Product Support Notice

PSN #	PSN020360u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date: 23-Aug-18. This is Issue #03, published date: 07-Mar-23.		Severity/risk level	Medium	Urgency	When convenient
Name of problem	PSN020360u - Avaya Aura® Software-only Environment Supported Third Party Applications				

Products affected

Avaya Aura® Application Enablement Services, Release 8.x, 10.1.x
Avaya Aura® Communication Manager, Release 8.x, 10.1.x
Avaya Aura® Session Manager, Release 8.x, 10.1.x
Avaya Aura® System Manager, Release 8.x, 10.1.x
Avaya Aura® WebLM (Standalone), Release 8.x, 10.1.x

Problem description

UPDATE: March 6, 2023 – Avaya Aura 8.x has reached End of Manufacturer Support (EOMS) per the Lifecycle Notice. Customers wishing to utilize third party applications with Avaya Aura 8.x and 10.1.x software only deployments should reference the requirements below.

Due to the increasing number of these antivirus and other 3rd-party applications/plug-ins it is not possible for Avaya to test and support these for each and every Avaya Aura application and its subsequent releases as well as keeping current with the ongoing updates from the 3rd-party vendors.

Installation of 3rd party applications/plug-ins, including antivirus and security monitoring tools, is not supported in Avaya Aura® 8.x and 10.1.x OVA deployments. *Reference PSN020591u- Avaya Aura® third party application support clarified*.

The 3rd party applications originally approved in the 8.0.x timeframe are no longer supported as Aura 8.x is now EOMS.

Historical Information from original Issue 1, 2 of this PSN which is obsolete going forward:

The Avaya Aura® Release 8.0.x supports software-only installation. For software-only deployment, the customer owns the operating system and the customer is responsible to provide and configure the operating system for use with the Avaya Aura® application. With the software-only offer, the customer can install and customize the operating system to meet the requirements to install Avaya Aura® applications.

The software-only offer allows the customer to install third party applications on the system and provides more control on the system. You must run the software-only offer on the supported environments to enable the use of Avaya approved third party applications.

This PSN lists the Avaya approved third party applications that are currently supported for the software-only products listed under the "Products affected" section of this PSN.

This PSN will be updated as additional third party applications are certified.

Any third party application not listed in this PSN is not a supported configuration and Avaya will not provide services support in that case.

Resolution

Historical Information from original Issue 1, 2 of this PSN which is obsolete going forward:

Avaya maintains a list of tested and certified software / agents for the "Software Only" deployment option.

These are applicable to all of the products listed under the "Products affected" section of this PSN except where noted below.

Currently supported third party applications:

SECURITY TOOLS	**Certified/Supported Aura Version**	**Comments**
Trend Micro - TrendMicro Deep Security as a Service on AWS	8.0 8.0.1	n/a
Symantec Endpoint Protection – Symantec Endpoint Protection 14.0.1	8.0 8.0.1	n/a

MP2 Linux Client EN		
McAfee Endpoint Security for Linux Threat Prevention Version: 10.5.0.1485 DAT Version: 9089.0 Engine Version: 5900.7806	8.0.1	**CM:** A default Access Protection rule defined for McAfee Endpoint Security 10.5 needs to be disabled. “IDS_AP_RULE_PREVENT_MODIFICATION_PASSWORDFILES_LINUX”. It blocks updates to password/shadow files and CM needs to modify them when adding/updating CM admin users (via SMI or filesync to standby machine). Follow McAfee documentation in link to disable this rule. https://docs.mcafee.com/bundle/endpoint-security-10.5.0-threat-prevention-product-guide-linux/page/GUID-94135CD9-4F0B-4E91-A21A-C4C735DC9D41.html **AES and SM:** If the McAfee Endpoint Protection is already installed and enabled, AES and SM installations might fail. Before installing AES or SM, you must disable the McAfee Endpoint Protection application by using the following command: isecav -setapstatus disable

MONITORING TOOLS	Certified/Supported Aura Version	Comments
SolarWinds - SolarWinds SAM (Server & Application Monitor) Version: 6.6.1	8.0 8.0.1	n/a
NetScout - Netscout mGeniousOne Version 6.0.1 (Build 270) for reporting VStream 6.0.1 (Build 245)	8.0 8.0.1	n/a
Splunk Enterprise Version: 7.2.0 Build: 8c86330ac18	8.0.1	Before and after the installation of Avaya Aura Applications, make sure that "9997" port is open on the application.

Additional third party applications will be tested and added to the list as they are approved.

To request an assessment of the feasibility of a third party application not listed above, please contact your Account Team to initiate the discussion.

Workaround or alternative remediation

n/a

Remarks

Issue 2 – Jan. 07, 2019: Added Splunk Universal Forwarder and McAfee Endpoint Security for Linux Threat Prevention. Removed AES 7.x.

Issue 3 – Mar 7, 2023: PSN updated to reflect Aura® 8.x EOMS and current policy.

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

n/a

Download

n/a

Patch install instructions — Service-interrupting?

n/a — Yes

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

n/a

Mitigation

n/a

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.