Avaya Solutions Platform 130 Release Notes

Release 5.1.x
Issue 11
March 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 LLC, ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA

AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA LLC OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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.

Shrink-wrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrink-wrap" 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 15https://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 LLC

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.

Contents

Change history

Issue	Date	Description
1	12-April-2022	Release notes for Avaya Solutions Platform 130 Release 5.1
2	10-May-2022	Updates to the What's New section
3	July-2022	Out Of Band Management (OOBM) support
4	5-Dec-22	Release Notes for Avaya Solutions Platform 130 5.1.0.1
5	16-Jan-23	Release Notes for Avaya Solutions Platform 130 5.1.0.2. Updated upgrade sections to reflect requirements for ASP 130 R4.0 to 5.1.0.x. Table added for supported upgrade paths.
6	6-Sep-23	Upgrade path table updated with an important note in regards SNMPv3 and deprecated authentication protocols no longer supported when **upgrading from ESXi 6.5.x to 7.0.x.**
7	19-Dec-23	Release Notes for Avaya Solutions Platform 130 5.1.0.3. Added Release History section
8	29-Apr-2024	Release Notes for Avaya Solutions Platform 130 5.1.0.4
9	1-Aug-24	*What's New* section updated to reflect unique license key label on server lid for all new ASP 5.1.x 130 orders, target cutover early-mid August, 2024. License key will no longer be posted in PLDS for all new orders.
10	19-Aug-24	Release Notes for Avaya Solutions Platform 130 5.1.0.5
11	21-Mar-25	Release Notes for Avaya Solutions Platform 130 5.1.0.6

Introduction

This document provides release notes, important notices, and describes known issues for the Avaya Solutions Platform (ASP) 130 5.1.x solution. This document is intended for users of Avaya Solutions Platform 130 and those interested in obtaining information about the solutions. 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 130 Release	Date Launched	VMware build
ASP 130 5.1.0.6	March 21, 2025	ESXi 7.0 Update 3s build 24585291 – *express patch update only applicable to ASP 130 R5.1.0.5.*
ASP 130 5.1.0.5	August 19, 2024	ESXi 7.0 Update 3q build 23794027
ASP 130 5.1.0.4	April 29, 2024	ESXi 7.0 Update 3p build 23307199
ASP 130 5.1.0.3	December 19, 2023	ESXI 7.0 Update 3o build 22348816
ASP 130 5.1.0.2	January 16, 2023	ESXi 7.0 Update 3i build 20842708
ASP 130 5.1.0.1	December 5, 2022	ESXi 7.0 Update 3d build 19482537
ASP 130 5.1	April 12, 2022	ESXi 7.0 Update 3c build 19193900

What's New in Avaya Solutions Platform 130 5.1.x

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 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.

What's new in Avaya Solutions Platform 130 5.1.0.6

- ASP 130 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 PCN2146S, 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 130 5.1.0.5

- ASP 130 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 130 5.1.0.4

- ASP 130 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 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 130 5.1.x.x.
- Beginning with ASP 130 5.1.0.4, the ESXi shell is enabled when deploying the ISO.

What's new in Avaya Solutions Platform 130 5.1.0.3

- ASP 130 Release 5.1.0.3 will go GA with VMware ESXi 7.0 U3o build 22348816.
- Updated Avaya Tools VIB to v1.4-3.
- New **asp_oobm_v3.sh** Out of Band Management (OOBM) script. For a complete feature description and how to implement OOBM in ASP 130 servers reference ***Securing Network Configuration on ASP 130*** in the Installing the Avaya Solutions Platform 130 Series document available in the Avaya support web site.
- 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 130 5.1.0.2

- ASP 130 Release 5.1.0.2 will go GA with VMware ESXi 7.0 U3i build 20842708.
- New **asp_oobm_v2.sh** Out of Band Management (OOBM) script. For a complete feature description and how to implement OOBM in ASP 130 servers reference ***Securing Network Configuration on ASP 130*** in the Installing the Avaya Solutions Platform 130 Series document available in the Avaya support web site.

What's new in Avaya Solutions Platform 130 5.1.0.1

- ASP 130 Release 5.1.0.1 will go GA with VMware ESXi 7.0 U3d build 19482537.
- Starting with ASP 130 Release 5.1.0.1, Dell's PowerEdge RAID Controller Command Line Interface (Perccli) Utility is included in the ISO and zip files.
- Due to supply chain issues, the ASP 130 will begin to ship with an H750 RAID Controller Adapter in place of the H730P Mini RAID Controller, and also the 4x1GbE Intel NIC daughter card (NDC) will be replaced by a 4x1GbE Broadcom NIC daughter card. These changes occur in 4QCY2022.

What's new in Avaya Solutions Platform 130 5.1

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

  Note: Avaya Aura® Release 8.1.3.x is supported on ASP 130 Release 5.0 and Release 5.1. 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.

- ASP 130 Release 5.1 will go GA with VMware ESXi 7.0 U3c
- With the introduction of Avaya Solutions Platform 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.
- ASP 120 Upgrade option to ASP 130 Release 5.1. This option allows you to stage the ESXi upgrade and the Application Virtual Machines that reside on your host.
- Avaya EASG is supported starting with Avaya Solutions Platform Release 5.1
- A new 5.1 directory ("`/opt/avaya/etc/`") is created with both the ESXi 7.0 zip upgrade file and the ESXi 7.0 ISO install file. The Avaya tools VIB will create this directory.
- The ASP 130 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 the 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 130 5.1 ISO and zip files.
- The ASP 130 Release 5.1 ISO for fresh install, recovery or catastrophic/forklift migrations includes the Avaya Tools VIB.
  - The EASG VIB must be downloaded separately from PLDS, copied to the shell, and manually applied after the ISO is installed.
- The ASP Release 5.1 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 130 Release 5.1 zip file is used for upgrades only.
- From ASP Release 5.1 onwards, **Autostart** is enabled and the **Autostart start delay** and **stop delay** fields are set to **0**.
- Out of Band Management (OOBM) is now supported. For a complete feature description and how to implement OOBM in ASP 130 servers reference to ***Chapter 7: Securing Network Configuration on ASP 130*** in the Installing the Avaya Solutions Platform 130 Series document available in the Avaya support web site.

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 ASP 120 (AVP) to the latest ASP 130 R5.1.X is a ***multi-step process***. It

is necessary to first migrate from **AVP 8.1.X to ASP 130 R5.1** and then upgrade to the latest ASP 130 R5.1.X. Refer to Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130.

- The migration from ASP 130 R4.0 to ASP 130 R5.1.0.3 and later is a ***multi-step process***. It is necessary to ensure ASP 130 4.0 is on the latest available Avaya approved/certified ESXi 6.5 U3 Build #19092475 prior to updating to ASP 130 5.1.0, 5.1.0.1 or 5.1.0.2. Upgrades to 5.1.0.3 and 5.1.0.4 are then possible after this first upgrade to earlier 5.1.x. Upgrades to 5.1.0.6 require the server to be on 5.1.0.5.
- 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.
- The MD5 authentication protocol is no longer supported starting with ESXi 7.0.x and later releases. Customers with ASP130 Compute servers running ESXi 6.5.x (R4.x) upgrading to ESXi 7.0.x (R5.x), with SNMPv3 configured using MD5 as the authentication protocol, must change it from MD5 to SHA1 prior to conducting the upgrade.

  Warning: Failure to update the deprecated authentication protocol in the SNMPv3 configuration will generate a PSOD (Purple Screen Of Death), the ESXi upgrade process will fail and Host will roll-back to the previous ESXi load.

Supported upgrade paths to Avaya Solutions Platform 130 5.1.0.6:

From ASP 130 Release	To ASP 130 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*
R5.1.0.4	Not supported *multi-step process* *MUST update to R5.1.0.5*
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 130 5.1.0.5:

From ASP 130	To ASP 130 R5.1.0.5

Release	
R4.0	Not supported *multi-step process*
R5.0	Not supported *multi-step process*
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

Avaya Customers that have not kept current with new releases must conduct a step-up upgrade to R5.1.0.3 or R5.1.0.4 first before upgrading to R5.1.0.5.

Supported upgrade paths to Avaya Solutions Platform 130 5.1.0.4:

From ASP 130 Release	To ASP 130 R5.1.0.4
R4.0	Not supported *multi-step process*
R5.0	Not supported *multi-step process*
R5.1	Supported
R5.1.0.1	Supported
R5.1.0.2	Supported
R5.1.0.3	Supported

Customers that are on R4.0 or R5.0 must conduct a step-up upgrade to R5.1, R5.1.0.1 or R5.1.0.2 first before upgrading to R5.1.0.4.

Supported upgrade paths to Avaya Solutions Platform 130 5.1.0.3:

From ASP 130 Release	To ASP 130 R5.1.0.3
R4.0	Not supported *multi-step process*
R5.0	Not supported *multi-step process*
R5.1	Supported
R5.1.0.1	Supported
R5.1.0.2	Supported

Customers that are on R4.0 or R5.0 must conduct a step-up upgrade to R5.1, R5.1.0.1 or R5.1.0.2 first before upgrading to R5.1.0.3.

Supported upgrade paths to Avaya Solutions Platform 130 5.1.0.2:

From ASP 130 Release	To ASP 130 R5.1.0.2	Direct Upgrade
R4.0	Supported	Supported from ESXi 6.5 U3 Build 19092475 **ONLY**
R5.0	Supported	Supported
R5.1	Supported	Supported
R5.1.0.1	Supported	Supported

Supported upgrade paths to Avaya Solutions Platform 130 5.1.0.1:

From ASP 130 Release	To ASP 130 R5.1.0.1	Direct Upgrade
R4.0	Supported	Supported from ESXi 6.5 U3 Build 19092475 **ONLY**
R5.0	Supported	Supported
R5.1	Supported	Supported

Avaya Solutions Platform Appliance key features and profiles

Key Features

The Avaya Dell PowerEdge R640 is the underlying server hardware used for the Avaya Solutions Platform 100 series. The PowerEdge R640 is a 1U single/dual socket CPU platform designed for Avaya's portfolio of applications. The R640 updates the CPU(s) and other server technologies over previous Avaya Common Server releases. It is used as the base platform for all new Avaya offers. The architecture of the R640 is designed to maximize performance and provide flexibility to optimize Avaya's applications and customer use cases.

Server Profiles

In the Avaya Solutions Platform 100 Series, server constructs are shared among Avaya Solutions Platform 110 Appliance, Avaya Solutions Platform 120 Appliance, and Avaya Solutions Platform 130 Appliance. The first table below designates ASP 100 Series servers and Intel Skylake CPU's. Those CPUs are no longer shipping in ASP 100 Series servers and have been upgraded to Intel Cascade Lake CPUs as designated in the second table below. Both CPU types are supported in 5.x and 4.0 releases. Base Server type (CPU type) must be known when using the Avaya One Source (A1S) Configurator tool prior to any application upgrade. Hardware configurations for each profile are locked. The addition of memory, storage, or changing out the NICs is not permitted and results in an unsupported configuration.

Table 1: Skylake CPUs

Appliance Constructs	Profile #2	Profile #3	Profile #4	Profile #5	Profile #51 (ASP 130 Only)
Rack Mount Unit (RMU)	1U	1U	1U	1U	1U
Intel Skylake CPU	S-4114	S-4114	G-6132	G-6132	G-6132
Number of CPUs	1	2	1	2	2
Number of Cores/Server	10	20	14	28	28
Core Frequency (GHz)	2.2	2.2	2.6	2.6	2.6
Number of 8GB RDIMMs	3	6	-	-	-
Number of 16 GB RDIMMs	-	-	6	12	12
Memory/Server in GB	24	48	96	192	192
10K 2.5” SAS HDD Size GB	600	600	600	600	600
Number of HDDs 2.5” 10K SAS	3	4	4	6	8
RAID Options	5	6	6	6	6
Usable Virtual Disk Capacity	1.2 TB	1.2 TB	1.2 TB	2.4 TB	3.6 TB
Network 1 Gb ports	6	6	6	6	6
Power Supplies (750W)	2	2	2	2	2
Rail Kit	Y	Y	Y	Y	Y
DVD-ROM Drive	Y	Y	Y	Y	Y

Table 2: Cascade Lakes CPUs

Appliance Constructs	Profile #2	Profile #3	Profile #4	Profile #5	Profile #51 (ASP 130 Only)
Intel Skylake CPU	S-4210	S-4210	G-6226R	G-6226R	G-6226R
Number of CPUs	1	2	1	2	2
Number of Cores/Server	10	20	16	32	32
Core Frequency (GHz)	2.2	2.2	2.9	2.9	2.9
Number of 8GB RDIMMs	3	6	-	-	-
Number of 16 GB RDIMMs	-	-	6	12	12
Memory/Server in GB	24	48	96	192	192

10K 2.5” SAS HDD Size GB	600	600	600	600	600
Number of HDDs 2.5” 10K SAS	3	4	4	6	8
RAID Options	5	6	6	6	6
Usable Virtual Disk Capacity	1.2 TB	1.2 TB	1.2 TB	2.4 TB	3.6 TB
Network 1 Gb ports	6	6	6	6	6
Power Supplies (750W)	2	2	2	2	2
Rail Kit	Y	Y	Y	Y	Y
DVD-ROM Drive	Y	Y	Y	Y	Y

Note: ASP S8300E R5.1 went GA March 2022. The ASP S8300E supports ESXi 7.0 and is an ODM blade server specifically designed to be part of single-box solutions using the G4x0 gateways and a specific sub-set of Avaya Aura applications.

Installing/Upgrading ASP 130 Release 5.1.x

New installations including recovery, remastering

Refer to Installing the Avaya Solutions Platform 130 Series and Maintaining and Troubleshooting ASP 130 Series for detailed procedures.

Upgrade to ASP 130 R5.1.0.6 (ESXi 7.0 U3s)

The ASP 130 5.1.0.6 release is launching with the Avaya Dell customized VMware ESXi 7.0 Update 3s build 24585291ZIP file for install on the ASP 130 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 130 R5.1.0.5 (ESXi 7.0 U3q)

The ASP 130 5.1.0.5 release is launching with the Avaya Dell customized VMware ESXi 7.0 Update 3q build 23794027 for install on the ASP 130 R640 servers. Customers can upgrade their ASP 130 Solution to ESXi 7.0 U3q using the Avaya Dell customized ESXi offline bundle zip file available on PLDS. This zip file can be used to upgrade ASP 130 R5.1.0.3 or R5.1.0.4 ESXi hosts to ASP 130 R5.1.0.5. 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 R5.1.0.3 or R 5.1.0.4 first before upgrading to R5.1.0.5.

Reference to the latest Product Correction Notice (PCN) *PCN2146S* on the Avaya Support website for the latest software, licensing instructions and any further details.

Reference to the Avaya Solutions Platform 130 Series Updating to R5.1.0.5.0 (ESXi 7.0 U3q) from R5.1x. (ESXi 7.0 U3x) *or earlier versions of this document as necessary and* Installing the Avaya Solutions Platform 130 Series documents on the Avaya Support website for installation and upgrade details, and instructions.

Upgrade to ASP 130 R5.1.0.4 (ESXi 7.0 U3p)

The ASP 130 5.1.0.4 release is launching with the Avaya Dell customized VMware ESXi 7.0 Update 3p build 23307199 for install on the ASP 130 R640 servers. Customers can upgrade their ASP 130 Solution to ESXi 7.0 U3p using the Avaya Dell customized ESXi offline bundle zip file available on PLDS. This zip file can be used to upgrade ASP 130 R5.1 ESXi hosts to ASP 130 R5.1.0.4. Customers that are on R4.0 (ESXi 6.5 – must be on latest release Build #19092475) or R5.0 (ESXi 7.0U2) must conduct a step-up upgrade to R5.1, R5.1.0.1, R5.1.0.2 or R5.1.0.3 first before upgrading to R5.1.0.4.

Reference to the latest Product Correction Notice (PCN) *PCN2146S* on the Avaya Support website for the latest software, licensing instructions and any further details.

Reference to the Avaya Solutions Platform 130 Series Updating to R5.1.0.4.0 (ESXi 7.0 U3p) from R5.1x. (ESXi 7.0 U3x) *or earlier versions of this document as necessary and* Installing the Avaya Solutions Platform 130 Series documents on the Avaya Support website for installation and upgrade details, and instructions.

Upgrade to ASP 130 R5.1.0.3 (ESXi 7.0 U3o)

The ASP 130 5.1.0.3 release is launching with the Avaya Dell customized VMware ESXi 7.0 Update 3o build 22348816 for install on the ASP 130 R640 servers. Customer can upgrade their ASP 130 Solution to ESXi 7.0 U3o using the Avaya Dell customized ESXi offline bundle zip file available on PLDS. This zip

file can be used to upgrade ASP 130 ESXi host from 7.0.x builds to ESXi 7.0 U3o. Customers that are on R4.0 (ESXi 6.5 – must be on latest release Build #19092475) or R5.0 (ESXi 7.0U2) must conduct a step-up upgrade to R5.1, R5.1.0.1 or R5.1.0.2 first before upgrading to R5.1.0.3.

Reference to the latest Product Correction Notice (PCN) *PCN2146S* on the Avaya Support website for the latest software, licensing instructions and any further details.

Reference to the Avaya Solutions Platform 130 Series Updating to R5.1.0.3.0 (ESXi 7.0 U3o) from R5.1.x (ESXi 7.0 U3x) *or earlier versions of this document as necessary* and Installing the Avaya Solutions Platform 130 Series documents on the Avaya Support website for installation and upgrade details, and instructions.

Upgrade to ASP 130 R5.1.0.2 (ESXi 7.0 U3i)

The ASP 130 5.1.0.2 release is launching with the Avaya Dell customized VMware ESXi 7.0 Update 3i build 20842708 for install on the ASP 130 R640 servers in release 5.1.0.2. Customer can upgrade their ASP 130 Solution to ESXi 7.0 U3i using the Avaya Dell customized ESXi offline bundle zip file available on PLDS. This zip file can be used to upgrade ASP 130 ESXi host from 6.5.x or earlier 7.0.x builds to ESXi 7.0 U3i.

Reference to the latest Product Correction Notice (PCN) *PCN2146S* on the Avaya Support website for the latest software, licensing instructions and any further details.

Reference to the "Avaya Solutions Platform 130 Series Upgrading to R5.1.0.2.0 (ESXi 7.0 U3i) from R4.x (ESXi 6.5.x) or R5.x (ESXi 7.0.x)" and Installing the Avaya Solutions Platform 130 Series documents on the Avaya Support website for installation and upgrade details, and instructions.

Note: ASP 130 R4.0 must be on Avaya approved/certified ESXi 6.5 U3 Build #19092475 prior to upgrading to ASP 130 5.1.0.2. Reference *PSN027079u- Avaya Solutions Platform 130 R4.0 Dell® R640 Customized Image of VMware ESXi 6.5.*

Upgrade to ASP 130 R5.1.0.1 (ESXi 7.0 U3d)

The ASP 130 5.1.0.1 release is launching with the Avaya Dell customized VMware ESXi 7.0 Update 3d build 19482537 for install on the ASP 130 R640 servers in release 5.1.0.1. For new ASP 130 builds from the integrator, ASP 130 Dell R640 servers will be shipped with ESXi 7.0 U3d installed and a standard ESXi license installed. The Customer/BP/APS only needs to activate the ESXi license on PLDS. For customers who would like to upgrade or work with Avaya to upgrade their ASP 130 solution can upgrade to ESXi 7.0 U3d using the Avaya Dell customized ESXi offline bundle ZIP file available on PLDS.

This method can be used to upgrade the ASP 130 ESXi host from 6.5.x/7.0.x to release 7.0 U3d using a ZIP file. In Release 5.1.0.1 there are new procedures in place to upgrade ESXi with an image profile update command to upgrade the host to ESXi 7.0 U3d.

Reference to the Avaya Solutions Platform 130 Series Updating to R5.1.0.3.0 (ESXi 7.0 U3o) from R5.1.x (ESXi 7.0 U3x) and Installing the Avaya Solutions Platform 130 Series documents on the Avaya Support website for installation and upgrade details, and instructions.

Note: ASP 130 R4.0 must be on Avaya approved/certified ESXi 6.5 U3 Build #19092475 prior to upgrading to ASP 130 5.1.0.1. Reference *PSN027079u- Avaya Solutions Platform 130 R4.0 Dell® R640 Customized Image of VMware ESXi 6.5.*

Upgrade to ASP 130 R5.1 (ESXi 7.0 U3c)

The ASP 130 5.1 release is launching with the Avaya Dell customized VMware ESXi 7.0 Update 3c build 19193900 for install on the ASP 130 R640 servers in release 5.1. For new ASP 130 builds from the

integrator, ASP 130 Dell R640 servers will be shipped with ESXi 7.0 U3c installed and a standard ESXi license installed. The Customer/BP/APS only needs to activate the ESXi license on PLDS. For customers who would like to upgrade or work with Avaya to upgrade their ASP 130 solution can upgrade to ESXi 7.0 U3c using the Avaya Dell customized ESXi offline bundle ZIP file available on PLDS.

This method can be used to upgrade the ASP 130 ESXi host from 6.5.x/7.0.x to release 7.0 U3c using a ZIP file. In Release 5.1 there are new procedures in place to upgrade ESXi with an image profile update command to upgrade the host to ESXi 7.0 U3c.

Reference to the *"Avaya Solutions Platform 130 Series Upgrading to R5.1 (ESXi 7.0 U3c) from R4.x (ESXi 6.5.x) or R5.0 (ESXi 7.0 U2a)"* and "*Installing the Avaya Solutions Platform 130 Series 5.1"* documents on the Avaya Support website for installation and upgrade details, and instructions.

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.*

For existing ASP 130 servers, when upgrading from ASP 130 R4.0 (ESXi 6.5.x) to ASP 130 R5.1.x.x (ESXi 7.0 U3c - R5.1, ESXi 7.0 U3d - R5.1.0.1, ESXi 7.0 U3i - R5.1.0.2, ESXi 7.0 U3o – R5.1.0.3) a new license key for vSphere 7 standard is required. The license will be available for activation on PLDS after the order is placed. For upgrades, migrations and recovery the implementor will need to retrieve the ESXi license from PLDS. When upgrading from ASP 130 R5.0 (ESXi 7.0 U2) to any ASP 130 5.1.x.x (ESXi 7.0 U3), a new license key is not required.

Existing vSphere 6.5 license keys which were shipped with the license key on the server lid, will not work for ESXi 7.0, a new license will be required. A license key per ASP 130 host is required.

Avaya's integrator will deliver the ASP 130 R5.x Dell R640 server with vSphere ESXi 7.0 loaded and a standard ESXi license installed. Installers should always verify the ASP 130 is at the latest posted certified version on PLDS and if necessary upgrade to the latest posted release.

See "*Installing the Avaya Solutions Platform 130 Series"* document for more details on the new PLDS licensing.

ESXi 7.0 System Storage changes

When using the ESXi 7.0.x ISO image there is a new VMFS-L partition that will be created when upgrading to or conducting a fresh install of ESXi 7.0. The VMFS-L partition consolidates the small core-dump, locker and large core-dump partitions enabling more space for frequently written data like logs and system configurations and state.

With an upgrade from ASP 130 R4.0 (ESXi 6.5) to ASP 130 R5.x (ESXi 7.0), the VMFS-L partition size will be 6.3 GB and with a fresh install of ESXi 7.0 the VMFS-L partition size will be 33GB. Avaya further customized the Dell ESXi 7.0 ISO image to set the VMFS-L partition through the boot config file. When upgrading from ASP 130 R5.0 to ASP 130 R5.1.x, the VMFS-L partition size will already be set to 6.3 GB.

For additional information refer to the following document:

ESXi System Storage Changes | VMware

ESXi 7.0 Datastore name

If you migrated from AVP 8.1.X on a ASP 120 the datastore will be "server-local-disk". If this was a fresh install or a recovery or remaster of the ASP 130 the datastore will be "datastore1".

/vmfs/volumes/server-local-disk

/vmfs/volumes/datastore1

VMFS Datastore version support

VMFS Filesystem versions 5 and 6 are both compatible with ASP 130 5.x.

- VMFS Filesystem version 6 on fresh ESXi 7.0 installs.
- VMFS Filesystem version 5 remains when upgrading ESXi from 6.5.x to 7.0.x. ESXi 7.0 is backwards compatible with previous filesystem types.

For a complete feature comparison between VMFS 5 and 6, refer to the following document:

Versions of VMFS Datastores (vmware.com)

Avaya Tools and EASG VIBs

The Avaya Tools and EASG VIBs provide Avaya support and technicians with access to the ASP 130 server for maintenance and troubleshooting activities.

Avaya Tools:

The ASP130-config-v1.sh also known as the Installation Configuration Script that was provided in previous ASP 130 4.0/5.0 releases is now included as part of the Avaya Tools VIB. When upgrading from ESXi 6.5.x/7.0 to 7.0 U3c or later, the script will be executed as part of the first boot script.

The Avaya Tools VIB also includes the Avaya EULA. Users are now prompted to accept the Avaya EULA after the first SSH login.

EASG:

When upgrading from ASP 130 R4.0/R5.0 (ESXi 6.5/7.0U2) to ASP 130 5.1.x, the EASG service will be enabled by default on the ESXi host.

A new sroot account gets automatically created during the upgrade process.

Note: Avaya Solutions Platform 130 5.1.x systems coming from Avaya's integrator will already have the Avaya Tools and EASG VIBs installed and will not require execution of the VIBs. Server recovery (FRU) and software remastering to release 5.1.x will require the EASG VIB to be copied to the host and the EASG script ran.

PowerEdge RAID Controller Command Line Interface (Perccli)

Beginning with ASP 130 release 5.1.0.1, the Dell Perccli utility is included in the ISO and zip files. The Perccli commands can be used to view the existing configuration including the status of the RAID controller, Virtual drive(s), Battery and Array.

Warning: Running certain Perccli commands not specified by Avaya may corrupt the Array and User data could be destroyed. Only conduct "show" commands specified in the Maintaining and Troubleshooting ASP 130 Series document.

ASP_SSH Script

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

On running this script the 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 the following command: `ASP_SSH enable`

The script can only be executed by root user privileged user for respective application. After the script is successfully run wait for 3 minutes before trying the SSH to ASP.

Note:

- By default SSH is enabled on ASP 130.
- In case ASP_SSH is run by mistake on a setup which had SSH enabled while installation; the script will override the timeout value and SSH will then be disabled after the 2 hour window.

Dell R640 Server Firmware updates

Always check support.avaya.com for the latest Avaya certified BIOS/Firmware updates available for the Dell R640 servers. As of December, 2023, the following is the most recent update available. Reference *PSN027110u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 15.0* for installation details and procedures.

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 130 Release 5.1.x Software files
The following tables provide the Avaya Solutions Platform 130 release 5.1.x file download information. For the latest deployment and upgrade procedures, see Avaya Solutions Platform 130 Series Updating to R5.1.0.6.0 (ESXi 7.0 U3s) from R5.1.0.5.0. (ESXi 7.0 U3q) or for updates to R5.1.0.5.0, see Avaya Solutions Platform 130 Series Updating to R5.1.0.5.0 (ESXi 7.0 U3q) from R5.1x. (ESXi 7.0 U3x) and Installing the Avaya Solutions Platform 130 Series documents on the Avaya Support website.

Required files for Avaya Solutions Platform 130 5.1.0.6:

Download ID	Download Name	File name	Description
ASP000000028	ASP 130 5.1.0.6 Dell® R640 Customized ESXi 7.0 U3s Build#24585291 ZIP File	AVAYA-DELL-ESXi-7u3s-24585291.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 files for Avaya Solutions Platform 130 5.1.0.5:

Download ID	Download Name	File name	Description
ASP000000025	ASP 130 Dell® R640 Customized ESXi 7.0 U3q Build#23794027 ZIP File	AVAYA-DELL-ESXi-7u3q-23794027.zip	VMware ESXi 7.0 U3q build 23794027 ZIP file used for upgrades.
ASP000000024	ASP 130 Dell® R640 Customized ESXi 7.0 U3q Build#23794027 ISO	AVAYA-DELL-ESXi-7u3q-23794027-min.iso	VMware ESXi 7.0 U3q build 23794027 ISO image used for fresh installs. ISO image is burnt to CD/DVD disk.
ASP000000026	ASP 100 Series Dell® R640 Avaya Certified BIOS/FW Update, V14.0	R640fw-v14.0.iso	New BIOS/firmware package for the ASP 130 Dell R640 server. Released August 19, 2024. Reference *PSN027109u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 14.0.*
ASP000000010	ASP 130 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 130 5.1.x servers. This is ONLY applicable to ASP 130 servers and ASP S8300 servers. **This v3 script replaces any existing OOBM scripts**. *Same file as was used with R5.1.0.4.*
ASP000000023	ASP 130 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 130 servers. **Version 1.1-7 replaces all earlier versions** of the customized EASG VIB on 5.1.x and is compatible with all ASP 130 5.1.x.x. *Same file as was used with R5.1.0.4.*

Required files for Avaya Solutions Platform 130 5.1.0.4:

Download ID	Download Name	File name	Description
ASP000000022	ASP 130 Dell® R640 Customized ESXi 7.0 U3p Build#23307199 ZIP File	AVAYA-DELL-ESXi-7u3p-23307199.zip	VMware ESXi 7.0 U3p build 23307199 ZIP file used for upgrades.
ASP000000021	ASP 130 Dell® R640 Customized ESXi 7.0 U3p Build#23307199 ISO	AVAYA-DELL-ESXi-7u3p-23307199-min.iso	VMware ESXi 7.0 U3p build 23307199 ISO image used for fresh installs. ISO image is burnt to CD/DVD disk.
ASP000000020	ASP 100 Series Dell® R640 Avaya Certified BIOS/FW Update, V13.0	R640fw-v13.0.iso	New BIOS/firmware package for the ASP 130 Dell R640 server. Released April 29, 2024. Reference *PSN027107u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 13.0.*
ASP000000010	ASP 130 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 130 5.1.x servers. This is ONLY applicable to ASP 130 servers and ASP S8300 servers. **This v3 script replaces any existing OOBM scripts**. PLDS ID remains the same.
ASP000000023	ASP 130 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 130 servers. **Version 1.1-7 replaces all earlier versions** of the customized EASG VIB on 5.1.x and is compatible with all ASP 130 5.1.x.x.

Required files for Avaya Solutions Platform 130 5.1.0.3:

Download ID	Download Name	File name	Description
ASP000000019	ASP 130 Dell® R640 Customized ESXi 7.0 U3o Build#22348816 ZIP File	AVAYA-DELL-ESXi-7u3o-22348816.zip	VMware ESXi 7.0 U3o build 22348816 ZIP file used for upgrades.
ASP000000018	ASP 130 Dell® R640 Customized ESXi 7.0 U3o Build#22348816 ISO	AVAYA-DELL-ESXi-7u3o-22348816-min.iso	VMware ESXi 7.0 U3o build 22348816 ISO image used for fresh installs. ISO image is burnt to CD/DVD disk.
ASP000000017	ASP 100 Series Dell® R640 Avaya Certified BIOS/FW Update, V12.0	R640fw-v12.0.iso	New BIOS/firmware package for the ASP 130 Dell R640 server. Released October 25, 2023. Reference *PSN027106u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 12.0..*
ASP000000010	ASP 130 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 130 5.1.x servers. This is ONLY applicable to ASP 130 servers and ASP S8300 servers. **This v3 script replaces any existing OOBM scripts**. PLDS ID remains the same.
ASP000000008	ASP 130 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 130 servers. *Same file as was used for ASP 130 R5.1, 5.1.0.1, 5.1.0.2*

Required files for Avaya Solutions Platform 130 5.1.0.2:

Download ID	Download Name	File name	Description
ASP000000016	ASP 130 Dell® R640 Customized ESXi 7.0 U3i Build#20842708 ZIP File	AVAYA-DELL-ESXi-7u3i-20842708.zip	VMware ESXi 7.0 U3i build 20842708 ZIP file used for upgrades.
ASP000000015	ASP 130 Dell® R640 Customized ESXi 7.0 U3i Build#20842708 ISO	AVAYA-DELL-ESXi-7u3i-20842708-min.iso	VMware ESXi 7.0 U3i build 20842708 ISO image used for fresh installs. ISO image is burnt to CD/DVD disk.
ASP000000014	ASP 100 Series Dell® R640 Avaya Certified BIOS/FW Update, V11.0	R640fw-v11.0.iso	New BIOS/firmware package for the ASP 130 Dell R640 server.
ASP000000010	ASP 130 OOBM Configuration script	asp_oobm_v2.sh	This is an Avaya script that facilitates the configuration of Out of Band Management (OOBM) on the ASP 130 5.1.x servers. This is ONLY applicable to ASP 130 servers and ASP S8300 servers. This v2 script replaces any existing OOBM scripts. PLDS ID remains the same.
ASP000000008	ASP 130 Customized EASG VIB *No change from ASP 130 5.1*	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 130 servers.

Required files for Avaya Solutions Platform 130 5.1.0.1:

Download ID	Download Name	File name	Description
ASP000000013	ASP 130 Dell® R640 Customized ESXi 7.0 U3d Build#19482537 ZIP File	AVAYA-DELL-ESXi-7u3d-19482537.zip	VMware ESXi 7.0 U3d build 19482537 ZIP file used for upgrades.
ASP000000012	ASP 130 Dell® R640 Customized ESXi 7.0 U3d Build#19482537 ISO	AVAYA-DELL-ESXi-7u3d-19482537-min.iso	VMware ESXi 7.0 U3d build 19482537 ISO image used for fresh installs. ISO image is burnt to CD/DVD disk for field technician.
ASP000000011	ASP 100 Series Dell® R640 Avaya Certified BIOS/FW Update, V10.2	R640fw-v10.2.iso	New firmware package for the ASP 130 Dell R640 server.
ASP000000010	ASP 130 OOBM Configuration script *No change from ASP 130 5.1*	asp_oobm_v1.sh	This is an Avaya script that facilitates the configuration of Out of Band Management (OOBM) on the ASP 130 5.1.x servers. This is ONLY applicable to ASP 130 servers and ASP S8300 servers.
ASP000000008	ASP 130 Customized EASG VIB *No change from ASP 130 5.1*	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 130 servers.

Required files for Avaya Solutions Platform 130 5.1:

Download ID	Download Name	File name	Description
ASP000000005	ASP 130 Dell® R640 Customized ESXi 7.0 U3c Build#19193900 ISO	AVAYA-DELL-ESXi-7.0U3c-19193900-min.iso	VMware ESXi 7.0 U3c build 19193900 ISO image used for fresh installs. ISO image is burnt to CD/DVD disk for field technician.
ASP000000006	ASP 130 Dell® R640 Customized ESXi 7.0 U3c Build#19193900 ZIP File	AVAYA-DELL-ESXi-7.0U3c-19193900.zip	VMware ESXi 7.0 U3c build 19193900 ZIP file used for upgrades.
ASP000000007	ASP 100 Series Dell® R640 Avaya Certified BIOS/FW Update, V10.1	R640fw-v10.1.iso	New firmware package for the ASP 130 Dell R640 server.
ASP000000008	ASP 130 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 130 servers.
ASP000000010	ASP 130 OOBM Configuration script	asp_oobm_v1.sh	This is an Avaya script that facilitates the configuration of Out of Band Management (OOBM) on the ASP 130 5.1 servers

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

Security Information

Security Statement

Avaya Solutions Platform is a solution comprised of hardware and software products. Security vulnerabilities for each product are 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).

Security Enhancements in ASP 130 R5.1.x.x

TLS protocols: In ESXi 7.0 TLS 1.0 and 1.1 are disabled by default whether it is a fresh install of ESXi 7.0 or an upgrade to ESXi 7.0. In the event it is required to re-enable TLS 1.0 and 1.1, procedures are available in order to re-enable. See the "*Installing the Avaya Solutions Platform 130 Series"* documentation for more details and procedures.

Improved SSH cipher strength (22/TCP): CBC-based ciphers are disabled by default (3DES-CBC). SSH supports only 256-bit and 128-bit AES ciphers for the connections.

SNMPv3: MD5 is no longer a supported authenticated method when configuring SNMPv3 on an ESXi server. It has been deprecated due to known weaknesses. To configure SNMPv3 on iDRAC and ESXi see the "*Installing the Avaya Solutions Platform 130 Series 5.1.x"* documentation for more details and procedures.

iDRAC: Starting with ASP 130 release 5.x and onward the community string will be set to Avaya123 by Avaya's Integrator instead of using the previous public community string.

Reference the **Fixes in Avaya Solutions Platform 130 5.1.x releases** section for details on VMSAs delivered in each release.

Fixes in Avaya Solutions Platform 130 5.1.x releases

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 – *N/A for ASP 130/S8300 as AD integration is not supported. There is also a QUALYS issue where it is flagging this CVE even though it is resolved in 7.0U3q.* 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.

Reference VMware 7.0 Release notes for additional details on all updates included in the individual releases.

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 u3c	Reconfigure event reported every 3 minutes on VMware console	5.1

Fixes in release 5.1

Note: Reference VMware ESXi 7.0 U3c Release Notes for additional information.

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ACP1XX-328	ESXi 6.5, 7.0	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.	4.0 and 5.0
ACP1XX-325	ESXi 6.5, 7.0	Security vulnerability VMSA-2022-0001.1 (CVE-2021-22045) found in security scan results.	4.0 and 5.0
ACP1XX-4	ESXi 6.5, 7.0	ESXi root account login credentials lost or forgotten. Cannot login into the ESXi vSphere UI from a web browser using the root credentials.	4.0 and 5.0
ACP1XX-79	ESXi 6.5	TLS 1.0 and 1.1 are not disabled by default in ESXi 6.5. In ESXi 7.0 TLS 1.0 and 1.1 are disabled by default	4.0
ACP1XX-89	ESXi 6.5	Security scans flag 3des-cbc in sshd_config file. 3des-cbc is not present in ESXi 7.0.	4.0

Known issues in Avaya Solutions Platform 130 5.1.x releases

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 5.1.0.6

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-837	CD-ROM drive model DU-8D5LH	PSOD	Refer to PSN027080u
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 130 currently ships with SSH enabled as it is required for installation/configuration. Release Notes for reference https://support.avaya.com/css/public/documents/101081340

Known issues and workarounds in release 5.1.0.5

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-837	CD-ROM drive model DU-8D5LH	PSOD	Refer to PSN027080u
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 130 currently ships with SSH enabled as it is required for installation/configuration. Release Notes for reference https://support.avaya.com/css/public/documents/101081340

Known issues and workarounds in release 5.1.0.4

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-837	CD-ROM drive model DU-8D5LH	PSOD	Refer to PSN027080u

Known issues and workarounds in release 5.1.0.3

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-837	CD-ROM drive model DU-8D5LH	PSOD	Refer to PSN027080u
ACP1XX-1082	ASP 5.1.x	ESXi shell not enabled at Avaya integrator or at time of installation of ISO	ESXi shell service is disabled by default beginning in ASP 130 R5.1. Steps to enable/disable as required to align with customer security policies are documented in Installing the Avaya Solutions Platform 130 Series.
ACP1XX-704	ASP 5.1.x	Special characters in the local datastore name can cause EASG install script to fail.	Do not use special characters for local datastore names.

Known issues and workarounds in release 5.1.0.2

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-837	CD-ROM drive model DU-8D5LH	PSOD	Refer to PSN027080u
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

ID	Minimum conditions	Visible symptoms	Workaround
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	No workaround from vendor. This will be resolved in a future release of ASP 130 5.1.0.x.
ACP1XX-564	ESXi 7.0 u3d	Security vulnerability VMSA-2022-0025 (CVE-2022-31680, CVE-2022-31681) found in security scan results	No workaround from vendor. This will be resolved in a future release of ASP 130 5.1.0.x.
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	No workaround from vendor. This will be resolved in a future release of ASP 130 5.1.0.x.

Known issues and workarounds in release 5.1

ID	Minimum conditions	Visible symptoms	Workaround
ACP1XX-88	ESXI 6.5, 7.0	Security scans flag UDP source port pass firewall	Reference *PSN027092u- Avaya Solutions Platform 130 Source Port Firewall flagged on Qualys Security Scan* for workaround.
ACP1XX-261	First login attempt after upgrading to ESXi 7.0 U2 returns error “Unhandled Exception (1)”	Behavior was observed after upgrading to ESXi 7.0 U2 and trying to access the ESXi UI from Browser Mozilla Firefox.	Upgrade the Firefox browser on PC/workstation to current browser version later than release v80.
ACP1XX-268	ESXI 7.0	Security scans flag Presence of a Load-Balancing Device Detected (tcp)	This is a false positive and can be ignored as long as external NTP servers are configured to properly synchronize the host time.

Resources

Documentation

List of documentation available for the Avaya Solutions Platform 130 5.1.x solution. Documents can be located on the Avaya Support Website: https://support.avaya.com

Title	Description
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform
Avaya Solutions Platform 130 Series – Updating to R5.1.0.6.0 (ESXi 7.0 U3q) from R5.1.0.5.0 (ESXi 7.0 U3q)	Describes procedure to perform upgrade to ASP 130 5.1.0.6.0 release from earlier ASP 130 5.1.x releases. Direct upgrade to 5.1.0.6.0 is only supported from 5.1.0.5.0.
Avaya Solutions Platform 130 Series – Updating to R5.1.0.5 (ESXi 7.0 U3q) from R5.1.x (ESXi 7.0 U3x)	Describes procedure to perform upgrade to ASP 130 5.1.0.5.0 release from earlier ASP 130 5.1.x releases.
Avaya Solutions Platform 130 Series – Updating to R5.1.0.4 (ESXi 7.0 U3p) from R5.1.x (ESXi 7.0 U3x)	Describes procedure to perform upgrade to ASP 130 5.1.0.4.0 release from earlier ASP 130 5.1.x releases.
Avaya Solutions Platform 130 Series - Updating to R5.1.0.3.0 (ESXi 7.0 U3o) from R5.1.x (ESXi 7.0 U3x)	Describes procedure to perform upgrade to ASP 130 5.1.0.3.0 release from earlier ASP 130 5.1.x releases.
Upgrading to R5.1.0.2 (ESXi 7.0 U3i) from R4.x (ESXi 6.5.x) or R5.x. (ESXi 7.0.x)	Describes procedure to perform upgrade to ASP 130 5.1.0.2.0 release from earlier ASP 130 5.1.x or 4.x releases.
Upgrading to R5.1.0.1.0 (ESXi 7.0 U3d) from R4.x (ESXi 6.5.x) or R5.x (ESXi 7.0.x)	Describes procedure to perform upgrade to ASP 130 5.1.0.1.0 release from ASP 130 5.1.x or 4.x releases.
Avaya Solutions Platform 130 Series Upgrading to R5.1 (ESXi 7.0 U3c) from R4.x (ESXi 6.5.x) or R5.0 (ESXi 7.0 U2a)	Describes procedures to perform upgrades/updates from ESXi 6.5.x and ESXi 7.0 U2a to ESXi 7.0 U3c. The specified installation media is an Avaya customized version of ESXi.
Installing the Avaya Solutions Platform 130 Series 5.1.x	Describes how to install Avaya Solutions Platform 130 Series.
Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series.
Avaya Solutions Platform 130 Series iDRAC9 Best Practices	Describes the best practices of using Integrated Dell Remote Access Controller (iDRAC).
PSN027110u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 15.0	This is a Product Support Notice about Dell® R640 Avaya Certified BIOS/FW Update. Always check support.avaya.com for the latest Avaya certified BIOS/Firmware updates available for the Dell R640 servers.
PSN027109u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 14.0	This is a Product Support Notice about Dell® R640 Avaya Certified BIOS/FW Update. Always check support.avaya.com for the latest Avaya certified BIOS/Firmware updates available for the Dell R640 servers.
PSN027107u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 13.0	This is a Product Support Notice about Dell® R640 Avaya Certified BIOS/FW Update. Always check support.avaya.com for the latest Avaya certified BIOS/Firmware updates available for the Dell R640 servers.

PSN027106u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 12.0	This is a Product Support Notice about Dell® R640 Avaya Certified BIOS/FW Update. Always check support.avaya.com for the latest Avaya certified BIOS/Firmware updates available for the Dell R640 servers.
PSN027105u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 11.0	This is a Product Support Notice about Dell® R640 Avaya Certified BIOS/FW Update. Always check support.avaya.com for the latest Avaya certified BIOS/Firmware updates available for the Dell R640 servers.
PSN027103u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 10.2	This is a Product Support Notice about Dell® R640 Avaya Certified BIOS/FW Update. Always check support.avaya.com for the latest Avaya certified BIOS/Firmware updates available for the Dell R640 servers.
PSN027102u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 10.1	This is a Product Support Notice about Dell® R640 Avaya Certified BIOS/FW Update. Always check support.avaya.com for the latest Avaya certified BIOS/Firmware updates available for the Dell R640 servers.
Port Matrix for ASP 130	This document provides a list of interfaces, TCP and UDP ports that hardware components and applications use for intra-connections and for inter-connections with external applications or devices.
Policies for technical support of the Avaya Solutions Platform (ASP) 130 R4.x, R5.x and S8300 R5.1	This document and statements related to support are only with respect to Avaya Services support of the software and hardware of the Avaya Solutions Platform (ASP) 130/S8300 servers based on supported and tested configurations.
Product Correction Notice for ASP 130 (PCN2146S)	Product Correction Notice (PCN) covering the new release software and firmware files required for install and upgrade of the ASP 130 5.1.x release.

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

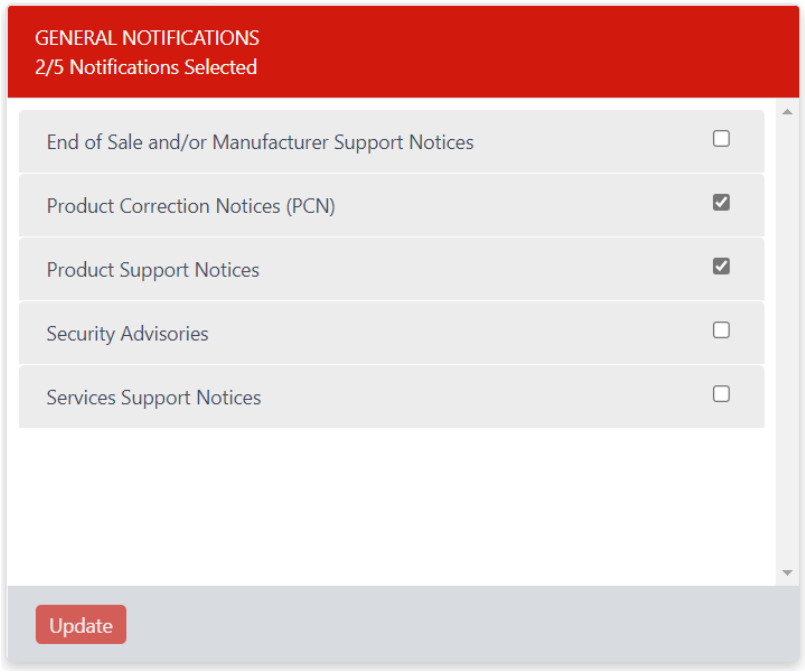
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

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.

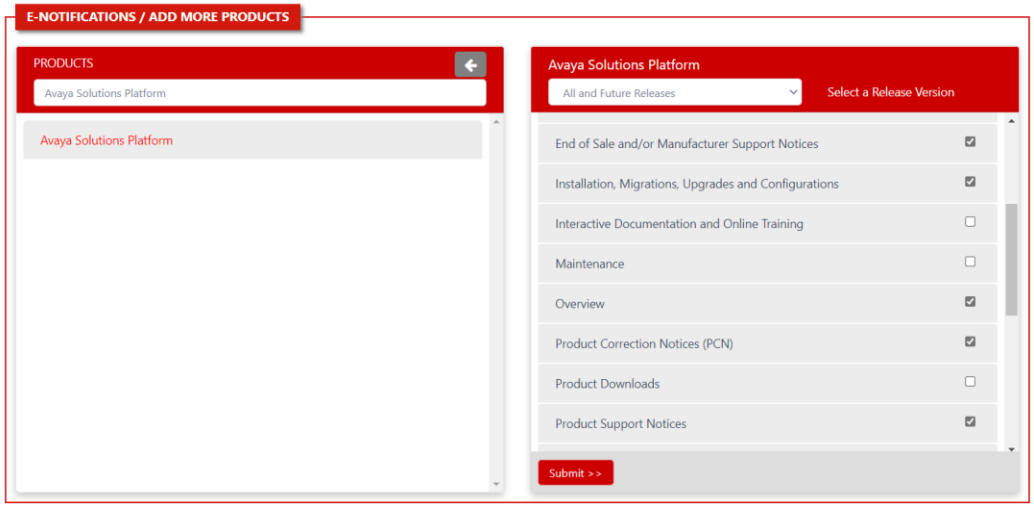
Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. At the top-right select the user, 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**.