virtualization Platform*.

## New in Appliance Virtualization Platform Release 7.1.2

### Configuration of the Appliance Virtualization Platform license file

From Appliance Virtualization Platform Release 7.1.2, you must install and configure an applicable license file for each Appliance Virtualization Platform host. Appliance Virtualization Platform licenses are according to the supported server types.

### Extended Security hardening

From Appliance Virtualization Platform Release 7.1.2, you can enable or disable the commercial grade security hardening for the Appliance Virtualization Platform host.

### Migration of the System Platform-based system and elements to Appliance Virtualization Platform remotely

You can migrate the System Platform-based system and elements to Appliance Virtualization Platform remotely by using the **Migrate With AVP Install** check box through System Manager Solution Deployment Manager.

For more information, see *Upgrading and Migrating Avaya Aura® applications from System Manager*.

## New in Appliance Virtualization Platform Release 7.1

### Generation of the Appliance Virtualization Platform kickstart file using Solution Deployment Manager

From System Manager Release 7.1, you can generate the kickstart file (`7.1ks.cfg`) by using Solution Deployment Manager for installing Appliance Virtualization Platform.

### Stricter password policy

You can enable or disable the stricter password policy.

### Support of third party certificate

You can import third party certificates to an Appliance Virtualization Platform host by using Solution Deployment Manager. Certificates key length must be 2048.

### Supported upgrade path

- From Appliance Virtualization Platform Release 7.0 to Release 7.1
- From System Platform-based Release 6.x applications to Appliance Virtualization Platform Release 7.1.

### Troubleshooting

From Appliance Virtualization Platform Release 7.1, vSphere Web Client replaces the VMware® vSphere Client for advanced troubleshooting.

# Chapter 6: What's new in Utility Services

This chapter provides an overview of the new features and enhancements for Avaya Aura® Utility Services Release 7.1 and later.

## New in Utility Services Release 7.1.3

### Linux kernel configuration

Utility Services Release 7.1.3 includes the Red Hat updates to support mitigation of the Meltdown and Spectre vulnerabilities. However, this can affect the performance of Utility Services. So, a script **`kernel_opts.sh`** is introduced that allows the setting of kernel options to control how these vulnerabilities are handled. The effect of running the kernel configuration script is immediate and will continue across reboots. You can run the script as an admin user by using the CLI.

The script has the following arguments:

- status — Displays the current status of the kernel options.
- enable — Enables all flags to provide maximum protection.
- disable — Disables all flags to provide maximum performance.

## New in Utility Services Release 7.1.2

### Appliance Virtualization Platform alarming

The Serviceability Agent that runs on Utility Services generates Appliance Virtualization Platform SNMP alarm messages. The alarm messages are then sent to the System Manager or Network Management System (NMS) depending on the configuration. Serviceability Agent converts specific rsyslog entries to SNMP traps.

You can configure the destination of alarm messages by using one of the following: :

- The System Manager web console.

- Utility Services CLI.

**Note:**

If System Manager does not exist in the solution, then you can configure NMS by using the Utility Services CLI.

## Extended security hardening

Avaya Aura® Utility Services 7.1.2 supports extended security hardening to reduce vulnerabilities and enhance the security of the Utility Services application. Utility Services 7.1.2 supports extended security hardening when deployed in one of the following modes only:

- Services Port Only
- Hardened Mode Services Port Only

# New in Utility Services Release 7.1

## Browser support

Utility Services supports the following browsers:

- Internet Explorer version 11.x
- Microsoft Edge (Spartan) Browser (included with Windows 10)
- Firefox versions 48, 49, and 50
- Google Chrome 53, 54, and 55

## Third-party certificate support

Utility Services contains a default certificate suite, but customers are recommended to install their own third-party certificates. IP Phones must have compatible third-party certificates. This enables IP Phones to use secure HTTP with Utility Services when downloading firmware and configuration files.

## Support for SHA-256 Signed IP Phone Firmware Packages

Utility Services Release 7.1 supports SHA-256 signed IP Phone firmware packages.

## Features not supported in Release 7.1

**Remote CDR Database Access:** : Utility Services Release 7.0.x and earlier supports read-only access to the CDR Database through the standard Postgres port 5432 to enable users to write their own CDR reports. With the security related improvements in Red Hat Enterprise Linux operating system Release 7.x, Utility Services Release 7.1 does not support this feature.

**Phone Firmware Manager (PFM):** : PFM uses a Java component that does not support modern ciphers that are in Utility Services Release 7.1. Therefore, Utility Services Release 7.1 does not support PFM.

# Chapter 7: What's new in System Manager

This chapter provides an overview of the new features and enhancements of System Manager Release 7.1 and later.

## New in System Manager Release 7.1.3

Avaya Aura® System Manager Release 7.1.3 supports the following new features and enhancements:

- System Manager supports cluster level alarms.
- For the 9641SIP template type, an **Attendant** check box is available:
  - On the New/Edit/View/Duplicate User Profile pages in the CM Endpoint Profile section.
  - On **General Options** tab on the New/Edit/View/Duplicate/ Endpoint, Global Endpoint Change, and New Endpoint Template pages.

  If you select the **Attendant** check box, you can administer the endpoint as an attendant.
- For the SIP template type, the **SIP URI** field is available:
  - On the New/Edit/View/Duplicate User Profile pages in the CM Endpoint Profile section.
  - On the New/Edit/View/ Hunt Group page.
- Bulk import and export of **Endpoints**, **Coverage Paths**, and **Hunt Groups** using System Manager. For adding, deleting and updating **Endpoints**, **Coverage Paths**, and **Hunt Groups** 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:
  - For Endpoints: **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** page
  - For Coverage Path: **Elements** > **Communication Manager** > **Coverage** > **Coverage Path** page
  - For Hunt Group: **Elements** > **Communication Manager** > **Groups** > **Hunt Group** page
- Using the `securityHardeningOptions` command, you can enable or disable one or more than one security hardening options. The security hardening options that you can:
  - Enable are selinux, audit, fips, aide, TLSv1, TLSv1.1, and TLSv1.2.

- Disable are selinux, audit, and aide.

- Using the `/swlibrary/reports/generate_report.sh` script, you can generate the report of virtual machines that are installed on the Appliance Virtualization Platform host.
- Using **More Actions** > **Snapshot Manager** on the **Hosts** tab, you can delete the virtual machine snapshots that are running on the Appliance Virtualization Platform host.

# New in System Manager Release 7.1.2

Avaya Aura® System Manager Release 7.1.2 supports the following new features and enhancements:

- Management of trunk group by using System Manager enhanced editor. Using the enhanced editor, you can:
  - Add, edit, view, and delete trunk group.
  - Schedule the addition and deletion of trunk group for a specific time.
  - Assign permissions to add, edit, view, and delete the trunk group for a user.
- Bulk import and export of Vector Directory Numbers (VDNs) using System Manager. For adding, deleting and updating VDNs in bulk, you can download a pre-loaded excel `VdnData.xlsx` file from **More Actions** > **Download Excel Template** on the **Elements** > **Communication Manager** > **Call Center** > **Vector Directory Number** page.
- Export of the added, updated, or deleted user-related data for the specific delta period. You can export the delta users from **More Actions** > **Export Delta Users** on the **Users** > **User Management** page.
- Migration of the System Platform-based system and elements to Appliance Virtualization Platform remotely by:
  - Using the **Migrate With AVP Install** check box through System Manager Solution Deployment Manager.
  - Importing the `AVP_Bulk import spread sheet.xlsx` spreadsheet through System Manager Solution Deployment Manager.
- System Manager Solution Deployment Manager automates the migration of Communication Manager LSPs to Release 7.1.2.
  - Communication Manager LSPs from Release 6.x Templates: Simplex Survivable Remote and Survivable Remote. This can include Communication Manager, Utility Services, or Branch Session Manager.
  - Communication Manager Release 5.2.1 bare Metal on S8300D

  Hardware Supported: S8300D, S8300E, and Common Server (1, 2 and 3) when configured as an LSP

- New System Manager Solution Deployment Manager capabilities:
  - Bulk Provisioning File (Excel): ability to import configuration parameters in bulk for upgrading or migrating to Appliance Virtualization Platform remotely.
  - Appliance Virtualization Platform upgrade integrated into the functions: Software Library, Analyze, Pre-upgrade checks, Logging, and RBAC.
- Configuration of WebLM Server that hosts the Appliance Virtualization Platform Release 7.1.2 license file. To fetch the license file for the Appliance Virtualization Platform host, you can configure the WebLM Server details under **More Actions** > **WebLM Configuration** on the **Hosts** tab.
- While updating the Appliance Virtualization Platform host, you must accept the End User License Agreement.
- Remote access of System Manager Web console and Command Line Interface by using EASG Login credentials for Avaya Technician.

# New in System Manager Release 7.1.1

Avaya Aura® System Manager Release 7.1.1 supports the following new features and enhancements:

- Management of hunt group by using System Manager enhanced editor. Using the enhanced editor, you can:
  - Add, edit, view, and delete hunt group.
  - Schedule the addition and deletion of hunt group for a specific time.
- Assign permissions to add, edit, view, and delete the hunt group and attributes of hunt group for a user. You can also specify the extension range for adding hunt group extensions.
- If Platform Service Controller (PSC) is configured to facilitate the SSO authentication service to a vCenter, then you can provide the IP or FQDN of PSC at the time of adding a vCenter to Solution Deployment Manager.
- For generating the kickstart file for the Appliance Virtualization Platform installation, the **Confirm Password** field is added on the Generate AVP Kickstart page.

# New in System Manager Release 7.1

Avaya Aura® System Manager Release 7.1 supports the following new features and enhancements:

- From System Manager Release 7.1, the root user account is disabled. You must log in with the administrator privilege account that you create during deployment or upgrade of System

Manager. You can use the same account for performing various operations on System Manager.

- Security profiles to enable hardened security modes:
  - Standard Grade Hardening
  - Commercial Grade Hardening
  - Military Grade Hardening
- Support for IPv6 addresses with dual stack.
- The System Manager system that has security hardening enabled, displays the login warning banner message.
- Authentication based on certificate to facilitate password-less login for System Manager user interface and CLI access.
- System Manager backup encryption based using a global password.
- Audit logging configuration to notify the System Manager administrator and perform the configured action in certain cases:
  - Audit failure
  - 75% occupation of audit partition
  - 90% occupation of audit partition
- Prerequisite for enabling and configuring Geographic Redundancy:
  1. Adding the primary System Manager server as Certificate Revocation List (CRL) in the secondary System Manager server.
  2. Adding trusted certificate of primary System Manager server to secondary System Manager server.
- Enhancements to Upgrade Management in System Manager:
  - Upgrade rollback option for System Manager instance those are present on the same host.
  - OVA, Data migration, and Service or Feature Pack file selection from **URL**, **S/W Library**, or **Browse**.
- When upgrading System Manager through CLI, you can use the different network parameters to configure the new system. However, the virtual FQDN (vFQDN) must be same on the new system as you recorded on the existing system.

  While restoring backup on the new system, you must use the same network and system parameters of the old system from which you have taken the backup. This is applicable for both regular backup/restore and cold standby procedures.
- Support for Remote Syslog server details configuration in System Manager:
  - Adding, editing, and deleting Syslog receiver configuration.
  - Viewing and pushing the virtual machine system log to the configured Syslog server.
- Regeneration of Symmetric and Asymmetric data protection keys in case of outdated or compromised keys.

- OVA signing to digitally sign OVAs to ensure the file integrity.
- Validation of file format during operations, such as uploading certificates, upgrades, and bulk importing users. System Manager filters uploaded files based on the file extension and mime type or bytes in the file.
- Using System Manager Web console, create kickstart file to install Avaya Virtualization Platform.
- For generating the new license file, the value of **Primary Host ID** is now 14 characters.

# Supported browsers

You can access the Avaya Aura® System Manager web interface on the following browsers:

- Internet Explorer 11.x and later
- Mozilla Firefox 48, 49, and 50

# Syslog Profile configuration

The Syslog service provides capabilities, such as configuration and pushing of system logs to Syslog servers. The Syslog service sends the system logs to the configured remote Syslog profile through TCP or UDP.

Syslog service also provides configuration for TLS-based remote host profiles. Users must import the remote syslog server certificate in System Manager if system logs are to be forwarded over TLS.

# Third-party certificate support

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

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

# Security hardening

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

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

# Certificate-based authentication

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

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

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

# Backup encryption

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

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

# Preserve disk on upgrade

From Release 7.1, disk preservation from old virtual machine to new virtual machine can be performed as specified in OVF for the element.

# Audit Logging

Using the audit logging configuration in System Manager 7.1, the system can notify the System Manager administrator and perform the configured action during one or all of the following events:

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

# Geographic Redundancy configuration prerequisites

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

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

# Regeneration of data protection keys

The service for regenerating security keys provides a utility to regenerate symmetric and asymmetric data protection keys for System Manager. These keys must be regenerated when the existing keys are outdated or if the system security is suspected to be compromised.

# Certificate revocation

With System Manager 7.1, you can revoke certificates to render them invalid, or to put them on hold. To implement the revocation, create a new CRL after the certificate is revoked. Only revoked certificates that are on hold can be unrevoked.

# Generation of the Appliance Virtualization Platform kickstart file using Solution Deployment Manager

From System Manager Release 7.1, you can generate the kickstart file (`7.1ks.cfg`) by using Solution Deployment Manager for installing Appliance Virtualization Platform.

# Security hardening options

System Manager provides the following security hardening options:

- selinux
- audit
- fips
- aide
- TLSv1, TLSv1.1, and TLSv1.2

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

# Virtual machine report

With System Manager Release 7.1.3 and later, you can generate a report of virtual machines that are installed on the Appliance Virtualization Platform host.

The script to generate the virtual machine report is in the `/swlibrary/reports/generate_report.sh` folder.

**Important:**

If you run the report generation script when an upgrade is in progress on System Manager, the upgrade might fail.

# Chapter 8: What's new in WebLM

This chapter provides an overview of the new and enhanced features of WebLM Release 7.1.

## New in Avaya WebLM Release 7.1.2

Avaya WebLM Release 7.1.2 supports the following new features:

### Deployment of Standalone Avaya WebLM on Amazon Web Services

You can deploy WebLM Release 7.1.2 and later on Amazon Web Services (AWS).

### Deployment of Standalone Avaya WebLM on Kernel-based Virtual Machine

You can deploy WebLM Release 7.1.2 and later on Kernel-based Virtual Machine (KVM).

KVM support is based on Red Hat Enterprise Linux operating system Release 7.3.

## New in Avaya WebLM Release 7.1

Avaya WebLM Release 7.1 and later supports the following new features and enhancements:

### Upgrade through Solution Deployment Manager

You can upgrade WebLM Release 7.1 and later by using Solution Deployment Manager

The system retains the Host ID after the WebLM system is upgraded.

### Browser support

WebLM Release 7.1 and later supports the following browsers:

- Internet Explorer 11.x and later
- Mozilla Firefox 48, 49, and 50

### Security enhancements

WebLM Release 7.1 and later supports SHA256 digital signature for signing the license files and the 14-character host ID.

# Chapter 9: What's new in Session Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® Session Manager Release 7.1 and later.

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

## New in Session Manager Release 7.1.3

### Support for User-to-User information in Session Manager CDR

From Release 7.1.3, Session Manager is enhanced to capture the contents User-to-User header, which contains the UCID value. The XML based CDRs are enhanced to support this function. When Session Manager receives INVITE request with User-to-User header, Session Manager copies the content of User-to-User in to the *uu-info* element of the CDR XML file.

### Ability to enable or disable AIDE

With Session Manager Release 7.1.3, you can selectively enable or disable Advanced Intrusion Detection Environment (AIDE). By default, AIDE is disabled.

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

### Support for SIP Attendant

With Session Manager Release 7.1.3, you can route SIP Attendant Console calls to Avaya Breeze™ based Avaya Equinox® Attendant.

# New in Session Manager Release 7.1.2

## Support for collecting CPU statistical data

With Session Manager Release 7.1.2, the **CPU** tab is restored on the System Performance page to collect the CPU statistical data. Earlier the **CPU** tab was available on the Session Manager Release 7.0 system. User can generate CPU Usage report which includes the following details:

- User
- System
- Idle
- IO Wait

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

## User registrations export enhancement

With Session Manager Release 7.1.2, a new **Start Export Job** button is added on the User Registration Export page for exporting more than 100,000 user registrations.

The system schedules the job to run immediately. After the job is complete, you can download the exported file with the registration data.

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

## Security hardening

With Session Manager Release 7.1.2, you can enable or disable the following profiles for Session Manager:

- Standard
- Hardened
- Custom

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

# New in Session Manager Release 7.1.1

## Ability to reboot SIP phone through Avaya Aura® System Manager API

The System Manager Web services interface allows remote rebooting of SIP phone.

The System ManagerWeb services interface provides programmatic access to the Session Manager dashboard and user registration data for querying, creating, and deleting all Session Manager routing domain data.

The System Manager Web Services API enforces the same level of data integrity as the GUI and import interfaces. The API components enforce the same validation logic the GUI and Import interfaces use.

The System Manager Web Services API is available on the Avaya DevConnect Web site at https://www.devconnectprogram.com/site/global/home/p_home.gsp.

## Emergency Calling Application Sequence

In the release 7.1.1, administrators can enable application for emergency calls. Administrators can assign emergency calling application sequences to a user.

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

## Regular Expression Pattern Rule

In the release 7.1.1, a new tab for regular expression pattern rules is introduced on the Implicit User Rule Editor page. This tab enables the administration of application sequences for emergency calling using regular expression based pattern rules.

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

## Backup and restore of pluggable adaptation modules

From the release 7.1.1, Session Manager supports backup and restore of pluggable adaptation module parameters. Pluggable adaptation module parameters are preserved during the upgrade of Session Manager.

## Ability to get user registration details through System Manager web console

With Avaya Aura® Session Manager Release 7.1.1, you can view the summary of user registration from the System Manager web console. For more information, see *Administering Avaya Aura® Session Manager*.

## Support for PIDF-LO

Avaya Aura® Session Manager Release 7.1.1 supports RFC 6442 and RFC 4975 to pass the Presence Information Data Format - Location Object (PIDF-LO) when a call is sequenced to Avaya Breeze™ application.

# New in Session Manager Release 7.1

## Complex Station Access Code

In Session Manager, administrators can set up a **Station Admin Password** to ensure secure log in and administration of the SIP phone. Before Release 7.1, Session Manager accepted only numeric values up to 32 digits in the **Station Admin Password** field.

From Session Manager Release 7.1, the administrator can define the Complex Station Access Code validation rules using the Station Access Code Policy screen on the Device and Location Configuration page. The administrator can establish parameters to define the access codes, such as minimum length, allowed characters, and inclusion of minimum character sets.

The administrator can set a numeric Station Admin Password and Complex Station Access Code simultaneously. Therefore, the system can support End of Sale (EOS), End of Life (EOL), and earlier endpoints along with new endpoints. Session Manager uses Complex Station Access Code for SIP 96x1 and Avaya J100 Series IP Phones. For desk phones earlier than 96x1, the system continues to use the numeric Station Admin password.

Complex Station Access Code is encrypted using encryption algorithm ensuring code security.

### Station Access Code policy constraints

- The administrator must define the minimum required length from 6 to 25 characters.

- The administrator must define one of the following:
  - Minimum character set. Administrator can choose any combination from the following character sets:
    - Upper case
    - Lower case
    - Numerics
    - Special characters
  - Minimum required characters for each character set.

  For example, set the **Minimum character set** field to 0 and **Upper case** and **Special character** set to 1. In this case, any password containing one upper case and special character is a valid Station Access Code.

  If you set the **Minimum character set** field to 2, the password must contain at least two characters from the numeric, upper, or special character sets.
- The administrator must ensure that the minimum required length is equal to or greater than the number of characters required for each character set.

**Note:**

If a password does not meet the password strength policy, the Device and Location Settings group administrator rejects the password.

## Certificate Revocation Lists

Digital Certificates identify communication entities in a Public Key Infrastructure (PKI). Certificate Authorities (CAs) issue certificates with a validity period. During validation, communicating entities ensure the certificate has not expired and also check the revocation status of the certificate. At times, the issuing CA might want to revoke the certificate before it expires. For example, when an employee leaves the company, the CA must revoke the certificates issued to that employee to avoid misuse. Session Manager 7.1 uses the Certification Revocation List (CRL) method for checking certificate revocation.

CRLs contain a list of serial numbers for certificates that are revoked. Entities with a revoked certificate must no longer be trusted. To revoke a certificate:

- The Certificate Authority (CA) administrator can log on to a CA and revoke the certificate.
- The CA publishes the CRL to an HTTP or LDAP repository referenced in the CRL Distribution Point (CDP) extension of a certificate.

Session Manager performs the required certificate revocation checks based on the global Certificate Revocation Check policy that is configured on System Manager.

If Certificate Revocation Checking is enabled, every certificate exchanged while establishing a TLS connection is verified against a CRL. Before using a CRL, Session Manager verifies the validity of CA’s digital signature in a CRL.

System Manager provides the ability to periodically download CRLs in advance to make them available before a TLS connection is attempted. If a CRL is not previously downloaded, the

system might attempt to download the CRL when trying to establish a TLS connection. In that case, the system attempts to download the CRLs from the URI specified in the certificate's CRL Distribution Point (CDP) extension. Multiple CDP locations may be included in the CDP extension. If multiple CDP locations are specified, an attempt is made to download a CRL from the first location, followed by the next location, and so on, until the system either downloads a CRL or times out.

### CRL revocation checking options

The following CRL revocation checking options are available:

- Mandatory: The certificate is considered valid if all CRLs in a certificate chain can be fetched and no certificate is present on any CRL.
- Best effort: The certificate is considered valid if none of the CRLs in a certificate chain that have been fetched indicate that the certificate has been revoked, or if CRL cannot be fetched.
- Off: No CRL revocation checking is performed.

## Assured Services SIP

Session Manager supports the Assured Services SIP feature by using a combination of different features. Administrators can enable or disable the Assured Services SIP feature using a Session Manager global setting and configuring the supported network domain. By default, the feature is disabled.

### Multilevel Precedence and Preemption

Session Manager allocates bandwidth to calls based on the priority of the calls. Session Manager determines the priority of the call from the Resource-Priority header in the Invite request. If Session Manager does not have adequate bandwidth to allocate to a high-priority call from the specific domain that is configured for precedence, Session Manager preempts one or more lower-priority calls. Preempting lower-priority calls frees up the associated bandwidth, allowing Session Manager to ensure that adequate bandwidth is available to successfully establish high-priority calls.

### Assured Services Admission Control

Assured Services Admission Control assigns bandwidth limits for audio and video to network entities and links. Assured Services Admission Control also monitors the bandwidth usage and ensures that the bandwidth used by network entities and links does not exceed the specified limits.

### Assured Services for SIP IP gateway

The Assured Services SIP IP gateway supports the insertion of necessary routes between Enterprise Session Controllers and Local Session Controllers which are connected with soft switches and SBCs. Session Controllers insert a primary route, which passes through a designated set of SBCs, when processing calls to the primary soft switch. The insertion of the primary route ensures that the routes of all calls are established through the set of SBCs. If the primary route components or the network fails, Session Controllers detect the failure using the SIP

OPTIONS method. Session Controllers establish all subsequent calls using the alternate route to the secondary soft switch that passes through a secondary set of SBCs.

## Ping-pong based health check mechanism

From Release 7.1, Session Manager provides the client and server side support of the ping-pong based health check mechanism for SIP entities. Previously, Session Manager only provided the server side support for endpoint connections. The administrator can enable and disable ping-pong based health monitoring at the SIP Entity level with the SIP entities. Session Manager as a client generates a ping or a double Carriage Return and Line Feed (CRLF). The response to a ping is a pong or a single CRLF response. If the Session Manager does not receive a pong response, it will mark the SIP Entity as down. Session Manager waits up to 10 seconds to receive a pong in response to a ping it sent out.

By default, the ping-pong based health monitoring is disabled. When ping-pong based health monitoring is enabled, the administrator can set the ping interval between 1 and 900 seconds. The default value of the ping interval is 120 seconds. After the ping-pong based health monitoring is enabled, Session Manager can send a periodic ping at the administered level.

# Chapter 10: What's new in Communication Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® Communication Manager Release 7.1.

For more information about these features, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

## New in Communication Manager Release 7.1.3

### Support for 9000 announcements

In earlier releases, Communication Manager supported 1024 announcements only. With Communication Manager Release 7.1.3, you can configure up to 9000 announcements for a single Avaya Aura® Media Server instance.

### Malicious Call Trace support on SIP

Communication Manager Release 7.1.3 can send Malicious Call Trace (MCT) notifications over SIP trunks.

### Alphanumeric URI dialing support

In Communication Manager Release 7.1.3:

- You can assign alphanumeric URIs to hunt groups and vector directory numbers (VDNs)
- You can dial a hunt group and a VDN using the SIP URI
- When a call is made from a station to a hunt group or a VDN using SIP URI, the call is sent to respective hunt group or VDN
- You can use alphanumeric handles for the following features:
  - Call forwarding
  - Priority calling
  - Whisper page
  - Directed call pickup
  - CPN block and unblock
  - Call unpark

**Note:**

Communication Manager supports alphanumeric URI dialing for SIP phones only.

### Security hardening commands enhancement

The following security hardening commands used in Communication Manager Release 7.1.2 are renamed in Communication Manager Release 7.1.3:

| Security hardening command name in Communication Manager Release 7.1.2 | Security hardening command name in Communication Manager Release 7.1.3 |
|---|---|
| `MUDG_part1` | `setCMHardening` |
| `sudo updateRegistry UseAIDE=enabled`<br>`sudo setPlatformAttributes` | `setCMAide` |
| `sudo updateRegistry UseClamav=enabled`<br>`sudo setPlatformAttributes` | `setCMClamav` |

### Support for SIP attendant

In Communication Manager Release 7.1.3, you can route attendant console calls to Avaya Breeze™-based Avaya Equinox® Attendant.

### Linux kernel configuration

Communication Manager Release 7.1.3 includes the Red Hat updates to support mitigation of the Meltdown and Spectre vulnerabilities. However, this can affect the performance of Communication Manager. So, a script **`kernel_opts.sh`** is introduced that allows the setting of kernel options to control how these vulnerabilities are handled. The effect of running the kernel configuration script is immediate and will continue across reboots. You can run the script as an admin user by using the CLI.

The script has the following arguments:

- status — Displays the current status of the kernel options.
- enable — Enables all flags to provide maximum protection.
- disable — Disables all flags to provide maximum performance.

# New in Communication Manager Release 7.1.2

## Alphanumeric URI dialing

An alphanumeric URI consists of alphanumeric handles that are used to identify a directory number. In Communication Manager Release 7.1.3:

- You can assign alphanumeric URIs to hunt groups and vector directory numbers (VDNs).

- You can dial a hunt group and a VDN by using the SIP URI. When a call is made from a station to a hunt group or a VDN by using SIP URI, the call is sent to the respective hunt group or VDN.
- You can use alphanumeric handles for the following features:
  - Call forwarding
  - Priority calling
  - Whisper page
  - Directed call pickup
  - CPN block and unblock
  - Call unpark

**Note:**

To use alphanumeric URIs, you must configure the users with both the numeric handle and the alphanumeric handle in System Manager, and assign the numeric handle as Preferred in System Manager. For more information on configuring the users with alphanumeric URI dialing, see the description of **Preferred Handle** in the “New User Profile field descriptions” section in *Administering Avaya Aura® System Manager*.

Communication Manager Release 7.1.2 and later support placing and receiving calls by using alphanumeric URIs. Communication Manager supports alphanumeric handles on both SIP and H.323 deskphones.

Communication Manager supports the following format for an alphanumeric URI:

- <handle>@domain. For example, 123john@avaya.com

After you configure users with alphanumeric URI dialing, you can:

- Register users by using an alphanumeric handle.
- Place calls to an alphanumeric URI.

## Extended security hardening

You can harden Communication Manager 7.1.2 and later to reduce vulnerabilities and enhance the security of the Communication Manager application. Hardening the Communication Manager provides an additional security mechanism to your application.

# New in Communication Manager Release 7.1.1

## Support for Channel Type identification over ASAI to CTI application

Communication Manager Release 7.1.1 supports channel type identification over ASAI to a CTI application. For incoming SIP trunk calls, Communication Manager Release 7.1.1 identifies the channel type as voice, video, or unknown when the call:

- Enters a monitored Vector Directory Number (VDN) or hunt group (skill/split).
- Is monitored and is alerting at a deskphone or Agent.

For this feature to work, the CTI link between Communication Manager and Application Enablement Services must be greater than 7.

This feature might not work or might show an unknown channel type on the CTI application when:

- The Direct Media feature is enabled.
- Communication Manager is not able to identify the channel from the incoming SIP request.

## Support for Service Observe and Barge-in features using feature access code through ASAI

Communication Manager Release 7.1.1 enables Avaya Oceana™ Solution to:

- Perform Service Observe and Barge-in operations on a voice channel.
- Add a Service Observer to a call by using Feature Access Codes.
- Toggle between listen-only and barge-in modes through CTI. To toggle between modes, Avaya Oceana™ Solution must drop a Service Observer while in a mode and add the Service Observer back while in another mode.

## Support to tandem MIME for PIDF-LO

Communication Manager Release 7.1.1 can tandem Multipurpose Internet Mail Extensions (MIME) attachments for Presence Information Data Format Location Object (PIDF-LO) in a SIP message. Communication Manager can also pass the PIDF-LO information in the SIP message.

## Support to drop or disconnect Service Observer from call using CTI application over ASAI

Prior to Communication Manager Release 7.1.1, a Service Observer was dropped or disconnected from a call only when the Service Observer goes on-hook. With Communication Manager Release 7.1.1, you can drop or disconnect a Service Observer from a call using a CTI application over ASAI.

# New in Communication Manager Release 7.1

## Updated browser support

Communication Manager Release 7.1 and later supports the following web browsers:

- Mozilla Firefox browser: version 45.0 and later
- Microsoft Internet Explorer browser: version 11

**Note:**

If you use unsupported browsers, some features might not work, or an application might not open.

## Compliance with DISA security STIGs

Communication Manager Release 7.1 is now compliant with the security requirements stated in Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs).

## Command History

Use this feature to define the number of months for which Communication Manager must maintain the command history and to compress the command history file after running the rotation action.

Define the number of months the system requires to maintain command history. Choose a duration between 3 months to 24 months.

In addition to the above, you can now compress the command history file after running the rotation action on the SMI page.

## CAC sharing between Communication Manager and Session Manager

Communication Manager can establish VoIP media for H.323 stations and trunks, for inter Port Network, gateway or Avaya Aura® Media Server IP connections and for non-Session Manager routed SIP trunks. These IP media connections are not visible to Session Manager. In Communication Manager 7.1, Session Manager can be configured as a central authority for bandwidth management. With this setting, Communication Manager requires bandwidth for voice and multimedia IP connections from Session Manager. You can set the bandwidth limits applicable for various locations through System Manager. For more information about setting bandwidth limits, see *Administering Avaya Aura® Session Manager*.

## Network preemption

Communication Manager supports network preemption. For network preemption to work, Communication Manager must be configured to use Session Manager as the bandwidth manager. To configure Session Manager as the bandwidth manager, see *Avaya Aura® Communication Manager Feature Description and Implementation*. The security administrator can assign bandwidth budgets for audio and video, to each network link on Session Manager. When server or network resources are running too low to allow additional calls, call preemption occurs. For more information, see *Administering Avaya Aura® Session Manager*.

## Discontinued support of default server identity certificate

From Communication Manager Release 7.1, the Communication Manager server no longer supports the use of the default server identity certificate, which is signed by Avaya Product Root CA, and is automatically loaded into the Communication Manager application Identity Certificate stores by Authentication File Server at the time of installation.

Starting with Communication Manager Release 7.1, you must import identity certificates for the Web Services application and the Communication User Services application.

To create Communication Manager Identity Certificates, do one of the following:

- Import certificates that are created and signed by a third party host. For example, Verisign.
- Create and sign the Identity Certificate for Communication Manager by using the Trust Management PKI feature of Avaya Aura® System Manager.
- Generate a Certificate Signing Request (CSR) by using the Communication Manager SMI interface. Send the CSR to a signing authority.

In each of the options, the Communication Manager SMI interface directs the download of the Identity Certificate to store into one or more of the Communication Manager application trust stores. These application trust certificates are exchanged during the TLS client or server handshake to securely confirm the identity of the Communication Manager application.

## Discontinued support of tethereal symbolic link to tshark

Communication Manager Release 7.1 and later does not support the symbolic link of tethereal command to the **tshark** command. Users must now use the **tshark** command to analyze the network traffic.

## Discontinued support for Telnet

Communication Manager Release 7.1 does not support Telnet.

# Chapter 11: What's new in Presence Services

This chapter provides an overview of the new and enhanced features of Presence Services Release 7.1.2.

### Zang federation

Presence Services Release 7.1.2 supports Zang federation. This feature enables:

- Sending IMs as SMS to a mobile user.
- Receiving SMS from a mobile user and deliver it as IM to an Aura user.

### Support for generic XMPP federation

Presence Services Release 7.1.2 supports generic federation with other XMPP servers. Any standards based XMPP server is supported using the generic XMPP federation.

### Support KVM deployment

Presence Services Release 7.1.2 supports deployment on Kernel-based Virtual Machine (KVM).

KVM is a full virtualization solution for Linux on x86 hardware. Using KVM, you can run multiple virtual machines that run various Avaya Aura components, including Presence Services on Breeze.

KVM virtualization solution is:

- Cost effective for the customers.
- Performance reliable and highly scalable.
- Secure as it uses the advanced security features of SELinux.
- Open source software that can be customized as per the changing business requirements of the customers.

For more information, see *Deploying Avaya Breeze™ on Kernel-based Virtual Machine for Avaya Aura®*.

### Support for Interoperability among clients

Presence Services Release 7.1.2 is compatible with existing Avaya endpoints that are used with Presence Services Release 7.x.

Presence/IM capable devices:

- Avaya Equinox 3.0, 3.1, 3.2 & 3.3
- 96X0 SIP (XMPP IM not supported)

- 96X1 SIP
- OneXC SIP
- OneXC H323
- Avaya Communicator
- Summit (XMPP IM not supported)
- One-X Agent

Non Presence/IM capable devices:

- 96X0 H323
- 96X1 H323

### Support for a privileged user

Presence Services Connector Release 7.1.2 supports a Service Attribute “Privileged User”, which will accept the login name of the presence-enabled Avaya Aura user. If you are using Equinox Attendant, then attendant user's login name is accepted.

For Equinox Attendant, ensure that only the attendant user has a service profile associated with Equinox Attendant snap-in.

### S4B interoperability with AMM using Federation Relay

Presence Services Release 7.1.2 supports additional routing assistance when AMM is included in Presence Services and Microsoft federation deployments.

If AMM is deployed, then the Session Manager routes IM messages to AMM. Else, Federation Relay will add a new flag “av-msfe-imgw” for IM messages, which will direct the Session Manager to route the IM messages to AMM. The flag allows the Session Manager to identify the Presence and IM messages, and route them to different destinations as required.

### Support for self-identity using REST API

Presence Services Release 7.1.2 supports self-identify using the following REST API:

**`application/vnd.avaya.presence-im.user-identity.v1+json`**

### Adding User’s ACL Policy to discover server capabilities

Presence Services Release 7.1.2 supports User’s ACL Policy , which is dynamic in nature that discovers Presence Services server capabilities.

### Support for Microsoft RTC status

Presence Services Release 7.1.2 supports the following:

- Subscribe for status with Microsoft RTC
- Publish status to Microsoft RTC

### Supported migration paths

The supported migration paths for Presence Services Release 7.1.2 are:

| Release | Requirement |
|---|---|
| 7.0.0.x | Direct upgrade to 7.1.2. |
| 7.0.1.x | Direct upgrade to 7.1.2. |
| 7.1.0 | Direct upgrade to 7.1.2. |

**Related links**

What’s new in Presence Services on page 56

# What’s new in Presence Services

This chapter provides an overview of the new and enhanced features of Presence Services Release 7.1.

## Compliance with DISA security STIGs

Presence Services is now compliant with the security requirements stated in Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG).

## Federation with Nextplane

Presence Services supports federation with Nextplane.

## Support for Multi User chat with Avaya Multimedia Messaging

Presence Services can interoperate with Avaya Multimedia Messaging (AMM) and an external XMPP federation system, such as Openfire, to support XEP-0045 style Multi-User Chat between AMM-enabled users and external XMPP federation users.

## Support for data filtering option

Presence Services implements a data filtering option to support:

- Reduce body size of the NOTIFY requests sent by Presence Services to endpoints.
- Reduce rate of notifications received by subscribing endpoints.

## Support for Interoperability among clients

Presence Services Release 7.1 is compatible with existing Avaya endpoints that are used with Presence Services Release 6.2.x and 7.0.x. Presence/IM capable devices:

- 96X0 SIP (XMPP IM not supported)
- 96X1 SIP
- OneXC SIP
- OneXC H323
- Avaya Communicator
- Summit (XMPP IM not supported)
- One-X Agent

Non Presence/IM capable devices:

- 96X0 H323
- 96X1 H323

Presence Services 7.1 is compatible with AMM 3.0, and with the new endpoints that support Rich Messaging.

### Supported migration paths

The supported migration paths for Presence Services Release 7.1 are:

| Release | Requirement |
|---|---|
| 6.x | Direct upgrade to 7.1. |
| 7.0.0.x | Direct upgrade to 7.1. |
| 7.0.1.x | Direct upgrade to 7.1. |

**Related links**

What’s new in Presence Services on page 54

# Chapter 12: What's new in Application Enablement Services

This chapter provides an overview of the new features and enhancements for Application Enablement Services (AE Services) Release 7.1 and later.

## New in AE Services Release 7.1.3

### Ability to enable TLS remote logging

With AE Services Release 7.1.3, you can enable TLS remote logging for secure and non secure connection between AE Services and remote rsyslog server.

### Certificate revocation configuration

The AE Services Release 7.1.3 introduces a certificate revocation configuration. The certificate revocation configuration is applicable for DMCC, TSAPI, and CVLAN client provided certificate validation and revocation check occurring on AE Services server.

## New in AE Services Release 7.1.2

### Support for Application Specific Licensing trusted applications

AE Services Release 7.1.2 supports the following Application Specific Licensing (ASL) trusted applications:

- Officelinx
- Avaya Cloud Application Link (ACAL)

- EP&T Breeze Snap-In
- CRA Breeze Snap-In

### Support for tracking pending agent work modes for Avaya Oceana™

AE Services Release 7.1.2 supports the pending agent work modes to track pending agent work modes for Avaya Oceana™.

## New in AE Services Release 7.1.1

### Channel Type identification over ASAI in Avaya Oceana™

AE Services identifies and indicates if the channel type is video or voice. This ensures proper solution level support of video in Avaya Oceana™.

Identifies an incoming SIP trunk call as either voice or video. AE Services 7.1.1 adds support for Channel Type in CSTA delivered and established events with the following values:

- `UNKNOWN` - The channel type is not specified
- `VOICE` - The channel type is voice
- `VIDEO` - The channel type is video

From AE Services Release 7.1.1, the TSAPI Service supports a new private data version: Version 13.

### ASAI version 8 support

AE Services7.1.x supports ASAI versions 1 thru to 8.

## New in AE Services Release 7.1

### TSAPI binary compatibility in Windows 10

AE Services 7.0.1 and earlier Windows-based client SDKs for TSAPI now support Windows 10 operating environment.

## Application Specific licensing support for AAWFO

AE Services now supports Application Specific licensing for Avaya Workforce Optimization Select (AAWFO Select). AAWFO Select is now an AE Services trusted application.

## Active Controlling Associations capacity increased from 32K to 50K

Active Controlling Associations are used to monitor stations only. The system wide capacity has been increased from 32000 associations to 50000 associations. Previously, the capacity was 32000 associations for large Communication Manager platforms, 32000 associations for medium Communication Manager platforms, and 2000 associations for small Communication Manager platforms.

## ASAI Notification Requests increased from 30K to 50K

In AE Services Release 7.1, ASAI Notification Requests have been increased from 30K to 50K. This enhancement is only limited to Communication Manager because it can support up to 50K ASAI event notifications and handle 50K domain control associations.

**Note:**

The limit on AE Services is 32K for each Communication Manager instance. However, when multiple AE Services are connected to a Communication Manager instance, the limit extends to support 50K. Also, when multiple Communication Manager instances are connected to one AE Services, it can support more than 32K.

The limit on AE Services is 32K for each Communication Manager instance. However, the limit extends to 50K in the following scenarios:

- Multiple AE Services are connected to a Communication Manager instance.
- Multiple Communication Manager instances are connected to one AE Services instance.

## Preservation of the AE Services Virtual Machine UUID

You can now preserve the Universally Unique Identifier (UUID) of the Virtual Machine (VM) by using Solution Deployment Manager (SDM) during an upgrade of the AE Services VM. The AE Services OVF profile is now updated to include the UUID_preservation_required property. This new OVF profile is packaged in the OVA and stored in the file. SDM preserves the UUID on an upgrade of the VM in both instances, VE and AVP . Rollback of the upgrade also preserves the UUID.

## VE and Avaya Appliance Upgrades from 7.0 and 7.0.1 to 7.1.1 using Solution Deployment Manager

Centralized System Manager Solution Deployment Manager now supports the upgrade of Avaya Aura® Application Enablement Services in VE and Avaya Virtual Appliance deployments from 7.0 and 7.0.1 to 7.1.1.

Once preupgrade checks are complete, System Manager Solution Deployment Manager maintains all configuration data, including automatic backup and restore of application data and settings. This ensures the deployment of the Avaya Aura® application OVA via a one-click upgrade process.

## License Preservation during AE Services upgrade using System Manager Solution Deployment Manager

The license file is preserved when AE Services Release 7.0.x is upgraded to AE Services Release 7.1.x using System Manager Solution Deployment Manager Release 7.1.x.

## Enterprise Directory Update

The AE Services 7.1.x external Enterprise Directory connection is only supported using the Secure LDAP (LDAPS) protocol.

## AE Services virtualization hardware resource increase

The supported AE Services 7.1.x virtual machine memory has increased by 2 GB for each of the supported AE Services footprint profiles. The disk space has increased to 30 GB.

## Remote Logging Support

rsyslog configuration to enable remote logging is now supported using the AE Services 7.1.x Management Console.

# Chapter 13: What's new in Media Server

The following chapter provides an overview of the new features and enhancements for Avaya Aura® Media Server Release 7.8.

## Configuration profiles

Additional Virtual Machine (VM) profiles for 16 vCPU have been added. The following newly added profiles are available in Avaya Aura® MS 7.8:

| Profile | Configuration |
|---|---|
| Profile 5 | 16 vCPUs, 16 GB Memory, 50 GB vDisk |
| Profile 6 | 16 vCPUs, 16 GB Memory, 250 GB vDisk |

## WebRTC Video Support

In addition to support for WebRTC in the previous releases of Avaya Aura® MS, this release adds video support for Google Chrome® and Mozilla Firefox® web browsers. This release also supports:

- A full range of video resolutions from 180p to 1080p is supported.
- Network congestion and loss countermeasures to provide the best possible experience over the open internet.

## System Manager enrollment updates

Some Avaya solutions which adopt Avaya Aura® MS use Avaya Aura® System Manager to provide an integrated point of management. You can use Avaya Aura® MS Element Manager (EM) to enroll media servers in Avaya Aura® System Manager.

Enrollment enables Avaya Aura® MS cluster management, single sign-on (SSO), and role-based access control (RBAC) managed by Avaya Aura® System Manager. After enrollment

administrators access the Avaya Aura® EM using Avaya Aura® System Manager administrative accounts which have permission to use EM.

This release adds the ability for the applications to discover media servers which have been assigned by the administrator on the System Manager. This capability is not widely used. See adoption solution documentation for applicability.

# Chapter 14: What's new in Branch Gateway

This chapter provides an overview of new features and enhancements for Branch Gateway Release 7.1 and later.

**Related links**

New in Branch Gateway Release 7.1.2 on page 64
New in Branch Gateway Release 7.1 on page 64

## New in Branch Gateway Release 7.1.2

The following new features and enhancements are available in Branch Gateway 7.1.2.

### Enhanced Access Security Gateway (EASG) support

Branch Gateway Release 7.1.2 now supports Enhanced Access Security Gateway (EASG). EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Logins to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

### EASG users

EASG access is permitted to five user accounts: init, inads, sroot, craft, and rasaccess.

### EASG Product certificate

The EASG Product certificate is embedded in gateway firmware. You can modify or replace the product certificate only through the new software deployment or through patch installation. Using the Branch Gateway CLI, you can view the EASG product certificate information.

**Related links**

What's new in Branch Gateway on page 64

## New in Branch Gateway Release 7.1

The following new features and enhancements are available in Branch Gateway 7.1.

### Password change on first login

Branch Gateway now prompts the user to change the password on the first login attempt.

### Notification message for a failed login

Branch Gateway now displays a notification message to a user who makes a failed login attempt.

### CLI Support for Secure Shell (SSH)

Branch Gateway CLI now allows the user to configure a set of ciphers, key exchange algorithms and MACs for SSH.

### Subject Alternate Name Validation for TLS

When enabled, this new TLS certificate validation option checks that the Subject Alternate Name field of the Root CA certificate matches the address of Communication Manager.

### TLS version selection

This new feature specifies what TLS versions are offered by the gateway when connecting to a server.

### Certificate Revocation Validation

Increased control over the degree of revocation validation that will performed when validating TLS Certificates.

### FIPS Mode Security

Ability to enable FIPS mode security.

**Related links**

What's new in Branch Gateway on page 64

# Chapter 15: What's new in Call Center Elite

This chapter provides an overview of the new and enhanced features of Call Center Elite Release 7.1.

## New in this release

## Agent Mobility integrates with Avaya Extension to Cellular

From Avaya Aura® Call Center Elite 7.1 onwards, Agent Mobility integrates with Avaya Extension to Cellular (EC500) enabling Expert Agent Selection (EAS) agents to function while outside the corporate network. Administrators can configure EC500 mapped mobile agents to log in and work while outside the corporate network. With the EC500 feature users can use a single number to make inbound and outbound calls. Do not configure EC500 Mobile Agents with local SIP extensions. Using Feature Name Extensions (FNEs), Mobile Agents can log in, log out, change work-modes, and query their work-mode. Agents can also use FNEs to perform additional functions, such as Idle Appearance Select, Conference Complete, Conference on Answer, Transfer Complete, and Transfer on Hang-Up.

**Note:**

Do not use Mobile Agents in an outbound contact center configuration.

## Agents log in to the available work mode

From Avaya Aura® Call Center Elite 7.1 onwards, administrators can ensure that when agents log in to Call Center Elite, they are automatically logged into the available work mode instead of the aux work mode. Administrators administer this feature on a per agent basis.

The administered work mode is overridden in the following cases:

- When an agent logs in to Call Center Elite using ASAI or CTI and the agent has entered a work mode using the ASAI or CTI command.

- When an agent logs in to Call Center Elite using Avaya one-X® Agent and the agent has specified a work mode.

# Agent identifier available in the VDN Return Destination feature

From Call Center Elite 7.1 onwards, the agent identifier can be added to the information available to the IVR system with a post-call survey. The agent identifier is made available in a new system-defined variable type in vectoring and is sent to an IVR application performing a post-call survey when a customer call is redirected by the VDN Return Destination (VRD) feature into vector processing. The agent identifier can be included in User-to-User Information (UUI) using existing vector commands before routing the call to an external IVR system. By adding the agent identifier in UUI, post-call surveys can furnish reports details down to the agent level.

Agent in this context is the agent who has disconnected from the customer session and the customer session is retained and is the VRD feature is processing the session. UUI can contain the agent identifier for only one agent. For example, in case of a call flow that has multiple transfers and multiple agents handling that customer call in a sequence then the UUI contains the agent identifier only for the last agent who spoke to the customer. In this case, the IVR/VRU system with a post-call survey application receives the agent information only for the last agent and the customer rating is for that agent.

# Vector name length increased to 27 characters and a new vdn-info button added

From Avaya Aura® Call Center Elite 7.1 onwards, vector names can have a maximum of 27 characters. Prior to Call Center Elite 7.1, vector names had a maximum of 15 characters.

Call Center Elite 7.1 also introduces a new station button, **VDN-INFO**, on Communication Manager for H.323 and DCP phones. When users press the **VDN-INFO** button, Communication Manager sends the complete VDN name for the active call in the existing display format to the phones. The VDN name displays 27 characters, which is the same number of characters that can be administered on Communication Manager. After 10 seconds, the phones display gets restored to their original display.

# Support for treating AUX work mode as idle for controlling the LOA queue

From Avaya Aura® Call Center Elite 7.1 onwards, you have the option for the Least Occupied Agent (LOA) skill queues to consider agents idle while they are in the AUX work mode.

Whenever an agent becomes available or enters the AUX work mode, the agent is queued if the **AUX Agent Remains in LOA Queue** field is set to the following parameters:

- `y` on the Agent LoginID screen.
- `system` on the Agent LoginID screen and `y` on the Feature-Related System Parameters screen.

Agent queuing also depends on the value set in the **ACW Agents Considered Idle** field. If the agent was not previously in the queue, agent queuing depends on when the agent enters the AUX work mode. In addition, occupancy of the agent remains frozen while the agent is in the AUX work mode.

# Chapter 16: Resources

## Documentation

The following table lists the documents related to the components of Avaya Aura® Release 7.1.3. Download the documents from the Avaya Support website at http://support.avaya.com.

| Document number | Title | Description | Audience |
|---|---|---|---|
| Implementation | | | |
| — | *Deploying Avaya Aura® applications from System Manager* | Describes the procedures for installation, configuration, initial administration, and basic maintenance checklist and procedures for deploying Avaya Aura® applications in Virtualized Environment by using Avaya Aura® System Manager Solution Deployment Manager. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| — | *Upgrading and Migrating Avaya Aura® applications from System Manager* | Describes the procedures and checklists for upgrading Avaya Aura® applications to Release 7.1.3. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| Administration | | | |
| 555-233-504 | *Administering Network Connectivity on Avaya Aura® Communication Manager* | Describes the network components of Communication Manager, such as gateways, trunks, FAX, modem, TTY, and Clear-Channel calls. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-300509 | *Administering Avaya Aura® Communication Manager* | Describes the procedures and screens used for administering Communication Manager. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| — | *Administering Avaya Aura® System Manager* | Describes the procedures for configuring System Manager | Solution Architects, Implementation |

*Table continues…*

| Document number | Title | Description | Audience |
|---|---|---|---|
| | | Release 7.1.3 and the Avaya Aura® applications and systems managed by System Manager. | Engineers, Sales Engineers, Support Personnel |
| — | *Avaya Aura® Presence Services Snap-in Reference* | Describes the steps to deploy and configure Presence Services. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| Using | | | |
| | *Using the Solution Deployment Manager client* | Deploy and install patches on Avaya Aura® applications. | System administrators |
| Understanding | | | |
| 555-245-205 | *Avaya Aura® Communication Manager Feature Description and Implementation* | Describes the features that you can administer using Communication Manager. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-602878 | *Avaya Aura® Communication Manager Screen Reference* | Describes the screen and detailed field descriptions of Communication Manager. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-603324 | *Administering Avaya Aura® Session Manager* | Describes how to administer Session Manager by using System Manager. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 555-245-207 | *Avaya Aura® Communication Manager Hardware Description and Reference* | Describes the hardware devices that can be incorporated in a Communication Manager telephony configuration. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| Maintenance and Troubleshooting | | | |
| 03-300431 | *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers* | Provides commands to monitor, test, and maintain hardware components of Avaya servers and gateways. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |

# Finding documents on the Avaya Support website

## Procedure

1. Navigate to http://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 an appropriate release number.
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 displays the documents only from the selected category.
7. Click **Enter**.

# Downloading documents from the Support website

## About this task

To download the latest version of Avaya documents from the Support website, perform the following steps:

## Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. At the top of the Avaya Support homepage, click the **Documents** tab.
3. In the **Enter Your Product Here** field, type the product name for which you want to download the documents. Once you start typing the product name, the website displays the results matching to the entered text. You can select the complete product name from the displayed list.
4. In the **Choose Release** field, select **7.0.x**.
5. Click **Enter**.

   **Note:**

   To refine the search results, select a document category. You can also select multiple categories. If no category is selected, the website displays all the documents for the selected product and release.

   The website displays a list of documents for the selected product and release.
6. To open a document, click the document title.

# 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 |
|---|---|
| Avaya Aura® core implementation | |
| 1A00234E | Avaya Aura® Fundamental Technology |
| 4U00040E | Avaya Aura® Session Manager and System Manager Implementation |
| 4U00030E | Avaya Aura® Communication Manager and Communication Manager Messaging Implementation |
| 10U00030E | Avaya Aura® Application Enablement Services Implementation |
| 8U00170E | Avaya Aura® Presence Services Implement and Support |
| AVA00838H00 | Avaya Aura® Media Server and Media Gateways Implementation Workshop |
| ATC00838VEN | Avaya Aura® Media Server and Gateways Implementation Workshop Labs |
| Avaya Aura® core support | |
| 5U00050E | Session Manager and System Manager Support |
| 5U00060E | ACSS - Avaya Aura® Communication Manager and CM Messaging Support |
| 4U00115I<br>4U00115V | Avaya Aura® Communication Manager Implementation Upgrade (R5.x to R6.x) |
| 1A00236E | Avaya Aura® Session Manager and System Manager Fundamentals |
| 2008W | What is New in Avaya Aura® Application Enablement Services 7.0 |
| 2008T | What is New in Avaya Aura® Application Enablement Services 7.0 Online Test |
| 2009W | What is New in Avaya Aura® Communication Manager 7 |
| 2009T | What is New in Avaya Aura® Communication Manager 7.0 Online Test |
| 2010W | What is New in Avaya Aura® Presence Services 7.0 |
| 2010T | What is New in Avaya Aura® Presence Services 7.0 Online Test |
| 2011W | What is New in Avaya Aura® Session Manager and Avaya Aura® System Manager 7.0 |
| 2011T | What is New in Avaya Aura® Session Manager and Avaya Aura® System Manager 7.0 Online Test |
| 2013V | Avaya Aura® 7 Administration |
| Avaya Aura® core administration and maintenance | |
| 9U00160E | Avaya Aura® Session Manager for System Administrators |
| 1A00236E | Avaya Aura® Session Manager and Avaya Aura® System Manager Fundamentals |
| 5U00051E | Avaya Aura® Communication Manager Administration |
| 5M00050A | Avaya Aura® Communication Manager Messaging Embedded Administration, Maintenance & Troubleshooting |

*Table continues…*

| Course code | Course title |
|---|---|
| 2012V | Migrating and Upgrading to Avaya Aura® 7.0 |
| 2012I | Migrating and Upgrading to Avaya Aura® 7 |
| 2017 | Avaya Aura® 7 Administration Delta |
| 2017V | Avaya Aura® 7 Administration Delta |

# 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.

### Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

**Note:**

Videos are not available for all products.

# Support

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

**Related links**

Using the Avaya InSite Knowledge Base on page 74

# 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.

**Related links**

Support on page 73

# 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 http://support.avaya.com.

   **Note:**

   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, enter 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.

   **Note:**

   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 the Avaya Support Web Tips and Troubleshooting: E-Notifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#.
2. Set up e-notifications.

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

# Index

## H



## I



## K



## L



## M



## N



## O



## P



## R



## S

## T



## U



## V



## W