Product Support Notice

PSN #	PSN004539u				
Original publication date: 21-Jul-15. This is Issue #10, published date: 15-Nov-16.		Severity/risk level	High	Urgency	Immediately

Name of problem

SAL Gateway does not support SHA-2 certificates; causes complete remote access failure.

(Upgrade steps for System Platform 6.2 and later were greatly simplified in issue 8.)

(Issue 9 was updated with information on the latest service packs.)

As previously announced, the SHA-1 certificates expire at the end of 2016. To provide a buffer for possible unforeseen issues, Avaya has scheduled the change to SHA-2 certificates to occur on December 14, 2016. After that date all SAL Gateways not SHA-2 compliant will become inoperable. As of this publish date, 90% of SAL Gateway managed elements are behind a SHA-2 compliant SAL Gateway.

Products affected

All SAL Gateway releases.

Avaya business partners and customers must make immediate plans to prepare for the deadlines conveyed in this PSN.

Problem description

A SAL Gateway on a customer premise communicates with a SAL Concentrator in the Avaya datacenter (or in some cases in the business partner datacenter). The authenticity of the concentrator is verified using digital certificates. The Avaya SAL Concentrator presents an identity certificate which is signed by a certificate authority (CA), and the SAL Gateway authenticates that certificate by using a CA root certificate.

A similar authentication process can occur between the SAL Policy Server and the SAL Gateway, with a different set of certificates that may be provided by the customer. This authentication does not occur if the customer does not load these certificates.

This process is analogous to a web browser authenticating a secure website. The secure web server presents an identity certificate signed by a CA – such as Symantec, for example. The web browser authenticates that identity certificate by using a Symantec root certificate. This certificate-based authentication employs data encryption using a Secure Hash Algorithm (SHA).

Without the latest service packs, SAL Gateways are only capable of processing Secure Hash Algorithm 1 (SHA-1). The industry is quickly moving away from SHA-1 to SHA-2. Most or all CAs stopped issuing SHA-1 certificates after Dec 2015. Existing SHA-1 certificates in the field are expected to expire by Dec 2016 or sooner. This means that for all deployed SAL Gateways, the remote access connection between the SAL Gateway and SAL Concentrator, and the connection between the SAL Gateway and SAL Policy Server, will break starting Jan 1, 2017, if no remediating action is taken.

A SHA-2 certificate cannot be loaded onto any SAL Concentrator until all SAL Gateways in the field receive a technology update to make them capable of processing SHA-2 certificates. This is because, from a security standpoint, the SAL Concentrator cannot present two identity certificates for authentication – one SHA-1 and one SHA-2. The SAL Concentrator must present one identity certificate (SHA-2), and all SAL Gateways must be capable of authenticating that certificate, which means they must be capable of processing SHA-2.

As a result of this technology shift, Avaya has issued an End of Services Support notice for all SAL Gateway 1.x releases. Avaya will provide a SHA-2 technology upgrade path for the SAL Gateway 2.x releases.

Resolution

For Business Partners:

Pursuant to the original release of this PSN on 21-Jul-2015, and updates thereafter in 2015, all business partners who have their own SAL Concentrator (grandfathered in from an offer that expired years ago) should have confirmed that your current SHA-1 certificate does not expire before Dec 31, 2016.

Do not load a SHA-2 identity certificate onto the SAL Concentrator (neither the remote access nor the alarm concentrator) until all SAL Gateways in the field receive the SHA-2 technology update.

Do not load a SHA-2 CA root certificate onto any SAL Gateway until it receives the SHA-2 technology update. After a SAL Gateway receives the SHA-2 technology update, it is okay for that SAL Gateway to have both the SHA-1 and SHA-2 CA root certificates, one for current operation and one in preparation for the SAL Concentrator cutting over to a SHA-2 identity certificate. The same applies for the certificates used for the SAL Policy Server-to-SAL Gateway connection.

For Customers:

A SAL Gateway is an important component of the Avaya support contract. It is the means by which Avaya delivers the services and service level objectives specified in the Avaya support contract. It is important for customers to take action to upgrade their gateways to avoid a disruption of service. Set a project target date of 1-Oct-2016 to accomplish this upgrade, instead of waiting until the end of the year. If not upgraded, Avaya will no longer be able to monitor product alarms, nor perform remote diagnostics on the products under coverage.

Customers are responsible for the SAL Gateway upgrade and any costs associated with it. Customers have the following options to upgrade the SAL Gateway:

1. Perform the upgrade yourself following product documentation.
    a. Those performing a software upgrade must be proficient in Red Hat Enterprise Linux or CentOS Linux, and Oracle JRE software installation and upgrade.
    b. In addition to the above, those performing an OVA upgrade must be proficient in VMware.
    c. Those performing an SVM upgrade must be proficient in System Platform administration.
2. Contact your account manager or channel partner to engage Avaya Professional Services to perform the upgrade. If you do not have an account manager or channel partner, please call (800) 852-2436 to engage APS directly.

Upgrade your SAL Gateway to the latest release, and apply the service pack containing the SHA-2 technology update.

Avaya has developed a playbook to assist with the upgrades outlined in the tables below.

SAL Gateway software on customer provided server and OS			
Starting Point	**Step 1**	**Step 2**	**SHA-2 Technology Update**
SAL GW 1.x	Upgrade to SAL GW 2.1	Upgrade to SAL GW 2.5	Apply ADS 2.5 SP3[1]
SAL GW 2.x	Upgrade to SAL GW 2.5		Apply ADS 2.5 SP3[1]

Note: SAL GW 2.5 is offered as part of the Avaya Diagnostic Server 2.5 package. The ADS 2.5 installation utility gives the customer the option to install only the SAL GW, or only the SLA Mon™ server, or both. Go to https://support.avaya.com/ads to download the ADS 2.5 software. See the ADS deployment guide for resource requirements and prerequisites.

[1]The latest release of SP3 is load 2.5.3.0-254. A previous release of SP3 had a different load number. If you installed the previous SP3 and your system shows 2.5.3.0-242 (see playbook for how to find this number), it is not necessary to install this SP3.

SAL Gateway on VMware OVA provided by Avaya			
Starting Point	**Step 1**	**Step 2**	**SHA-2 Technology Update**
SAL 2.2 OVA	Upgrade to ADS 2.0 OVA	Upgrade the software on this OVA to ADS 2.5	Apply ADS 2.5 SP3[1]
ADS 2.0 OVA	Upgrade the software on this OVA to ADS 2.5		Apply ADS 2.5 SP3[1]
SAL 2.5 OVA[2] for Avaya Aura 7 Appliance Virtualization Platform			Apply ADS 2.5 SP3[1]
Note: There is a VMware-managed upgrade path from the SAL GW 2.2 OVA to the ADS 2.0 OVA. *Note:* Avaya did not create a separate ADS 2.5 OVA, so the software on the ADS 2.0 OVA must be upgraded to ADS 2.5. Go to https://support.avaya.com/ads to download the ADS 2.0 OVA. See the VMware deployment guide for resource requirements and prerequisites. [1]The latest release of SP3 is load 2.5.3.0-254. A previous release of SP3 had a different load number. If you installed the previous SP3 and your system shows 2.5.3.0-242 (see playbook for how to find this number), it is not necessary to install this SP3. [2]The SAL 2.5 OVA for Avaya Aura 7 Appliance Virtualization Platform is a small capacity SAL Gateway that supports only 15 managed devices, analogous to the Services Virtual Machine on System Platform. It is intended for use only as a component of the Appliance Virtualization Platform, not as a standalone SAL Gateway.			

SAL Gateway on System Platform			
Starting Point	**Step 1**	**Step 2**	**SHA-2 Technology Update**
SAL GW 1.x on Sys Platform 1.x and 6.0.x	Recommended: Deploy a standalone SAL Gateway 2.5 with service pack 2 or later. SAL Gateway 1.x will be end of services support on Oct 1, 2016.		
	Optional: Upgrade System Platform and product template to 6.3.1 or later	Install Services Virtual Machine 3 (SVM3), which contains SAL GW 2.2	Apply SVM3 SP1[1]
SAL GW 2.1 on System Platform 6.2.x Services Virtual Machine 1	Upgrade SVM1 to SVM3 (does not impact the products on System Platform)		Apply SVM3 SP1[1]
SAL GW 2.2 on System Platform 6.3.0 Services Virtual Machine 2	Upgrade SVM2 to SVM3 (does not impact the products on System Platform)		Apply SVM3 SP1[1]
SAL GW 2.2 on System Platform 6.3.1+ Services Virtual Machine 3			Apply SVM3 SP1[1]
Note: Consult the System Platform compatibility matrix for details. Download the SVM3 software and the SVM3 documentation. *Note:* Customers who have multiple System Platforms with multiple SVM SAL Gateways in operation would be better served to consolidate to a standalone, full-scale SAL Gateway that manages all of the devices collectively. Installing a standalone, full-scale SAL Gateway may be an easier path even for customers with only one or two System Platforms. [1]The latest release of SP1 is load 3.0.1.0.2. A previous release of SP1 had a different load number. If you installed the previous SP1 and your system shows 3.0.1.0.1 (see playbook for how to find this number), it is not necessary to install this SP1.			

Avaya manages the certificates used between the SAL Concentrator and SAL Gateway, but the customer controls the optional certificates used between the SAL Policy Server and SAL Gateway. Do not load a SHA-2 CA root certificate onto any SAL Gateway until it receives the SHA-2 technology update. After a SAL Gateway receives the SHA-2 technology update, it is okay for that SAL Gateway to have both the SHA-1 and SHA-2 CA root certificates, one for current operation and one in preparation for the SAL Policy Server cutting over to a SHA-2 identity certificate. After a SAL Gateway receives the SHA-2 technology update, it is okay to install SHA-2 certificates in both the SAL Policy Server and SAL Gateway.

Workaround or alternative remediation*

None

Remarks
n/a

Patch Notes

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

Backup before applying the patch	
Recommended	
Download	
Per the tables above	
Patch install instructions	**Service-interrupting?**
See release notes included with software download	Yes
Verification	
See release notes	
Failure	
See release notes	
Patch uninstall instructions	
See release notes	

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.