Product Support Notice

PSN #	PSN004962u				
Original publication date: 06-Apr-17. This is Issue #02, published date: 08-Sep-17.		Severity/risk level	High	Urgency	Immediately

Name of problem

Secure Access Link (SAL) 3.0 is new technology, incompatible with previous SAL.

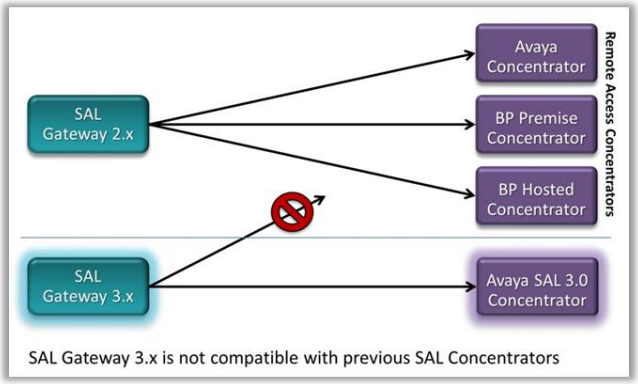
Products affected

- SAL 2.x Gateways
- SAL 2.x Concentrators
- Policy Server all releases

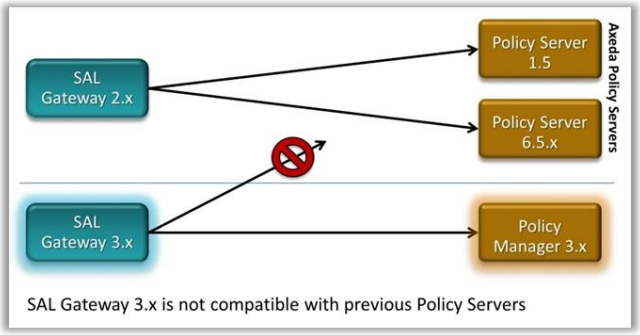
Customers and business partners should begin planning immediately for future upgrades and migrations.

Problem description

To deliver new features and latest security and technology updates, Avaya has released and is releasing SAL 3.0, which includes a new SAL Gateway, SAL Concentrator, and Policy Manager. The new SAL 3.0 technology is incompatible with the previous SAL 2.x technology and associated Policy Server.

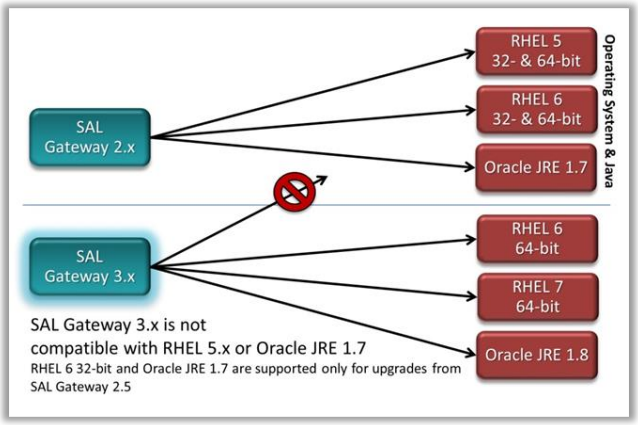


SAL Gateway 3.0 can only communicate with a SAL 3.0 Concentrator. Avaya has a SAL 3.0 Concentrator, but business partners will not have one until Dec 2017. Customers whose SAL Gateways are connected to a BP premise or hosted concentrator must wait until Dec 2017 to upgrade.



SAL Gateway 3.0 can only communicate with Policy Manager 3.0. If you have deployed a Policy Server, implement a new Policy Manager first, and then upgrade to SAL Gateway 3.0.

SAL Gateway 3.0 and Policy Manager 3.0 require RHEL 6 or 7. SAL Gateway releases 2.x installed on RHEL 6 may be upgraded to SAL Gateway 3.0. SAL Gateways installed on RHEL 5 must be migrated to a new installation of SAL Gateway 3.0 on RHEL 6 or 7.



The following announcements have been released:

- End of Sale for SAL Gateway 2.x and Policy Server all releases
- End of Services Support for SAL Gateway 2.x and Policy Server all releases
- End of Services Support for business partner SAL Concentrators

Resolution

Customers and business partners must migrate to SAL 3.0 technology by Dec 31, 2018. A **SAL Gateway 3.0 Upgrade Playbook** has been provided to assist with the upgrades and migrations.

SAL Gateway software on customer provided server and OS (Mar 31, 2017) For SAL Gateways connected directly to Avaya; Gateways connected to BP must wait until Dec 2017			
Starting Point	**Step 1**	**Step 2**	**Step 3**
Functioning software SAL Gateway 2.5 with - remote agent push - or SP2 (2.5.2.x) - or SP3 (2.5.3.x) - installed on RHEL 6	Upgrade the software to SAL Gateway 3.0		
Functioning software SAL Gateway 2.0, 2.1, 2.2, 2.3 with - remote agent push - installed on RHEL 6	Upgrade the software to SAL Gateway 2.5	Install ADS 2.5 SP3 (this is required to get the SHA-2 agent on the gateway prior to upgrade)	Upgrade the software to SAL Gateway 3.0
Any functioning SAL Gateway 2.5 with - remote agent push - or SP2 (2.5.2.x) - or SP3 (2.5.3.x)	Backup SAL Gateway using migration utility script, and store the backup archive	Install SAL Gateway 3.0 on a RHEL 6 or 7 machine, restoring the previous backup during installation	
Any functioning SAL Gateway 2.x that is SHA-2 compliant	Install SAL Gateway 3.0 on a RHEL 6 or 7 machine	Export the managed elements list via the web UI and save to file	Import the managed elements list to the new SAL Gtwy via the web UI
Note: SAL Gateway 2.5/3.0 is offered as part of the Avaya Diagnostic Server 2.5/3.0 package. The ADS 2.5/3.0 installer gives the customer the option to install either the SAL Gateway or the SLA Mon™ Server or both.			

SAL Gateway on Services-VM on System Platform (Jul 31, 2017) For SAL Gateways connected directly to Avaya; Gateways connected to BP must wait until Dec 2017	
Starting Point	**Step 1**
Functioning Services-VM 1.0 or 2.0 or 3.0 on System Platform 6.2.x or later	Upgrade to Services-VM 4.0 using System Platform VM upgrade utility (Services-VM 4.0 has SAL Gateway 3.0)

Small SAL Gateway OVA on AVP (Jul 31, 2017) For SAL Gateways connected directly to Avaya; Gateways connected to BP must wait until Dec 2017			
Starting Point	**Step 1**	**Step 2**	**Step 3**
Functioning small SAL 2.5 OVA with - remote agent push - or SP2 (2.5.2.x) - or SP3 (2.5.3.x)	Upgrade the software to SAL Gateway 3.0 on this same OVA		
	Backup SAL Gateway using the small OVA procedures, and store the backup archive	Deploy the small SAL 3.0 OVA using SDM	Restore the previous backup using the small OVA procedures

SAL Gateway on VMware OVA provided by Avaya (Aug 18, 2017) For SAL Gateways connected directly to Avaya; Gateways connected to BP must wait until Dec 2017			
Starting Point	**Step 1**	**Step 2**	**Step 3**
Functioning ADS 2.0 OVA upgraded to ADS 2.5 with - remote agent push - or SP2 (2.5.2.x) - or SP3 (2.5.3.x)	Backup SAL Gateway using migration utility script, and store the backup archive	Deploy ADS 3.0 OVA and install SAL Gateway 3.0, restoring the previous backup during installation	
Functioning ADS 2.0 OVA upgraded to ADS 2.5 Functioning ADS 2.0 OVA with remote agent push Functioning SAL 2.2 OVA with remote agent push	Deploy ADS 3.0 OVA and install SAL Gateway 3.0	Export the managed elements list via the web UI and save to file	Import the managed elements list to the new SAL Gtwy via the web UI

Workaround or alternative remediation

Continue running on SAL Gateway 2.x until the package you require, and BP concentrator where applicable, is available.

Remarks

n/a

Patch Notes

N/A – SAL Gateway 3.0 and Policy Manager 3.0 require an upgrade or new installation and migration.

Backup before applying the patch

Download

Patch install instructions Service-interrupting?

Verification

Failure

Patch uninstall instructions

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

Not Susceptible

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.