Avaya Solutions Platform S8300 Release Notes

Release 5.1.x

Issue 12

September 2025

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. 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 Designated Processor that hosts 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 on a number of Designated Processors up to the number indicated in the order. 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 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 15 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).

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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.

Table of Contents

Avaya Solutions Platform S8300 Release Notes 1
Change history 8
Introduction 9
Release History 9
What's New in Avaya Solutions Platform 5.1.x 9
Avaya Solutions Platform R5.1.x to R6.0.x Configuration Migration Utility 9
Licensing Update – applicable to all new ASP 5.1.x orders 10
What's new in Avaya Solutions Platform S8300 5.1.0.7 10
What's new in Avaya Solutions Platform S8300 5.1.0.6 10
What's new in Avaya Solutions Platform S8300 5.1.0.5 10
What's new in Avaya Solutions Platform S8300 5.1.0.4 11
What's new in Avaya Solutions Platform S8300 5.1.0.3 11
What's new in Avaya Solutions Platform S8300 5.1.0.2 11
What's new in Avaya Solutions Platform S8300 5.1.0.1 11
What's new in Avaya Solutions Platform S8300 5.1 11
Supported Upgrade Paths 12
Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.7: 12
Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.6: 13
Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.5 14
Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.4 14
Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.3 14
Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.2 14
Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.1 14
Avaya Solutions Platform Appliance key features 15
Key Features 15
Installing ASP S8300 Release 5.1.x 15
New installations including recovery, remastering 15
Upgrade to ASP S8300 R5.1.0.7 (ESXi 7.0 U3w) 15
Upgrade to ASP S8300 R5.1.0.6 (ESXi 7.0 U3s) 15
Upgrade to ASP S8300 R5.1.0.5 (ESXi 7.0 U3q) 15
Upgrade to ASP S8300 R5.1.0.4 (ESXi 7.0 U3p) 15
Upgrade to ASP S8300 R5.1.0.3 (ESXi 7.0 U3o) 16
Upgrade to ASP S8300 R5.1.0.2 (ESXi 7.0 U3i) 16
Upgrade to ASP S8300 R5.1.0.1 (ESXi 7.0 U3d) 16
Migrating to ASP S8300 Release 5.1.x from AVP 16
ESXi 7.0 Licensing 16
ESXi 7.0 Datastore name 17

Avaya EASG VIB 17
ASP_SSH Script 17
Product Registration 18
Avaya Solutions Platform S8300 5.1.x Software files 18
Required artifacts for Avaya Solutions Platform Configuration Migration Utility 18
Required artifacts for Avaya Solutions Platform S8300 5.1.0.7 19
Required artifacts for Avaya Solutions Platform S8300 5.1.0.6 19
Required artifacts for Avaya Solutions Platform S8300 5.1.0.5 20
Required artifacts for Avaya Solutions Platform S8300 5.1.0.4 21
Required artifacts for Avaya Solutions Platform S8300 5.1.0.3 22
Required artifacts for Avaya Solutions Platform S8300 5.1.0.2 23
Required artifacts for Avaya Solutions Platform S8300 5.1.0.1 24
Required artifacts for Avaya Solutions Platform S8300 5.1 25
Security Information 25
Security Statement 25
Fixes in Avaya Solutions Platform 5.1.x 26
Fixes in release 5.1.0.7 26
Fixes in release 5.1.0.6 26
Fixes in release 5.1.0.5 26
Fixes in release 5.1.0.4 27
Fixes in release 5.1.0.3 27
Fixes in Release 5.1.0.2 28
Fixes in Release 5.1.0.1 28
Fixes in Release 5.1 29
Known issues and workarounds in 5.1.x 29
Known issues and workarounds in Release 5.1.0.7 29
Known issues and workarounds in Release 5.1.0.6 30
Known issues and workarounds in Release 5.1.0.5 30
Known issues and workarounds in Release 5.1.0.4 31
Known issues and workarounds in Release 5.1.0.3 31
Known issues and workarounds in Release 5.1.0.2 31
Known issues and workarounds in Release 5.1.0.1 32
Known issues and workarounds in Release 5.1. 32
Resources 33
Documentation 33
Support 34
Subscribing to e-notifications 34

Change history

Issue	Date	Description
1	14-Mar-2022	Release Notes for Avaya Solutions Platform S8300 Release 5.1.
2	9-May-2022	Updates to the What's New section.
3	10-Jun-22	Updates to the Known issues section.
4	5-Dec-22	Updated OOBM script to asp_oobm_v1.sh Release Notes for Avaya Solutions Platform S8300 5.1.0.1
5	16-Jan-23	Release Notes for Avaya Solutions Platform S8300 5.1.0.2. Table added for supported upgrade paths.
5.1	18-Jan-23	Clarification on upgrade-asp-S8300 script in What's New section.
6	19-Dec-23	Release Notes for Avaya Solutions Platform S8300 5.1.0.3. Added Release History Section
7	29-Apr-24	Release Notes for Avaya Solutions Platform S8300 5.1.0.4
8	1-Aug-24	*What's New* section updated to reflect unique license key label on HDD/SDD for all new ASP 5.1.x S8300 orders, target cutover early-mid August 2024, subject to change. License key will no longer be posted in PLDS for all new orders.
9	19-Aug-24	Release Notes for Avaya Solutions Platform S8300 5.1.0.5
10	21-Mar-25	Release Notes for Avaya Solutions Platform S8300 5.1.0.6
11	26-Aug-25	Release Notes for Avaya Solutions Platform S8300 5.1.0.7
12	30-Sept-25	• Updated ACP1XX-1334 updated to remove inaccurate statement about a QUALYS false positive for CVE-2024-37085. This specific CVE was never addressed in ESXi 7.0. This CVE is not applicable to ASP 130/S8300 as Active Directory integration is not supported. • Updated for ASP R5.1.x to R6.0.x Configuration Migration Utility

Introduction

This document provides release notes, important notices, and describes known issues for the Avaya Solutions Platform S8300 5.1.x solution. The ASP S8300 solution was first introduced with ASP R5.1. There was no previous version of ASP S8300. This document is intended for users of Avaya Solutions Platform S8300 and those interested in obtaining information about this solution. This audience can include:

- System Administrators
- Data Center Personnel
- Avaya Sales Engineers
- Avaya Systems Engineers
- Certified Repair and Maintenance Personnel

Note: Please reference *Policies for technical support of the Avaya Solutions Platform (ASP) 130 R4.x, R5.x and S8300 R5.1*. This document identifies VMware native features and those that are not supported by Avaya for the ASP 130 and S8300 R5.1 hosts, and where the demarcation points for technical support responsibility lie if issues were to arise.

Release History

ASP S8300 Release	Date Launched	VMware build
ASP S8300 5.1.0.7	August 26, 2025	ESXi 7.0 Update 3w build 24784741
ASP S8300 5.1.0.6	March 21, 2025	ESXi 7.0 Update 3s build 24585291– *express patch update only applicable to ASP S8300 R5.1.0.5.*
ASP S8300 5.1.0.5	August 19, 2024	ESXi 7.0 Update 3q build 23794027
ASP S8300 5.1.0.4	April 29, 2024	ESXi 7.0 Update 3p build 23307199
ASP S8300 5.1.0.3	December 19, 2023	ESXI 7.0 Update 3o build 22348816
ASP S8300 5.1.0.2	January 16, 2023	ESXi 7.0 Update 3i build 20842708
ASP S8300 5.1.0.1	December 5, 2022	ESXi 7.0 Update 3d build 19482537
ASP S8300 5.1	March 14, 2022	ESXi 7.0 Update 2d build 18538813

What's New in Avaya Solutions Platform 5.1.x

Avaya Solutions Platform R5.1.x to R6.0.x Configuration Migration Utility

Avaya introduces an ***Avaya Solutions Platform R5.1.x to R6.0.x Configuration Migration Utility***.

Migrations are catastrophic. Several steps are required prior to a catastrophic migration, including backing up host and application-level data. The migration utilities facilitate the migration of host-level parameters and include export and import functionality. They are provided in a zip file on PLDS and will need to be extracted to the individual components. PLDS requires a unique PLDS ID if the same file is located under multiple Releases/Versions, therefore there will be unique PLDS IDs for each release within ASP S8300 and ASP 130. The zip file (*asp_migration_utility-v1.zip*) will extract to the following python scripts:

host_config_export_v1.py

host_config_import_v1.py

Reference PCN2146Su and the *Application Note for ASP R5.1.x to ASP R6.0.x Configuration Migration Utility* for detailed instructions

Licensing Update – applicable to all new ASP 5.1.x orders

These notes will be updated when the cutover date is finalized; target cutover is tentatively scheduled for early-mid August, 2024, subject to change. Ensure you are signed up for e-notification.

Due to changes in our third-party vendor agreement, all NEW orders for ASP 5.1.x will no longer have the ESXi license key posted in PLDS. A unique foundations license key will be provided on a label on the ASP S8300 HDD/SSD. In the event of an S8300E replacement, the unique license code on the ASP S8300 HDD/SSD will need to be removed and placed on the replacement S8300E. If it is not possible to remove the label, care must be taken to record the unique license key for use on the replacement S8300E and for future use in the event the ASP S8300E would need to have ESXi reinstalled. Existing ASP S8300 servers with a license obtained from PLDS are **not** impacted by this change, only new orders shipped from Avaya's Integrator and warehouses. Existing inventory that was previously sold to Distributors and Partners and is present in their supply chain, will still have the old key. Only when they replenish stock with new orders, post the cutover, will the change take place.

What's new in Avaya Solutions Platform S8300 5.1.0.7

ASP S8300 Release 5.1.0.7 (Avaya customized ESXi 7.0 U3w Build# 24784741) addresses the following VMSAs:

VMSA	VMSA Severity	Associated CVEs
VMSA-2025-0013	Critical	CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, CVE-2025-41239
VMSA-2025-0010	Important	CVE-2025-41225, CVE-2025-41226, CVE-2025-41227, CVE-2025-41228

Note: ASP 130 Release 5.1.0.7 includes all updates from the 5.1.0.6 express patch and is therefore cumulative.

What's new in Avaya Solutions Platform S8300 5.1.0.6

- ASP S8300 Release 5.1.0.6 (Avaya customized ESXi 7.0 U3s Build# 24585291) addresses the critical VMSA-2025-0004 vulnerability and its associated CVEs (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226). **This update is based on an express patch from VMware/Broadcom and therefore is NOT cumulative. It must only be applied to ASP R5.1.0.5**.

  NOTE: *Avaya is providing this immediate, vendor-provided response to VMSA-2025-004 to permit customers who are bound by governmental regulations to mitigate within certain timeframes. Avaya will, in parallel, run their regular qualification activities and will provide an update as to whether the earlier update can stand, or if there are updates to software or to process and documentation.*

- As noted in PCN2145S, Avaya and VMware by Broadcom have agreed that the fix in VMware's December 12, 2024 release of ESXi 7.0 U3r (build number 24411414) is not applicable to ASP 130 or ASP S8300 as it is specific to the vMotion feature which is not supported on ASP 130/S8300. When the system is updated to ASP R5.1.0.6, it will not include the fix in 7.0 U3r as the express patch 7.0 U3s is not cumulative.

What's new in Avaya Solutions Platform S8300 5.1.0.5

- ASP S8300 Release 5.1.0.5 will go GA with VMware ESXi 7.0 U3q build 23794027.

- Updated Avaya Tools VIB to v1.6-3

What's new in Avaya Solutions Platform S8300 5.1.0.4

- ASP S8300 Release 5.1.0.4 will go GA with VMware ESXi 7.0 U3p build 23307199.
- Updated Avaya Tools VIB to v1.5-3
- Updated *aspupdate.sh* script included in zip file (*upgrade-asp-s8300-5.1.0.3.0-05.zip)* for upgrades from earlier ASP S8300 5.x releases to 5.1.0.3. Note: The migration from AVP deployed on S8300 to the latest ASP S8300 R5.1.x is a multi-step process.
- Updated EASG VIB to v1.1-7. Version 1.1-7 replaces all earlier versions of the customized EASG VIB on 5.1.x and is compatible with all ASP S8300 5.1.x.x.

What's new in Avaya Solutions Platform S8300 5.1.0.3

- ASP S8300 Release 5.1.0.3 will go GA with VMware ESXi 7.0 U3o build 22348816.
- Updated Avaya Tools VIB v1.4-3.
- New **asp_oobm_v3.sh** Out of Band Management (OOBM) script.
- Updated *aspupdate.sh* script included in zip file (*upgrade-asp-s8300-5.1.0.3.0-05.zip)* for upgrades from earlier ASP S8300 5.x releases to 5.1.0.3. Note: The migration from AVP deployed on S8300 to the latest ASP S8300 R5.1.x is a multi-step process.
- Avaya Aura® Release 10.2 which went GA on December 18, 2023 is supported on Avaya Solutions Platform (ASP) S8300 Release 5.1.x and ASP 130 Release 5.0 and Release 5.1.x.

What's new in Avaya Solutions Platform S8300 5.1.0.2

- ASP S8300 Release 5.1.0.2 will go GA with VMware ESXi 7.0 U3i build 20842708
- Updated OOBM (Out of Band Management) script for ASP S8300 to *asp_oobm_v2.sh*.
- Updated *aspupdate.sh* script included in zip file for upgrades from earlier ASP S8300 5.x releases to 5.1.0.3, *upgrade-asp-s8300-5.1.0.2.0-04.zip.* Note: The migration from AVP deployed on S8300 to the latest ASP S8300 R5.1.x is a multi-step process.

What's new in Avaya Solutions Platform S8300 5.1.0.1

- ASP S8300 Release 5.1.0.1 will go GA with VMware ESXi 7.0 U3d build 194825374
- Updated OOBM script for ASP S8300 to *asp_oobm_v1.sh*.
- Script included in zip file for upgrades from ASP S8300 5.1 release to 5.1.0.1, *upgrade-asp-s8300-5.1.0.1.0-08.zip.* Note: The migration from AVP deployed on S8300 to the latest ASP S8300 R5.1.x is a multi-step process.

What's new in Avaya Solutions Platform S8300 5.1

- Avaya Aura® Release 10.1 is supported on Avaya Solutions Platform (ASP) S8300 Release 5.1.x and ASP 130 Release 5.0 and Release 5.1.x.

  NOTE: Avaya Aura® Release 8.1.3.x is supported on ASP S8300 5.1.x.
  However, after migrating from Avaya Aura® Appliance Virtualization Platform (AVP) Release 8.1.x on an S8300E to ASP S8300 Release 5.1, Avaya Aura® Release 8.1.x applications are still running on ASP S8300 Release 5.1.
  Prolonged running in this type of mixed configuration is not supported. Avaya recommends running in a mixed configuration only as long as necessary to support application upgrades. If an issue is identified on an Avaya Aura® 8.1.x application running on ASP S8300 Release 5.1 Avaya will require an upgrade of the Avaya Aura® solution to Release 10.1.
  All future ASP 5.x security updates will only be provided on the latest ASP Release 5.x release currently available. For example, if ASP Release 5.1 is the most recent available release, security updates will only be provided on Release 5.1. They will not be provided on Release 5.0.

- With the introduction of ASP 5.x and Avaya Aura® 10.1, AVP/AVPU goes end of sale. Last supported AVP/AVPU release is Avaya Aura® 8.1.3.x. AVP and AVPU are not supported with Avaya Aura® 10.1.
- EASG is supported starting with ASP Release 5.1
- A new 5.1 directory ("/opt/avaya/etc/") is created with both the ASP S8300 zip upgrade file and the ASP S8300 ISO install file. The Avaya Tools VIB will create this directory.
- The ASP S8300 Release 5.1 has the Avaya Tools VIB, which replaces the functionality of Avaya-Config-v1 script file in the ASP 130 Release 4.0 and Release 5.0
    - In ASP 130 Release 4.0 and Release 5.0, the Avaya-Config-v1 script file configured the services port and had to be copied to the shell and manually applied.
    - In ASP Release 5.1, this is no longer necessary. The Avaya Tools VIB is part of the ASP S8300 5.1 ISO and zip files
- The ASP S8300 Release 5.1.x ISO for fresh install, recovery or catastrophic/forklift migrations includes the Avaya Tools VIB.
    - The Avaya EASG VIB must be downloaded separately from PLDS, copied to the shell, and manually applied after the ISO is installed.
- The ASP S8300 Release 5.1.x upgrade zip file contains the Avaya Tools VIB and the Avaya EASG VIB, thus no need to download the Avaya EASG VIB from PLDS..
    - The ASP S8300 Release 5.1.x zip file is used for upgrades only.
- From ASP Release 5.1 onwards, in the change autostart configuration window, "start delay" and "stop delay" fields are set to '0'.
- New shipments of the ASP S8300 R5.1.x servers will initially ship blank and will need to have the R5.1.x software installed and the license key installed. At a future date, new shipments will be preloaded with R5.1.x and prelicensed. Installers should always verify the ASP S8300 is at the latest posted certified version on PLDS and if necessary upgrade to the latest posted release.

Supported Upgrade Paths

Important Notes:

- It is imperative that customers stay current with the latest Avaya certified ESXi release to ensure a robust security environment. After ASP R5.1.0.4, **Avaya will only be testing upgrade paths from N-2 releases**. **With exceptions for R5.1.0.6 which requires the server to be on R5.1.0.5 prior to updating to R5.1.0.6.**
  With the release of R5.1.0.5, the supported upgrade paths are from 5.1.0.3 and 5.1.0.4.
  With the release of R5.1.0.6, the only supported upgrade path is from 5.1.0.5.
- The migration from AVP deployed on S8300 to the latest ASP S8300 R5.1.x is a multi-step process. It is necessary to first migrate from AVP 8.1.x on S8300E to ASP S8300 R5.1, then upgrade from ASP S8300 R5.1 to R5.1.x.x. Reference Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300.
- Unless otherwise stated by Avaya, DO NOT change the default Port Group labels for virtual machine traffic and ESXi management services traffic that are created during the ESXi installation as this may impact integration with other Avaya applications and scripts.

Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.7:

From ASP S8300 Release	To ASP S8300 R5.1.0.7
R4.0	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.0	Not supported *multi-step process* *MUST update to R5.1.0.5 first*

R5.1	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.1.0.1	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.1.0.2	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.1.0.3	Not supported *multi-step process* *MUST update to R5.1.0.5*
R5.1.0.4	Not supported *multi-step process* *MUST update to R5.1.0.5*
R5.1.0.5	Supported
R5.1.0.6	Supported

Avaya Customers that have not kept current with new releases must conduct a multi-step upgrade to R5.1.0.5 first before upgrading to R5.1.0.7.

Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.6:

From ASP S8300 Release	To ASP S8300 R5.1.0.6
R4.0	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.0	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.1	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.1.0.1	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.1.0.2	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.1.0.3	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.1.0.4	Not supported *multi-step process* *MUST update to R5.1.0.5 first*
R5.1.0.5	Supported

Avaya Customers that have not kept current with new releases must conduct a multi-step upgrade to R5.1.0.5 first before upgrading to R5.1.0.6.

Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.5

From ASP S8300 Release	To ASP S8300 R5.1.0.5
R5.1	**Not Supported** *multi-step process*
R5.1.0.1	**Not Supported** *multi-step process*
R5.1.0.2	**Not Supported** *multi-step process*
R5.1.0.3	**Supported**
R5.1.0.4	**Supported**

Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.4

From ASP S8300 Release	To ASP S8300 R5.1.0.4
R5.1	**Supported**
R5.1.0.1	**Supported**
R5.1.0.2	**Supported**
R5.1.0.3	**Supported**

Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.3

From ASP S8300 Release	To ASP S8300 R5.1.0.3
R5.1	**Supported**
R5.1.0.1	**Supported**
R5.1.0.2	**Supported**

Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.2

From ASP S8300 Release	To ASP S8300 R5.1.0.2
R5.1	**Supported**
R5.1.0.1	**Supported**

Supported upgrade paths to Avaya Solutions Platform S8300 5.1.0.1

From ASP S8300 Release	To ASP S8300 R5.1.0.1
R5.1	**Supported**

Avaya Solutions Platform Appliance key features

Key Features

The Avaya S8300 is the underlying server hardware used for the Avaya Solutions Platform S8300 solution. The S8300E is Avaya's current generation embedded server for Avaya's portfolio of applications. The design is done by a third party ODM supplier with Avaya development oversight. S8300 server series are plugged directly into a G430 or G450 Gateway and provide a platform for running software applications in a small form factor blade server.

Installing ASP S8300 Release 5.1.x

New installations including recovery, remastering

Refer to *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300* for detailed procedures.

Upgrade to ASP S8300 R5.1.0.7 (ESXi 7.0 U3w)

The ASP S8300 5.1.0.7 release is launching with the Avaya Dell customized VMware ESXi 7.0 Update 3w build 24784741 for install on the ASP S8300 R640 servers. Customers can upgrade their ASP S8300 Solution to ESXi 7.0 U3w using the Avaya Dell customized ESXi offline bundle zip file available on PLDS. This zip file can be used to upgrade ASP S8300 R5.1.0.5 or R5.1.0.6 ESXi hosts to ASP S8300 R5.1.0.7. Customers that are on R4.0 (ESXi 6.5 – must be on latest release Build #19092475) or R5.0 (ESXi 7.0U2) or R5.1.x < R5.1.0.3 or R5.1.0.4 must conduct a step-up upgrade to R5.1.0.5 first before upgrading to R5.1.0.7.

Upgrade to ASP S8300 R5.1.0.6 (ESXi 7.0 U3s)

The ASP S8300 5.1.0.6 release is launching with the Avaya Dell customized VMware ESXi 7.0 Update 3q build 23794027 ZIP file for install on the ASP S8300 R640 R5.1.0.5 servers. **This update is based on an express patch from VMware/Broadcom and therefore is NOT cumulative. It must only be applied to ASP R5.1.0.5**. While the version number will now reference ESXi 7.0 U3s Build# 24585291, it is NOT a complete image and only will address the VMSA-2025-0004 vulnerability and only for ASP 130 R5.1.0.5 and ASP S8300 R5.1.0.5. It is not supported on any other release of ASP R5.1.x. Customers on releases earlier than ASP R5.1.0.5 must first update to R5.1.0.5 and then update to R5.1.0.6. There is no associated ISO image released since this update is not a complete image.

Upgrade to ASP S8300 R5.1.0.5 (ESXi 7.0 U3q)

The ASP S8300 5.1.0.5 release is launching with the Avaya customized VMware ESXi 7.0 Update 3q build 23794027 for install on the ASP S8300 servers. Customer can upgrade their ASP S8300 Solution to ESXi 7.0 U3q using the Avaya customized ESXi offline bundle zip file available on PLDS. This zip file can be used to upgrade ASP S8300 R5.1.0.3 or R5.1.04 hosts to ASP 130 R5.1.0.5. Customers that are on 5.1.x < R5.1.0.3 or R5.1.0.4 must conduct a step-up upgrade to R5.1.0.3 or R 5.1.0.4 first before upgrading to R5.1.0.5

Refer to ASP S8300 PCN2145 for the latest software (including PLDS Download IDs). Detailed instructions for Upgrades can be found in the *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300* guide.

Upgrade to ASP S8300 R5.1.0.4 (ESXi 7.0 U3p)

The ASP S8300 5.1.0.4 release is launching with the Avaya customized VMware ESXi 7.0 Update 3p build 23307199 for install on the ASP S8300 servers. Customer can upgrade their ASP S8300 Solution to ESXi 7.0 U3p using the Avaya customized ESXi offline bundle zip file available on PLDS. This zip file can be used to upgrade ASP S8300 ESXi host from 7.0.x builds to ESXi 7.0 U3p.

Refer to ASP S8300 PCN2145 for the latest software (including PLDS Download IDs). Detailed instructions for Upgrades can be found in the *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300* guide.

Upgrade to ASP S8300 R5.1.0.3 (ESXi 7.0 U3o)

The ASP S8300 5.1.0.3 release is launching with the Avaya customized VMware ESXi 7.0 Update 3o build 22348816 for install on the ASP S8300 servers. Customer can upgrade their ASP S8300 Solution to ESXi 7.0 U3o using the Avaya customized ESXi offline bundle zip file available on PLDS. This zip file can be used to upgrade ASP S8300 ESXi host from 7.0.x builds to ESXi 7.0 U3o.

Refer to ASP S8300 PCN2145 for the latest software (including PLDS Download IDs). Detailed instructions for Upgrades can be found in the *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300* guide.

Upgrade to ASP S8300 R5.1.0.2 (ESXi 7.0 U3i)

The ASP S8300 5.1.0.2 release is launching with the Avaya customized VMware ESXi 7.0 Update 3i build **20842708** for install on the ASP S8300 servers. Customer can upgrade their ASP S8300 Solution to ESXi 7.0 U3i using the Avaya customized ESXi offline bundle zip file available on PLDS. This zip file can be used to upgrade ASP S8300 ESXi host from 7.0.x builds to ESXi 7.0 U3o.

Refer to ASP S8300 PCN2145 for the latest software (including PLDS Download IDs). Detailed instructions for Upgrades can be found in the *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300* guide.

Upgrade to ASP S8300 R5.1.0.1 (ESXi 7.0 U3d)

The ASP S8300 5.1.0.1 release is launching with the Avaya customized VMware ESXi 7.0 Update 3d build 19482537 for install on the ASP S8300 servers. Customer can upgrade their ASP S8300 Solution to ESXi 7.0 U3d using the Avaya customized ESXi offline bundle zip file available on PLDS. This zip file can be used to upgrade ASP S8300 ESXi host from 7.0.x builds to ESXi 7.0 U3o.

Refer to ASP S8300 PCN2145 for the latest software (including PLDS Download IDs). Detailed instructions for Upgrades that were previously in the PCN are not incorporated in the *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300* guide.

Migrating to ASP S8300 Release 5.1.x from AVP

AVP 8.1.x deployed on S8300E migrations to ASP S8300 require that the same application with the same profile is used for the migration. If the end customer needs to increase profile size or add a new application, this will need to take place post migration and will need to be based on available resources as determined by the A1S Configurator. If the final ASP S8300 release is 5.1.x.x it will be a 2 step process to migrate from AVP to ASP. First migrate to ASP S8300 R5.1, then upgrade from ASP S8300 R5.1. to R5.1.x.x.

A detailed procedure on migration from AVP 8.1.x to ASP S8300 Release 5.1.x can be found in - ***Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300***.

ESXi 7.0 Licensing

NOTE: Licensing Update – applicable to all new ASP 5.1.x orders, target cutover is tentatively scheduled for early-mid August, 2024, subject to change.

Due to changes in our third-party vendor agreement, all NEW orders for ASP 5.1.x will no longer have the ESXi license key posted in PLDS. A unique standard license key will be provided on a label on the ASP 130 server lid. In the event of a server replacement, the server lid with the ESXi license key must be

moved to the new replacement server. Existing ASP 130 servers with a license obtained from PLDS are ***not*** *impacted by this change, only new orders shipped from Avaya's Integrator and warehouses. Existing inventory that was previously sold to Distributors and Partners and is present in their supply chain, will still have the old key. Only when they replenish stock with new orders, post the cutover, will the change take place.*

S8300 uses a Foundation level of ESXi licensing.

New shipments of the ASP S8300 R5.1 servers initially shipped blank and will need to have the R5.1.x software installed and the license key installed. ASP S8300 R5.1 begins shipping from Avaya's integrator preloaded and pre-licensed in October 2022. Installers should always verify the ASP S8300 is at the latest posted certified version on PLDS. A license key per each ASP S8300 host is required.

For those who are migrating from AVP to ESXi 7.0, or are doing a recovery/re-install, they will be able to get both the software and the license via PLDS once their account is "entitled".

ESXi 7.0 Datastore name

When AVP 8.1.x deployed on S8300E is migrated to ASP S8300 R5.1, the persistent storage directory name will always remain as "server-local-disk". For ASP S8300Es shipping preloaded from Avaya's integrator, the persistent storage directory name will always be "datastore1". Installing ASP S8300 R5.1.x on a blank S8300E or remastering an existing ASP S8300 R5.x (even if it migrated from AVP) will always result in a persistent storage name of "datastore1". Upgrades withing the ASP S8300 R5.1.0.x release will maintain the existing persistent storage directory name.

/vmfs/volumes/server-local-disk/

/vmfs/volumes/datastore1

Avaya EASG VIB

The Avaya EASG VIB is run to provide Avaya support and technicians with access to the ASP S8300 server for maintenance and troubleshooting activities.

Refer *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300* for instructions on how to install Avaya EASG VIB.

Note:

Avaya Solutions Platform S8300 5.1 systems that are preloaded and pre-licensed coming from Avaya's integrator will already have the Avaya EASG VIB installed and will not require execution of this VIB. Server recovery (FRU) and software remastering to release 5.1.x will require the VIB to be copied to the ESXi shell and executed as noted in the *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300 document.*

ASP_SSH Script

ASP_SSH is a script which can be used to enable SSH for troubleshooting purpose in case SSH has been disabled by customer for security reasons.

On running this script administrator will get a window of 2 hours and SSH will automatically be disabled after that.

To use this script one should login to one of the VMs (CM, AES, SM, SMGR, AEP, SAL, ADS, SBC, AADS) installed on the ASP host and run following command:

ASP_SSH enable

The script can only be executed by root user or privileged user for respective application.

After the script is successfully run wait for 3 minutes before trying to SSH to ASP.

NOTE:

- By default the SSH is enabled on ASP.

- In case ASP_SSH is run by mistake on a setup which had SSH enabled while installation/ migration; the script will override the timeout value and SSH will then be disabled after 2 hours window.

Product Registration

In order to receive support from Avaya Services, Avaya Customers and Avaya Channel Partners must have their end user product information in the **HealthCheck** tool.

End User product install base is a prerequisite for services support of Avaya Solutions Platform. Registration establishes accurate inventory, test SAL connectivity, alarm configuration (if necessary) and ensures proper on-boarding of customer into all levels of Avaya Support.

General information on registration can be found at https://support.avaya.com/registration

The Heathcheck tool can be accessed at: https://secureservices.avaya.com/osm-phs/views/home.xhtml?null

Avaya Solutions Platform S8300 5.1.x Software files

The following sections provides the Avaya Solutions Platform S8300 release 5.1.x downloading information. For deployment and upgrade procedures, see *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300*, *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300* and PCN2145 on the Avaya Support website.

Required artifacts for Avaya Solutions Platform Configuration Migration Utility

Download ID	Description/File name	Description
ASP000000118	ASP S8300 R5.1.x.Migration Utility v1 ZIP File *asp_migration_utility-v1.zip*	ASP Migration Utility v1 to be used when performing migrations from ASP R5.1.x (ESXi 7.0) to ASP R6.x (KVM on RHEL 8.10).

Required artifacts for Avaya Solutions Platform S8300 5.1.0.7

Download ID	Description/File name	Description
ASP000000116	ASP S8300 5.1.0.7 Customized ESXi 7.0 U3w Build#24784741 ISO File *asp-s8300-5.1.0.7.0-01.iso*	Customized ESXi 7.0 U3w build 24784741 ISO image used for fresh installs on ASP S8300 servers. ISO image is burnt to CD/DVD disk for field technician.
ASP000000117	ASP S8300 5.1.0.7 Customized ESXi 7.0 U3w Build#24784741 ZIP File *upgrade-asp-s8300-5.1.0.7.0-01.zip*	Customized ESXi 7.0 U3w build 24784741 file used for upgrades
ASP000000112	ASP S8300 Customized EASG VIB *AVA-avaya-easg_1.1-7_23348963.zip*	Avaya EASG VIB; installation is only required if a fresh ESXi installation is conducted on the ASP S8300 servers. **Version 1.1-7 replaces all earlier versions** of the customized EASG VIB on 5.1.x and is compatible with all ASP S8300 5.1.x.x. *Same file as was used with previous release.*
ASP000000103	ASP S8300 OOBM Configuration script *asp_oobm_v3.sh*	This is an Avaya script that facilitates the configuration of Out of Band Management (OOBM) on the ASP S8300 5.1.x servers. This is ONLY applicable to ASP S8300 servers and ASP 130 servers. **This v3 script replaces any existing OOBM scripts.** *Same file as was used with previous release.*

Required artifacts for Avaya Solutions Platform S8300 5.1.0.6

Download ID	Description/File name	Description
ASP000000115	ASP S8300 5.1.0.6 Customized ESXi 7.0 U3s Build#24585291 ZIP File *upgrade-asp-s8300-5.1.0.6.0-01.zip*	VMware ESXi 7.0 U3s build 24585291 ZIP file used for upgrades from R5.1.0.5 to R5.1.0.6 only. **This update is based on an express patch from VMware/Broadcom and therefore is NOT cumulative. It must only be applied to ASP R5.1.0.5**.

Required artifacts for Avaya Solutions Platform S8300 5.1.0.5

Download ID	Description/File name	Description
ASP000000113	ASP S8300 5.1.0.5 Customized ESXi 7.0 U3q Build#23794027 ISO File *asp-s8300-5.1.0.5.0-01.iso*	Customized ESXi 7.0 U3q build 23794027 ISO image used for fresh installs on ASP S8300 servers. ISO image is burnt to CD/DVD disk for field technician.
ASP000000114	ASP S8300 5.1.0.5 Customized ESXi 7.0 U3q Build#23794027 ZIP File *upgrade-asp-s8300-5.1.0.5.0-01.zip*	Customized ESXi 7.0 U3q build 23794027 file used for upgrades
ASP000000112	ASP S8300 Customized EASG VIB *AVA-avaya-easg_1.1-7_23348963.zip*	Avaya EASG VIB; installation is only required if a fresh ESXi installation is conducted on the ASP S8300 servers. **Version 1.1-7 replaces all earlier versions** of the customized EASG VIB on 5.1.x and is compatible with all ASP S8300 5.1.x.x. *Same file as was used with R5.1.0.4.*
ASP000000103	ASP S8300 OOBM Configuration script *asp_oobm_v3.sh*	This is an Avaya script that facilitates the configuration of Out of Band Management (OOBM) on the ASP S8300 5.1.x servers. This is ONLY applicable to ASP S8300 servers and ASP 130 servers. **This v3 script replaces any existing OOBM scripts.** *Same file as was used with R5.1.0.4.*

Required artifacts for Avaya Solutions Platform S8300 5.1.0.4

Download ID	Description/File name	Description
ASP000000110	ASP S8300 5.1.0.4 Customized ESXi 7.0 U3p Build#23307199 ISO File *asp-s8300-5.1.0.4.0-02.iso*	Customized ESXi 7.0 U3p build 23307199 ISO image used for fresh installs on ASP S8300 servers. ISO image is burnt to CD/DVD disk for field technician.
ASP000000111	ASP S8300 5.1.0.4 Customized ESXi 7.0 U3p Build#23307199 ZIP File *upgrade-asp-s8300-5.1.0.4.0-02.zip*	Customized ESXi 7.0 U3p build 23307199 file used for upgrades
ASP000000112	ASP S8300 Customized EASG VIB *AVA-avaya-easg_1.1-7_23348963.zip*	Avaya EASG VIB; installation is only required if a fresh ESXi installation is conducted on the ASP S8300 servers. **Version 1.1-7 replaces all earlier versions** of the customized EASG VIB on 5.1.x and is compatible with all ASP S8300 5.1.x.x.
ASP000000103	ASP S8300 OOBM Configuration script *asp_oobm_v3.sh*	This is an Avaya script that facilitates the configuration of Out of Band Management (OOBM) on the ASP S8300 5.1.x servers. This is ONLY applicable to ASP S8300 servers and ASP 130 servers. **This v3 script replaces any existing OOBM scripts.** PLDS ID remains the same.

Required artifacts for Avaya Solutions Platform S8300 5.1.0.3

Download ID	Description/File name	Description
ASP000000108	ASP S8300 5.1.0.3 Customized ESXi 7.0 U3o Build#22348816 ISO File *asp-s8300-5.1.0.3.0-05.iso*	Customized ESXi 7.0 U3o build 22348816 ISO image used for fresh installs on ASP S8300 servers. ISO image is burnt to CD/DVD disk for field technician.
ASP000000109	ASP S8300 5.1.0.3 Customized ESXi 7.0 U3o Build#22348816 ZIP File *upgrade-asp-s8300-5.1.0.3.0-05.zip*	Customized ESXi 7.0 U3o build 22348816 file used for upgrades
ASP000000102	ASP S8300 Customized EASG VIB *AVA-avaya-easg_1.0-2_19246618.zip* *No change from ASP S8300 5.1, 5.1.0.1, 5.1.0.2*	Avaya EASG VIB; installation is only required if a fresh ESXi installation is conducted on the ASP S8300 servers
ASP000000103	ASP S8300 OOBM Configuration script *asp_oobm_v3.sh*	This is an Avaya script that facilitates the configuration of Out of Band Management (OOBM) on the ASP S8300 5.1.x servers. This is ONLY applicable to ASP S8300 servers and ASP 130 servers. **This v3 script replaces any existing OOBM scripts.** PLDS ID remains the same.

Required artifacts for Avaya Solutions Platform S8300 5.1.0.2

Download ID	Description/File name	Description
ASP000000106	ASP S8300 5.1.0.2 Customized ESXi 7.0 U3i Build#20842708 ISO File *asp-s8300-5.1.0.2.0-04.iso*	Customized ESXi 7.0 U3i build 20842708 ISO image used for fresh installs on ASP S8300 servers. ISO image is burnt to CD/DVD disk for field technician.
ASP000000105	ASP S8300 5.1.0.2 Customized ESXi 7.0 U3di Build#20842708 ZIP File *upgrade-asp-s8300-5.1.01.0-04.zip*	Customized ESXi 7.0 U3d build 19482537 file used for upgrades
ASP000000102	ASP S8300 Customized EASG VIB *AVA-avaya-easg_1.0-2_19246618.zip* *No change from ASP S8300 5.1, 5.1.0.1*	Avaya EASG VIB; installation is only required if a fresh ESXi installation is conducted on the ASP S8300 servers
ASP000000103	ASP S8300 OOBM Configuration script *asp_oobm_v2.sh*	Script to configure the Out of Band Management connection on the ASP S8300 R5.1.x servers.. Updated script *asp_oobm_v2.sh* is now available and replaces previous *asp_oobm_v1.sh.* PLDS ID remains the same. This is ONLY applicable to ASP S8300 servers and ASP 130 5.1.x servers.

Required artifacts for Avaya Solutions Platform S8300 5.1.0.1

Download ID	Description/File name	Description
ASP000000104	ASP S8300 5.1.0.1 Customized ESXi 7.0 U3d Build#19482537 ISO File *asp-s8300-5.1.0.1.0-08.iso*	Customized ESXi 7.0 U3d build 19482537 ISO image used for fresh installs on ASP S8300 servers. ISO image is burnt to CD/DVD disk for field technician.
ASP000000105	ASP S8300 5.1.0.1 Customized ESXi 7.0 U3d Build#19482537 ZIP File *upgrade-asp-s8300-5.1.01.0-08.zip*	Customized ESXi 7.0 U3d build 19482537 file used for upgrades
ASP000000102	ASP S8300 Customized EASG VIB *AVA-avaya-easg_1.0-2_19246618.zip* *No change from ASP S8300 5.1*	Avaya EASG VIB; installation is only required if a fresh ESXi installation is conducted on the ASP S8300 servers
ASP000000103	ASP S8300 OOBM Configuration script *asp_oobm_v1.sh*	Script to configure the Out of Band Management connection on the ASP S8300 R5.1.x servers.. Updated script *asp_oobm_v1.sh* is now available and replaces original *asp_oobm.sh.* PLDS ID remains the same. This is ONLY applicable to ASP S8300 servers and ASP 130 5.1.x servers.

Required artifacts for Avaya Solutions Platform S8300 5.1

Download ID	Description/File name	Description
ASP000000100	ASP S8300 Customized ESXi 7.0 U2d Build#18538813 ISO File *asp-s8300-5.1.09.iso*	Customized ESXi 7.0 U2d build 18538813 ISO image used for fresh installs on ASP S8300 servers. ISO image is burnt to CD/DVD disk for field technician.
ASP000000101	ASP S8300 Customized ESXi 7.0 U2d Build#18538813 zip File *upgrade-asp-s8300-5.1.09.zip*	Customized ESXi 7.0 U2d build 18538813 file used for upgrades
ASP000000102	ASP S8300 Customized EASG VIB *AVA-avaya-easg_1.0-2_19246618.zip*	Avaya EASG VIB; installation is only required if a fresh ESXi installation is conducted on the ASP S8300 servers
ASP000000103	ASP S8300 OOBM Configuration script *asp_oobm_v1.sh*	Script to configure the Out of Band Management connection on the ASP S8300 R5.1 servers.. Updated script *asp_oobm_v1.sh* is now available and replaces original *asp_oobm.sh.* PLDS ID remains the same. This is ONLY applicable to ASP S8300 servers and ASP 130 5.1 servers.

Note: Only Avaya provided updates can be used. Updating directly from the VMware's web sites will result in an unsupported configuration.

Security Information

Security Statement

Avaya Solutions Platform is a solution compromised of hardware and software products. Security vulnerabilities for each product is tracked individually by the product development team. There are also third party products that are part of the Avaya Solutions Platform solution. The security vulnerabilities of those products are the responsibility of their product development teams.

Avaya uses an industry standard security scanning tool to conduct internal security compliance scans on GA candidate software prior to releasing it to the public. Avaya mitigates Critical, High and Medium vulnerabilities discovered and generated in the scan report whether these are **confirmed** or **potential**. Best effort is applied on Low vulnerabilities whether these are confirmed or potential.

It is important to remember that ESXi is not built upon the Linux kernel or a commodity Linux distribution. It uses its own VMware specialized and proprietary kernel and software tools, delivered as a self-contained unit, and does not contain applications and components from Linux distributions.

Confirmed Vulnerabilities

Vulnerability scans often report as high or critical vulnerabilities that are related to the SSL Certificate installed on the ESXi Host. By default, VMware ESXi during the hypervisor installation generates and installs on the Host Web server an SSL self-signed certificate. Broadcom/VMware Vendor as well as Avaya, as a best practice, strongly recommends replacing SSL self-signed certificates with a certificate

that has been signed by a third-party, trusted, reputable, **Certificate Authority** (CA). Certificates that have been signed by an internal, corporate CA such as a Windows server or Avaya System Manager, may still be considered not secure by the scanner and therefore SSL Certificate related vulnerabilities may still continue to be flagged.

Reference the ***Replacing ESXi SSL certificates and Keys with Custom Certificates*** section in the Installing the Avaya Solutions Platform 130 series Document for replacing SSL certificates on ESXi as vulnerabilities which are related to SSL certificates must be mitigated in the field by the Customer or Partner.

Qualys QIDs related to load balance device detected can be safely disregard as they are not applicable to ESXi.

Potential Vulnerabilities

Potential vulnerabilities are not confirmed until the security administrator goes thru the report in detail and confirms whether the system is susceptible or not. Often, vulnerability scanners flag a potential vulnerability just by the component version in question e.g. OS version, OpenSSH version running on ESXi. Also, scanners sometime are not capable of determining if a workaround provided by the vendor has been applied or not, thus, vulnerabilities may still be reported under the potential vulnerabilities section (scanner detection logic).

Fixes in Avaya Solutions Platform 5.1.x

Fixes in release 5.1.0.7

Note: Reference VMware ESXi 7.0 U3v Release Notes and VMware ESXi 7.0 U3w Release Notes for additional information.

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ACP1XX-1954	ESXi 7.0U3s or earlier	Security Vulnerability VMSA-2025-0013 CVE-2025-41236 CVE-2025-41237 CVE-2025-41238 CVE-2025-41239	5.1, 5.1.0.1, 5.1.0.2, 5.1.0.3, 5.1.0.4 5.1.0.5 5.1.0.6
ACP1XX-1973	ESXi 7.0U3s or earlier	Security Vulnerability VMSA-2025-0010 CVE-2025-41225 CVE-2025-41226 CVE-2025-41227 CVE-2025-41228	5.1, 5.1.0.1, 5.1.0.2, 5.1.0.3, 5.1.0.4 5.1.0.5 5.1.0.6

Fixes in release 5.1.0.6

Note: Reference VMware ESXi 7.0 U3s Release Notes for additional information.

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ACP1XX-1185 ACP1XX-1890	ESXi 7.0U3q or earlier	Security Vulnerability VMSA-2025-0004 CVE-2025-22224 CVE-2025-22225 CVE-2025-22226	5.1, 5.1.0.1, 5.1.0.2, 5.1.0.3, 5.1.0.4 5.1.0.5

Fixes in release 5.1.0.5

Note: Reference VMware ESXi 7.0 U3q Release Notes for additional information.

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ACP1XX-1184	ESXi 7.0U3p or earlier	Security Vulnerability VMSA-2024-0011 CVE-2024-22273 CVE-2024-22274 – *N/A for ESXi* CVE-2024-22275 – *N/A for ESXi*	5.1, 5.1.0.1, 5.1.0.2, 5.1.0.3, 5.1.0.4
ACP1XX-1334	ESXi 7.0U3p or earlier	Security Vulnerability VMSA-2024-0013 **CVE-2024-37085** –*was **NOT** delivered into VMSA-2024-0013.* ***N/A for ASP 130/S8300 as AD integration is not supported.*** *QUALYS scans will set CVE-2024-37085 as practice (Potential vulnerability) as QID 216333 does not check if a workaround is implemented.* **CVE-2024-37086** – *Confirmed with Broadcom that this is included even though not mentioned specifically in the 7.0U3q release notes.* **CVE-2024-37087** – *N/A for ESXi*	5.1, 5.1.0.1, 5.1.0.2, 5.1.0.3, 5.1.0.4

See the **Security Information** section of these Release Notes for additional information related to **Confirmed** and **Potential** vulnerabilities.

Fixes in release 5.1.0.4

Note: Reference VMware ESXi 7.0 U3p Release Notes for additional information.

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ACP1XX-1095	ESXi 7.0U3o or earlier	Security vulnerability VMSA-2024-0006 (CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255) found in security scan results	5.1, 5.1.0.1, 5.1.0.2, 5.1.0.3
ACP1XX-1077	ESXi 7.0U3o or earlier	ESXi Shell Service is not getting enabled through deployment. Updated Avaya Tools VIB 1.5-3 resolves this issue.	5.1, 5.1.0.1, 5.1.0.2, 5.1.0.3
ACP1XX-704	EASG VIB on ESXi 7.0 U3o or earlier	Special characters not supported. Updated Avaya EASG VIB 1.1-7 resolves this issue.	5.1, 5.1.0.1, 5.1.0.2, 5.1.0.3

NOTE: Avaya has conducted internal vulnerability scans against ESXi 7.0U3p and the following **potential** vulnerabilities have been flagged: CVE-2023-51767, CVE-2023-38408, CVE-2023-51385, CVE-2021-36368.

Avaya opened **SR 24511285704** with the Broadcom/VMware vendor for a confirmation if these potential vulnerabilities are applicable or not to ESXi. Vendor completed their evaluation stating that the reported CVEs are not applicable to the ESXi product. ESXi is not susceptible to CVEs: CVE-2023-51767, CVE-2023-38408, CVE-2023-51385, CVE-2021-36368.

See the **Security Information** section of these Release Notes for additional information related to **Confirmed** and **Potential** vulnerabilities.

Fixes in release 5.1.0.3

Note: Reference VMware ESXi 7.0 U3o Release Notes for additional information.

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ACP1XX-847, ACP1XX-882	Any web browser used to access the ESXi UI.	AutoComplete Attribute Not Disabled for Password in Form Based Authentication. Security vulnerability found in security scan results. Qualys QID 86729.	5.0, 5.1, 5.1.0.1, 5.1.0.2
ACP1XX-1031	Avaya Tools v1.1-2, v1.3-1	Support for special characters in the local datastore name.	5.1, 5.1.0.1, 5.1.0.2

The following specific Security updates were delivered in ESXi 7.0 U3o:

- The cURL library is updated to version 8.1.2.
- The ESXi userworld libxml2 library is updated to version 2.10.4.
- The SQLite library is updated to version 3.42.0.
- The OpenSSL package is updated to version 1.0.2zh.

Note that many of these are not applicable to the ASP environment, thus Avaya only calls out the fixes/updates in the latest Avaya certified release that may have an impact on an ASP solution.

Fixes in Release 5.1.0.2

Note: Reference VMware ESXi 7.0 U3i Release Notes for additional information.

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ACP1XX-563	ESXi 7.0 u3d	Security vulnerability VMSA-2022-0020 (CVE-2022-29901, CVE-2022-28693, CVE-2022-23816, CVE-2022-23825, CVE-2022-26373) found in security scan results	5.1.0.1
ACP1XX-564	ESXi 7.0 u3d	Security vulnerability VMSA-2022-0025 (CVE-2022-31680, CVE-2022-31681) found in security scan results	5.1.0.1
ACP1XX-558	ESXi 7.0 u3d	Security vulnerability VMSA-2022-0016 (CVE-2022-21123, CVE-2022-21125, CVE-2022-21166) found in security scan results	5.1.0.1
N/A	ESXi 7.0 u3d	Security vulnerability VMSA-2022-0030 (CVE-2022-31696, CVE-2022-31699)	5.1.0.1

Fixes in Release 5.1.0.1

Note: Reference VMware ESXi 7.0 U3d Release Notes for additional information.

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ACP1XX-351	ESXi 7.0 u2d	Reconfigure event reported every 3 minutes on VMware console	5.1
ACP1XX-370	ESXi 7.0 u2d	When resetting the system from the gateway using “reset mm v1” command, S8300 stops responding and just shuts down	5.1

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ACP1XX-328	ESXi 7.0 u2d	Security vulnerability VMSA-2022-0004 (CVE-2021-22040, CVE-2021-22041, CVE-2021-22042, CVE-2021-22043, CVE-2021-22050) found in security scan results.	5.1
ACP1XX-325	ESXi 7.0 u2d	Security vulnerability VMSA-2022-0001 (CVE-2021-22045) found in security scan results.	5.1
SMGR-68473	SMGR 10.1.0.0	Platform Type is now changed from ASP 130 to ASP 130/S8300 when using SMGR SDM or SDM Client	SMGR 10.1.0.0 *Resolved in SMGR 10.1.0.2*

Fixes in Release 5.1

Note: Reference VMware ESXi 7.0 U2d Release Notes for additional information. As 5.1 is the first release, there are no specific fixes.

ID	Minimum Conditions	Visible symptoms	Issue found in Release
NA	NA	NA	NA

Known issues and workarounds in 5.1.x

Best practice is to always utilize the latest SDM Client 10.1 or 10.2 release. If utilizing earlier clients, the following PSN will apply:

Use of Solution Deployment Manager (SDM) with ASP S8300 R5.1 REQUIRES an updated SDM Client as noted in *PSN005569u – New Solution Deployment Manager Client for 10.1.0.0 release*

If utilizing SMGR SDM release < 10.1.0.1, the following PSN will apply:

Use of Avaya Aura® System Manager (SMGR) Solution Deployment Manager (SDM) 10.1.0.0 with ASP S8300 R5.1 REQUIRES the latest SMGR 10.1.0.0 Hot Fix as noted in *PSN005568u - System Manager 10.1.0.0 Hot Fix 1.*

Known issues and workarounds in Release 5.1.0.7

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-1332	ASP 5.1.x	CVE-2024-6387 flagged on Qualys scan	VMware does not have any plans currently to upgrade OpenSSH for this OpenSSH signal handler race condition vulnerability. They stated the risk is low as it is only relevant for 32 bit, not 64 bit. ESXi 7.x versions of OpenSSH are 64-bit and the exploit has not been encountered there. If Customers want to disable SSH, they need to understand that Avaya will need SSH enabled to perform any troubleshooting or remote support on the system. Aura applications do contain ASP_SSH script that can be executed and run from the application to enable SSH for a short window. It will automatically disable after 2 hours, or the Avaya engineer can execute the script again with the “disable” option once the troubleshooting is completed. ASP currently ships with SSH enabled as it is required for installation/configuration.

			Release Notes for reference https://support.avaya.com/css/public/documents/101081340
ACP1XX-1334	ESXi 7.0U3s or earlier	CVE-2024-37085 flagged on Qualys scan	CVE-2024-37085 – ***N/A for ASP 130/S8300 as AD integration is not supported.*** *QUALYS scans will set CVE-2024-37085 as practice (Potential vulnerability) as QID 216333 does not check if a workaround is implemented.* This CVE was **NOT** delivered into VMSA-2024-0013

Known issues and workarounds in Release 5.1.0.6

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-1332	ASP 5.1.x	CVE-2024-6387 flagged on Qualys scan	VMware does not have any plans currently to upgrade OpenSSH for this OpenSSH signal handler race condition vulnerability. They stated the risk is low as it is only relevant for 32 bit, not 64 bit. ESXi 7.x versions of OpenSSH are 64-bit and the exploit has not been encountered there. If Customers want to disable SSH, they need to understand that Avaya will need SSH enabled to perform any troubleshooting or remote support on the system. Aura applications do contain ASP_SSH script that can be executed and run from the application to enable SSH for a short window. It will automatically disable after 2 hours, or the Avaya engineer can execute the script again with the "disable" option once the troubleshooting is completed. ASP currently ships with SSH enabled as it is required for installation/configuration. Release Notes for reference https://support.avaya.com/css/public/documents/101081340
ACP1XX-1334	ESXi 7.0U3s or earlier	CVE-2024-37085 flagged on Qualys scan	CVE-2024-37085 – ***N/A for ASP 130/S8300 as AD integration is not supported.*** *QUALYS scans will set CVE-2024-37085 as practice (Potential vulnerability) as QID 216333 does not check if a workaround is implemented.* This CVE was **NOT** delivered into VMSA-2024-0013

Known issues and workarounds in Release 5.1.0.5

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-1332	ASP 5.1.x	CVE-2024-6387 flagged on Qualys scan	VMware does not have any plans currently to upgrade OpenSSH for this OpenSSH signal handler race condition vulnerability. They stated the risk is low as it is only relevant for 32 bit, not 64 bit. ESXi 7.x versions of OpenSSH are 64-bit and the exploit has not been encountered there. If Customers want to disable SSH, they need to understand that Avaya will need SSH enabled to perform any troubleshooting or remote support on the system. Aura applications do contain ASP_SSH script that can be executed and run from the application to enable SSH for a short window. It will automatically disable after 2 hours, or the Avaya engineer can execute the script again with the "disable" option once the troubleshooting is completed.

			ASP currently ships with SSH enabled as it is required for installation/configuration. Release Notes for reference https://support.avaya.com/css/public/documents/101081340
ACP1XX-1334	ESXi 7.0U3s or earlier	CVE-2024-37085 flagged on Qualys scan	CVE-2024-37085 – ***N/A for ASP 130/S8300 as AD integration is not supported.*** *QUALYS scans will set CVE-2024-37085 as practice (Potential vulnerability) as QID 216333 does not check if a workaround is implemented.* This CVE was **NOT** delivered into VMSA-2024-0013

Known issues and workarounds in Release 5.1.0.4

Best practice is to always utilize the latest SDM Client 10.1 or 10.2 release. If utilizing earlier clients, the following PSN will apply:

Use of Solution Deployment Manager (SDM) with ASP S8300 R5.1 **REQUIRES** an updated SDM Client as noted in *PSN005569u – New Solution Deployment Manager Client for 10.1.0.0 release*

If utilizing SMGR SDM release < 10.1.0.1, the following PSN will apply:

Use of Avaya Aura® System Manager (SMGR) Solution Deployment Manager (SDM) 10.1.0.0 with ASP S8300 R5.1 **REQUIRES** the latest SMGR 10.1.0.0 Hot Fix as noted in *PSN005568u - System Manager 10.1.0.0 Hot Fix 1.*

Known issues and workarounds in Release 5.1.0.3

Best practice is to always utilize the latest SDM Client 10.1 release. If utilizing earlier clients, the following PSN will apply:

Use of Solution Deployment Manager (SDM) with ASP S8300 R5.1 **REQUIRES** an updated SDM Client as noted in *PSN005569u – New Solution Deployment Manager Client for 10.1.0.0 release*

If utilizing SMGR SDM release < 10.1.0.1, the following PSN will apply:

Use of Avaya Aura® System Manager (SMGR) Solution Deployment Manager (SDM) 10.1.0.0 with ASP S8300 R5.1 **REQUIRES** the latest SMGR 10.1.0.0 Hot Fix as noted in *PSN005568u - System Manager 10.1.0.0 Hot Fix 1.*

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-704	ASP 5.1.x	Special characters in the datastore name can cause EASG install script to fail.	Do not use special characters for datastore names.

Known issues and workarounds in Release 5.1.0.2

Best practice is to always utilize the latest SDM Client 10.1 release. If utilizing earlier clients, the following PSN will apply:

Use of Solution Deployment Manager (SDM) with ASP S8300 R5.1 **REQUIRES** an updated SDM Client as noted in *PSN005569u – New Solution Deployment Manager Client for 10.1.0.0 release*

If utilizing SMGR SDM release < 10.1.0.1, the following PSN will apply:

Use of Avaya Aura® System Manager (SMGR) Solution Deployment Manager (SDM) 10.1.0.0 with ASP S8300 R5.1 **REQUIRES** the latest SMGR 10.1.0.0 Hot Fix as noted in *PSN005568u - System Manager 10.1.0.0 Hot Fix 1.*

ID	Minimum conditions	Visible symptoms	Workaround

ACP1XX-847	Any web browser used to access the ESXi UI.	AutoComplete Attribute Not Disabled for Password in Form Based Authentication. Security vulnerability found in security scan results. Qualys QID 86729.	Turn off autocomplete through the web browsers. See the following link for instructions to disable autocomplete/autofill for each major web browser. https://support.iclasspro.com/hc/en-us/articles/218569268-How-Do-I-Disable-or-Clear-AutoFill-AutoComplete-Information-

Known issues and workarounds in Release 5.1.0.1

Best practice is to always utilize the latest SDM Client 10.1 release. If utilizing earlier clients, the following PSN will apply:

> Use of Solution Deployment Manager (SDM) with ASP S8300 R5.1 **REQUIRES** an updated SDM Client as noted in *PSN005569u – New Solution Deployment Manager Client for 10.1.0.0 release*

If utilizing SMGR SDM release < 10.1.0.1, the following PSN will apply:

> Use of Avaya Aura® System Manager (SMGR) Solution Deployment Manager (SDM) 10.1.0.0 with ASP S8300 R5.1 **REQUIRES** the latest SMGR 10.1.0.0 Hot Fix as noted in *PSN005568u - System Manager 10.1.0.0 Hot Fix 1.*

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-558	ESXi 7.0 u3d, u2d	Security vulnerability VMSA-2022-0016 (CVE-2022-21123, CVE-2022-21125, CVE-2022-21166) found in security scan results.	None per VMware. Will be resolved in a future release of ASP S8300 5.1.0.x
ACP1XX-563	ESXi 7.0 u3d, u2d	Security vulnerability VMSA-2022-0020 (CVE-2022-29901, CVE-2022-28693, CVE-2022-23816, CVE-2022-23825, CVE-2022-26373) found in security scan results	None per VMware. Will be resolved in a future release of ASP S8300 5.1.0.x
ACP1XX-564	ESXi 7.0 u3d, u2d	Security vulnerability VMSA-2022-0025 (CVE-2022-31680, CVE-2022-31681) found in security scan results.	None per VMware. Will be resolved in a future release of ASP S8300 5.1.0.x

Known issues and workarounds in Release 5.1.

Use of Avaya Aura® System Manager (SMGR) Solution Deployment Manager (SDM) with ASP S8300 R5.1 **REQUIRES** the latest SMGR 10.1.0.0 Hot Fix as noted in *PSN005568u - System Manager 10.1.0.0 Hot Fix 1.*

Use of Solution Deployment Manager (SDM) with ASP S8300 R5.1 **REQUIRES** an updated SDM Client as noted in *PSN005569u – New Solution Deployment Manager Client for 10.1.0.0 release.*

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-370	ESXi 7.0 u2d	When resetting the system from the gateway using "reset mm v1" command, S8300 stops responding and just shuts down	There are 2 workarounds available for this: 1. Reseat of S8300 card (this will need person to be physically present onsite). 2. From gateway CLI run command "reset chassis". Please Note: this will reset all the cards present on the gateway, hence will be service impacting.
SMGR-68597	Migrating CM and BSM on ASP S8300	All profiles for CM and BSM are visible in the drop down list	Select only below mentioned profile: • *For Communication Manager (LSP): CM Main Max User 1000' and 'CM Survivable Max User 1000'* • *For Branch Session Manager: 'BSM Profile 1 Max Devices 1,000'.*
SMGR-68472	Regeneration of certificate	Offer type column of ASP S8300 host is changed to "Customer VE" unexpectedly and the Platform type column of ASP S8300 host doesn't display any information.	Remove the ASP host from SDM and re-add ASP host keeping host type as "ASP130"
SMGR-68310	Kickstart file generation *for ASP S8300 5.1 installation.*	*User cannot enter FQDN in the hostname field*	Use hostname for kickstart file generation
SMGR-68309	Add host in SDM with wrong host type	Host is added without any error in the SMGR SDM	N/A

Resources

Documentation

Title	Description
Migrating from Appliance Virtualization Platform deployed on S8300 Server to Solutions Platform S8300	Describes checklists and procedures for migrating Appliance Virtualization Platform Release 8.1.x deployed on S8300E Server to Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1.x.

Installing, Maintaining and Troubleshooting the Avaya Solutions Platform S8300	Describes procedures to maintain and troubleshoot Avaya Solutions Platform S8300.
Policies for technical support of the Avaya Solutions Platform (ASP) 130 R4.x, R5.x and S8300 R5.1.x	Describes the support of the software and hardware based on supported and tested configurations. Identifies features that are not supported and the demarcation points for technical support responsibility.
Avaya Solutions Platform S8300 Port Matrix – S8300E	This document provides a list of interfaces, TCP and UDP ports that hardware components and applications use for intra-connections and for interconnections with external applications or devices.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge base articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request (SR). 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.

Subscribing to e-notifications

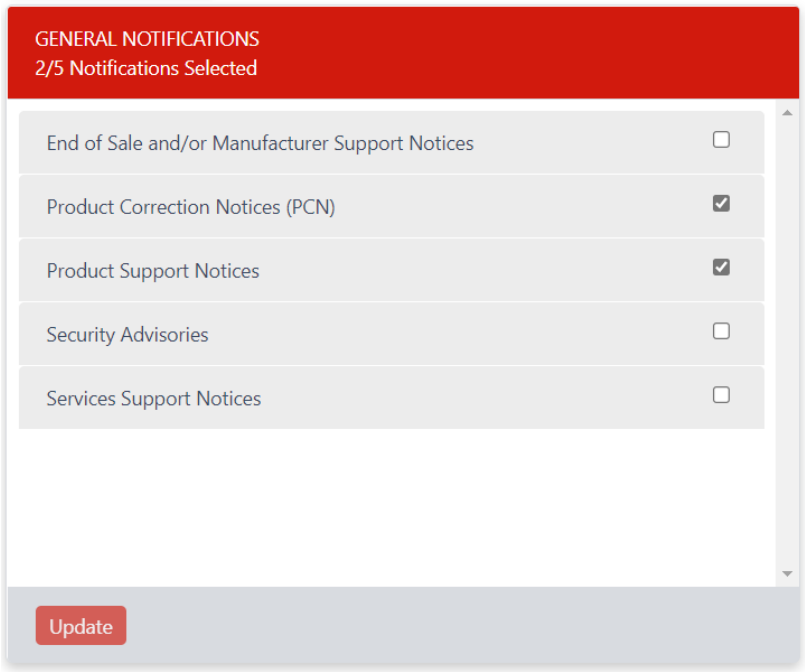
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Product Support Notices for Avaya Solutions Platform.

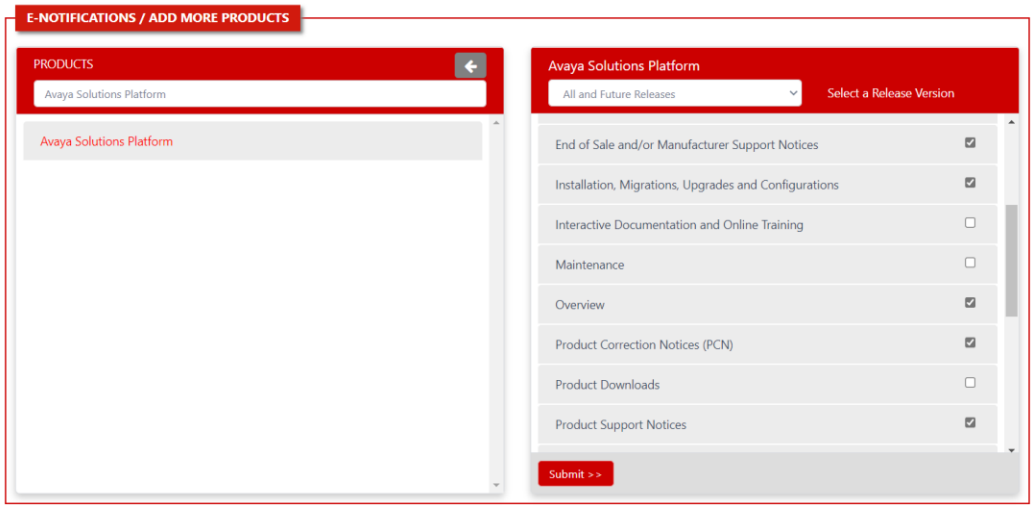
Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Account (your login name in upper right of screen)** , select My **SSO Profile**.
4. Under **User Profile**, select **E-Notification**.
5. In the **General Notification** area, select the required documentation types and then click **Update**.



6. It is displayed that the General notification has been updated successfully.
7. In the Product notifications area, click **Add More Products**.

8. Scroll through the list, and then select the product name.
9. Select the release version.
10. Select the check box next to the required documentation types.



11. Click **Submit**.