Upgrading Secure Access Link (SAL) Gateway for SHA-2 Security Compliance

A Playbook for a Successful Upgrade

Issue: 1.7

Date: September 30, 2016

Table of Contents

1. Introduction and Purpose

This document is written to aid anyone (novice to expert) with the summary of steps and options for upgrading a Secure Access Link (SAL) Gateway (GW) on a customer premise. This playbook's intent is to compile information that has been previously provided into a summary that aids in more quickly finding various resources & collateral useful in the upgrade endeavor.

Knowing that the majority of the users of this document will use it many times, Section 2 gets right into how to do the various upgrade scenarios. If the reader is using this document for the first time, it is recommended to read Section 3 before Section 2.

This document is based upon the Product Support Notice (PSN004539u) which in July 2015 originally communicated the industry drive to a higher more secure version of digital certificates. These certificates, issued by Certificate Authorities (CAs) are used in authentication throughout the industry as well within the SAL infrastructure. 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 CA digital certificates. These digital certificates employ data encryption (specifically data authenticity) using a Secure Hash Algorithm (SHA).

SAL Gateways of earlier vintage are only capable of processing Secure Hash Algorithm 1 (SHA-1). The industry is moving away from SHA-1 to SHA-2. All Certificate Authorities stopped issuing SHA-1 certificates in Dec 2015. Existing SHA-1 certificates in the field are expected to expire by Dec 2016. 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 to support SHA-2 is taken.

Again, this document is written to compile available information and to help streamline the upgrade required (unique to each individual customer) including recommendations/options for upgrading the SAL Gateway to support SHA-2. Since the upgrade of the SAL Gateway is the remote connection, the upgrade process can only be performed locally as appropriate (not over a remote connection that will be lost during the upgrade). This is a "living document" and will be updated on the Avaya Support Web-Site (https://support.avaya.com) as new content becomes available. Please be sure to always check for the latest version.

If you have comments on improving this document or corrections please email alarmadmin@avaya.com and reference Upgrading Secure Access Link (SAL) for SHA-2 Security Compliance Playbook.

2. Context for the SAL Gateway SHA-2 Upgrade

The following sections are important context for those new to SHA-2 upgrades, but not something one will need to review for each upgrade.

A. Responsibility for the SAL Gateway SHA-2 Upgrade

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. Customer performs the upgrade themselves, following this guide and 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 a Services-VM upgrade must be proficient in System Platform administration.
2. Contact the Avaya account manager to engage Avaya Professional Services to perform the upgrade. If the customer does not know their account manager, may call +1 (800) 852-2436 to engage APS directly.
3. Contact an Avaya Authorized Business Partner to perform the upgrade. If the customer does not know their channel partner, please call +1 (800) 852-2436.

B. Value Proposition of SAL and Avaya Remote Connectivity

Establishing remote connectivity between a customer site and Avaya delivers significant value to both the customer, Avaya and business partners:

1. With Secure Access Link (SAL) in place, support requests are resolved 42% faster than when it is not present
2. When paired with EXPERT Systems^{SM}, customers are 73% more likely to avoid a system outage.
3. Enables Avaya to use automated diagnostic tools like Configuration Validation Tool (CVT) which gives Avaya and/or Partner the ability to quickly identify root cause and rely less on customers for troubleshooting.

To learn more about the value of SAL and Avaya remote connectivity, refer to these blogs and their embedded YouTube videos:

- Proactive Support: http://bit.ly/1MU22tc
- Connectivity: http://bit.ly/1OVBScN
- Alarming: http://bit.ly/1Z7yJtW
- SLA Mon^{TM}: http://bit.ly/1LR6Hty

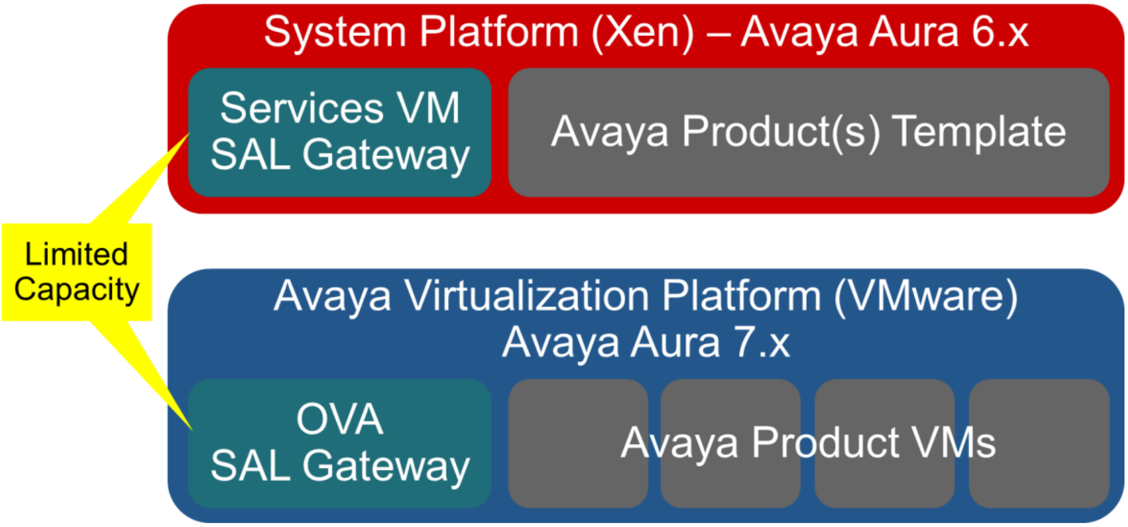
For Avaya associates and Business Partners, you may also consult the Enabling Healthy Remote Connectivity for Customers: An Account Team Playbook.

C. Standalone SALGW vs. System Platform based VSALGW

There are two types of SAL Gateways. The first is a standalone SAL Gateway, and it has a SE Code of “SALGW” (for definition of SE Code see Appendix A: Glossary). These gateways are deployed on their own instance of Linux, either on their own physical server or within a virtual machine (e.g. running under VMware). SALGWs can support up to 500 devices (SEIDs) and still perform appropriately. For most customer enterprises, use of SALGWs is the recommended solution.

The other type of SAL Gateway is the VSALGW. While the software application is the same, the deployment model is quite different. VSALGWs are part of the Avaya Aura System Platform architecture and have a very small footprint, limiting them to supporting only 15 managed elements (SEIDs).

As Avaya products move to the “Avaya Virtualization Platform”, the concept of a VSALGW will continue.


System Platform (Xen) – Avaya Aura 6.x
Services VM SAL Gateway
Avaya Product(s) Template
Limited Capacity
Avaya Virtualization Platform (VMware) Avaya Aura 7.x
OVA SAL Gateway
Avaya Product VMs

D. Software-only or VMware OVA

The standalone SAL Gateway software, as part of the Avaya Diagnostic Server bundle, is available in two deployment models.

1. Software only
    a. A server (physical or virtual) must be provided that meets the documented SAL Gateway requirements
    b. A supported version of Red Hat Enterprise Linux (RHEL) must be installed, along with other prerequisites
    c. SAL Gateway software is then installed in this environment
2. VMware OVA file
    a. For customers that use VMware virtualization, the OVA file may be deployed directly into VMware
    b. The SAL and Avaya Diagnostic Server OVAs include both the CentOS operating system and the SAL Gateway application.

E. Determining SAL Gateway deployment type thru swversion command

If you don't already know the type of SAL Gateway you have deployed, there is an easy way you can make this determination by displaying the software details of the software version command (swversion). Once you have obtained the IP address of your Secure Access Link Gateway (see Appendix A), perform the following steps.

- With the admin user, SSH into your gateway using ssh admin@<gateway ipaddress>
- Authenticate with the admin credentials.
- Switch to user root using the command 'su - root'
- Authenticate with the root credentials.
- Execute the command by typing 'swversion' at the command prompt.

The swversion command is available for the following SAL Gateway deployments:

- SAL OVA deployed on VMware or with Avaya's Appliance Virtualization Platform.
- SAL Embedded or Services-VM deployed on System Platform
- SAL deployed with the ION Appliance (SA5610-SAL and SA5600-SAL)

Note – The swversion command is not available with pre-version 2.5 Software Only deployment model (OS + SAL Gateway software application). It is however accurate to deduce a software-only install by the absence of this command (see case in the table below = swversion: command not found). See the table below for more details.

‘swversion’ Command Output	Deployment Type
VSP - Platform Information **===============================** **Version: 6.0.3.0.3 – 6.2.0.0.15** **OR** **System Platform Information – cdom** **==================================** **Version 6.3.0.0.18002**	System Platform (Embedded or Services-VM)
SAL Gateway Product Version: 2.x.x.x.x **OR** **SAL Gateway Version: 2.x.x.x**	SAL OVA (VMware or AVP)
[root@npse-salgw-sv ~]# swversion **-bash: swversion: command not found**	Software Only (Customer owned Hardware)

F. Finding the SAL Version by logging into the SAL Gateway Web UI or command-line

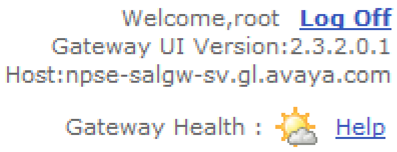
Before you can confirm the version details of your SAL Gateway you must first locate its IP address. Please ask your network administrator for the IP address of your SAL Gateway or obtained the IP address of your Secure Access Link Gateway (see Appendix A).

If you determined that your deployment type was a SAL OVA from the previous section, it is possible to skip directly to Section 6 and refer to output of the swversion command as that is your SAL Gateway version. For all other deployment types (Software-Only, System Platform), please continue with the following:

Once you have your Secure Access Link Gateway IP address, there are two ways of confirming your SAL Gateway version (all deployment types): using the Web User Interface or command-Line. Either method is effective, but both are listed here as users often have their own preference.

Web User Interface (UI):

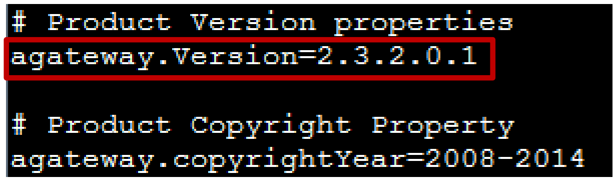
- With the root user, log into your gateway using the following URL https://<gw-ipaddress>:7443.
- From the home page on the top right of the screen you will see your SAL Gateway’s version
- For example, 2.3.2.0.1 in the screenshot below



Welcome,root Log Off
Gateway UI Version:2.3.2.0.1
Host:npse-salgw-sv.gl.avaya.com
Gateway Health : Help

Command Line Interface (CLI):

- Authenticate into the SAL Gateway host as "root"
    - E.g., SSH into your SAL Gateway using ssh <non-root user>@gw-ipaddress.
    - Switch to root user: su -root
- Execute the following command
    - `cat /opt/avaya/SAL/gateway/GatewayUI/config/agentgateway.properties`
- Note - If the SAL Gateway is installed in a different directory than the default, you can still locate this file using the following command:
    - find / -name agentgateway.properties
- From the output, look for the following line agateway.Version=2.3.2.0.1



```
# Product Version properties
agateway.Version=2.3.2.0.1

# Product Copyright Property
agateway.copyrightYear=2008-2014
```

G. SAL Gateway Versions ready for SHA-2

When the version number is identified it will come in the form of a numbering scheme that is formatted as X.y.a.b.c (e.g. 2.5.2.0.6) where:

- X – represents the Major version of the software
- y – represents the minor version of the software
- a – represents the service pack level applied (for the SHA-2 effort this deepest level of the version string which Is useful in determining SHA-2 readiness)
- b & c - representing patch and build information that for the purposes of this SHA-2 effort are not incrementally informational

The following table shows which versions are SHA-2 compliant:

Version	System Platform	SHA-2 Compliant	Notes
1.8.0.0.74	Possible	No	1.x will be End of Services Support (EoSS) on October 1st, 2016
2.1.0.0.38	Possible	No	
2.2.0.0.25	Possible	No	
2.2.2.0.1	This software version is only on System Platform	Yes	Yes, 2.2.2 is the version for VSALGW that supports SHA-2. It is numbered 2.2.2 and not 2.5+ as it's a derivate on VSALGW (System Platform) that does not have a path to 2.5
2.3.2.0.1	N/A	No	While more than 2.2.2 this is a SALGW which must be of version 2.5.2 and greater
2.5.1.0.5	N/A	No	
2.5.2.0.6	N/A	Yes	The 1st version of the SALGW software that supports SHA-2
2.5.3.0.4	N/A	Yes	Service Pack 3 for SALGW

When software-only or OVA based SAL Gateway (SE Code of "SALGW") is updated to support SHA-2 it will report its version as v2.5.2 or greater (note that today there is a 2.5.3 which is 2.5 with Service Pack #3).

When a Services-VM on System Platform based SAL Gateway (SE Code of "VSALGW") is updated to support SHA-2 it will report its version as v2.2.2.x. There is no planned upgrade path on System Platform to Avaya Diagnostic Server / SAL Gateway 2.5.

H. Determining the IP address of your SAL Gateway so you can login

Before you can confirm the deployment details of your Secure Access Link (SAL) Gateway, you must first locate its IP address. Please ask your network administrator for the IP address of your SAL Gateway.

If you are still unable to get the IP address of your Secure Access Link Gateway from your network administrator and are unsure where to begin, here are a few other suggestions that should help.

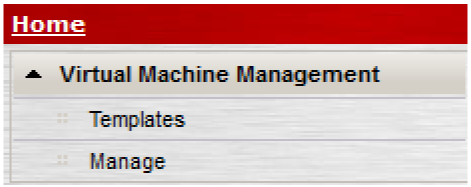
1. Reference other Avaya applications

Log into any of your Avaya applications that you are familiar with and that you know alarm (i.e. AES, CM, System Manager), then check the NMS or alarming configuration there. If these applications are configured with an IP address this is very likely the SAL Gateway IP.

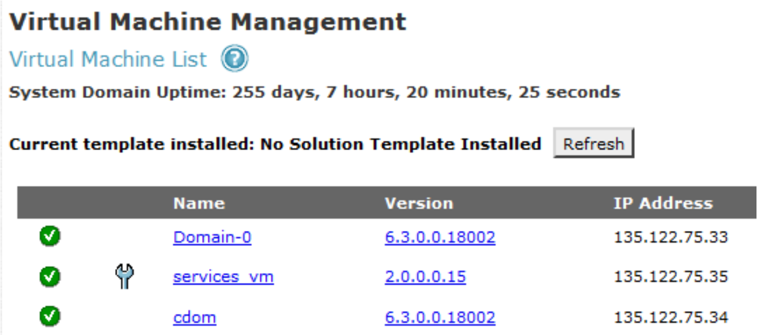
2. Use VSPU/CDom for a VSALGW

If you suspect that you are using a VSALGW on System Platform and know the IP address of the VSPU/CDom Web Console, you can make the determination from there

2.1. Log into your System Platform Web Console using the following URL https://<System Platform CDom IP>/webconsole.
2.2. Authenticate using the admin user and password credentials.
2.3. On the left navigation pane, click on 'Virtual Machine Management → Manage



2.4. If you are running the Service Virtual Machine, you will see a line entry and IP address for your



Virtual Machine Management

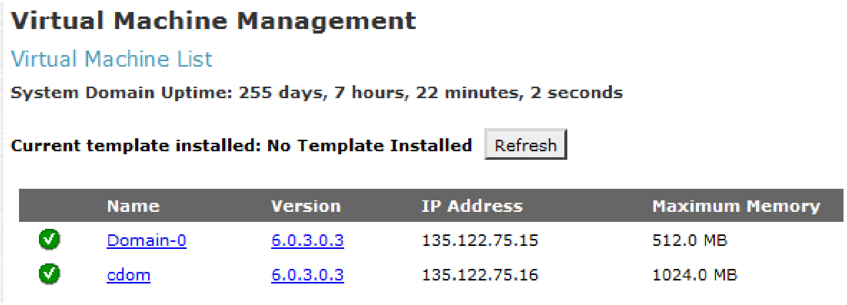
Virtual Machine List

System Domain Uptime: 255 days, 7 hours, 20 minutes, 25 seconds

Current template installed: No Solution Template Installed Refresh

		Name	Version	IP Address
✓		Domain-0	6.3.0.0.18002	135.122.75.33
✓	🔧	services_vm	2.0.0.0.15	135.122.75.35
✓		cdom	6.3.0.0.18002	135.122.75.34

2.5. If however, you are still running the embedded Secure Access Link Gateway, then you will not see a separate line for Services VM as the IP address of your VSALGW is that of your cdom line. This would be applicable to any version of System Platform 6.0.



Virtual Machine Management

Virtual Machine List

System Domain Uptime: 255 days, 7 hours, 22 minutes, 2 seconds

Current template installed: No Template Installed

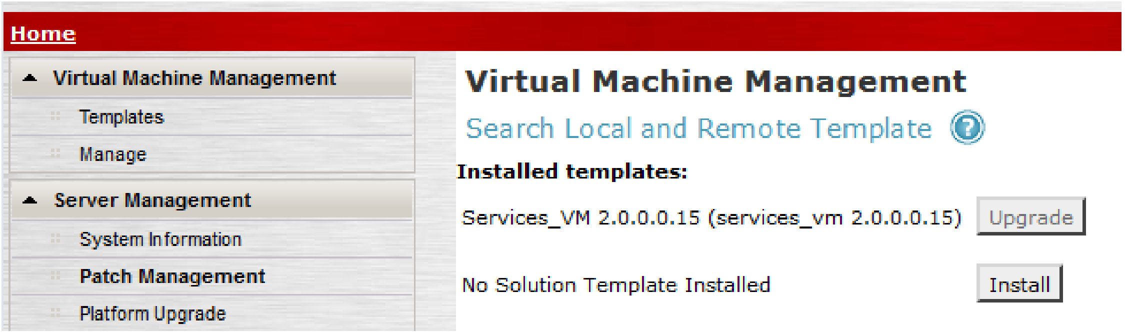
	Name	Version	IP Address	Maximum Memory
✓	Domain-0	6.0.3.0.3	135.122.75.15	512.0 MB
✓	cdom	6.0.3.0.3	135.122.75.16	1024.0 MB

I. Finding the Services Virtual Machine (Services-VM) version

If the user is interested in the specific version of Services-VM, the most direct method of determining the version of Services-VM (aka SMV or Services Virtual Machine) is to.

1. Log on to the System Platform Management Console

2. Click Virtual Machine Management then Installed Templates



Virtual Machine Management

Search Local and Remote Template

Installed templates:

Services_VM 2.0.0.0.15 (services_vm 2.0.0.0.15)

No Solution Template Installed

3. If this is a VSALGW on System Platform and you know the SAL Gateway version

If the SAL Gateway version is known and it is known that the implementation is on an Avaya appliance managed by System Platform the following may be useful. Again directly logging into System Platform Console is preferred, but if the user is having difficulty logging into System Platform the following table is useful in defining Services-VM version knowing the SAL version:

SAL Gateway Version	Services-VM version	System Platform Version
2.1.0.0.38	Services-VM 1.0	6.2.0.0.27 – 6.2.2.09001.0
2.2.0.0.25	Services-VM 2.0	6.3.0.0.18002 – 6.3.8.01001.0
2.2.0.0.26	Services-VM 3.0	An upgrade path originally used on 6.3.1+

4. Service Pack Versioning

Note patches could have been applied for a higher SAL Gateway version number on the same Services-VM version. The above table only includes reference versions for the original install and version – which is 80+% of the field cases. The below table has a few of the SAL Gateway versions with Service Packs that could be found in an Services-VM (it is not a comprehensive list but examples)

SAL Gateway Version with Service Pack	Services-VM version
2.1.2.2.2	Services-VM 1.0 with Service Pack
2.2.1.0.2	Services-VM 2.0 with Service Pack
2.2.2.0.4	Services-VM 3.0 with Service Pack

J. Determining Operating System Version to determine if OS upgrade is also required

This is exclusively important in the software-only SAL cases where the customer owns the operating system and is recommended to upgrade and care for the OS. It is recommended that the customer upgrade to a RHEL 6.x to stay current with the industry and ease future updates and upgrades.

The next major release of SAL Gateway will run on RHEL 6.x and later, so an OS upgrade will be required from 2.5 to 3.x if not done now.Also know this planning allows the customer to employ the sw-auto-update feature to upgrade/update to the future Avaya Diagnostic Server 3.0.

RHEL 5.x is also 3.5 years behind RHEL 6.x in Red Hat's lifecycle process. You can read more about the current lifecycle status and dates for RHEL 5.x at (link).

Please use the following steps to determine your Operating System Version

1. Locate the IP address of your SAL Gateway

2. SAL Gateways 2.2 and earlier

- `cat /etc/redhat-release or uname –a`
- `Red Hat Enterprise Linux Server release 6.6 (Santiago)`
- `Linux npse-salgw-sv.gl.avaya.com 2.6.32-504.3.3.el6.i686`
- `#1 SMP Fri Dec 12 16:06:14 EST 2014 i686 i686 i386 GNU/Linux`

3. SAL Gateways 2.3 and later

- `cat /etc/redhat-release or uname –a`
- `Red Hat Enterprise Linux Server release 6.7 (Santiago)`
- `Linux ve-avaya-sa 2.6.32-573.8.1.el6.x86_64 #1 SMP Fri Sep 25`
- `#1 SMP Fri Sep 25 19:24:22 EDT 2015 x86_64 x86_64 x86_64 GNU/Linux`

K. Special consideration for Redundant SAL Gateways

Redundancy is supported between two SAL Gateways that are of the same version. You can upgrade the redundant SAL Gateways one by one without affecting the redundancy configuration. After both SAL Gateways upgrade to the latest version, the redundancy feature works as expected.

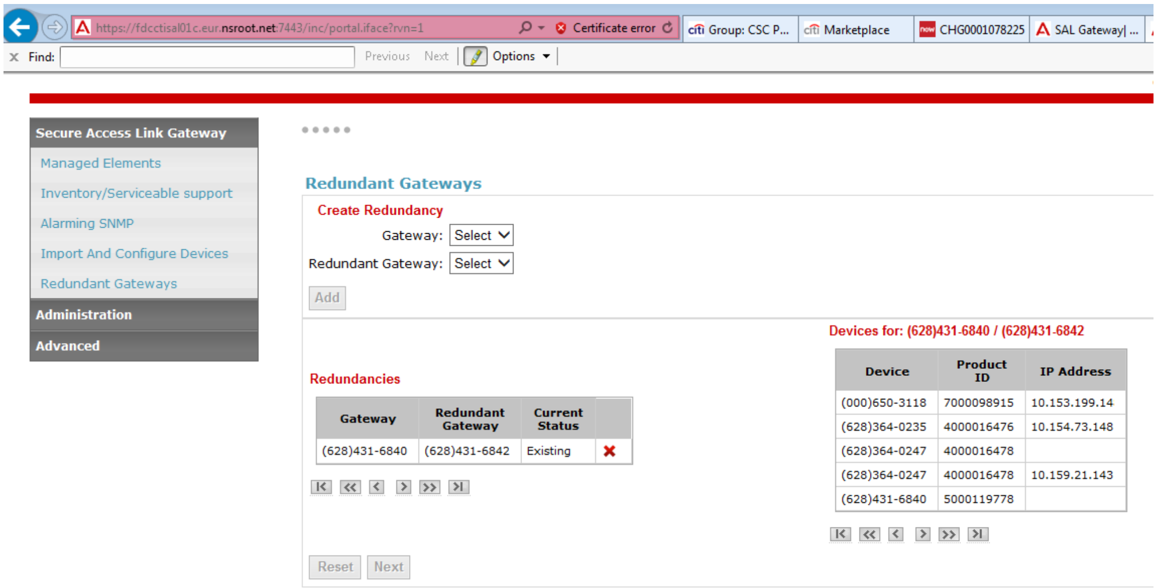
During the timeframe when you upgrade one SAL Gateway yet the second is not started, the managed element synchronization between the two SAL Gateways might not happen. However, alarm transfer, remote access, and other functionalities remain available through the second SAL Gateway that participates in redundancy.

When one of the gateways in redundant pair has been upgraded, care must be taken that configuration related to managed elements is not changed on any of the gateway since it may result in the mismatch of the data on the redundant pair.

It is recommended to upgrade the second gateway of the redundant pair as soon as the first gateway is upgraded to not have any synchronization issues in the pair.

In order to check that the gateway is redundant to another gateway, please follow below steps:

1. **Login into the SAL Gateway UI using https://<sal-gateway-ipaddress>:7443**
2. **Authenticate with the root user and password**
3. **Click on 'Redundant Gateways' link on the left menu**
4. **If Existing Redundant SAL Gateway**
   If the redundant gateways page appears and this gateway's SEID appears in the Redundancies table with the status as 'Existing' then the gateway is redundant to another gateway mentioned in the table. As shown below:



Redundant Gateways

Create Redundancy

Gateway: Select

Redundant Gateway: Select

Add

Redundancies

Gateway	Redundant Gateway	Current Status	
(628)431-6840	(628)431-6842	Existing	✖

Devices for: (628)431-6840 / (628)431-6842

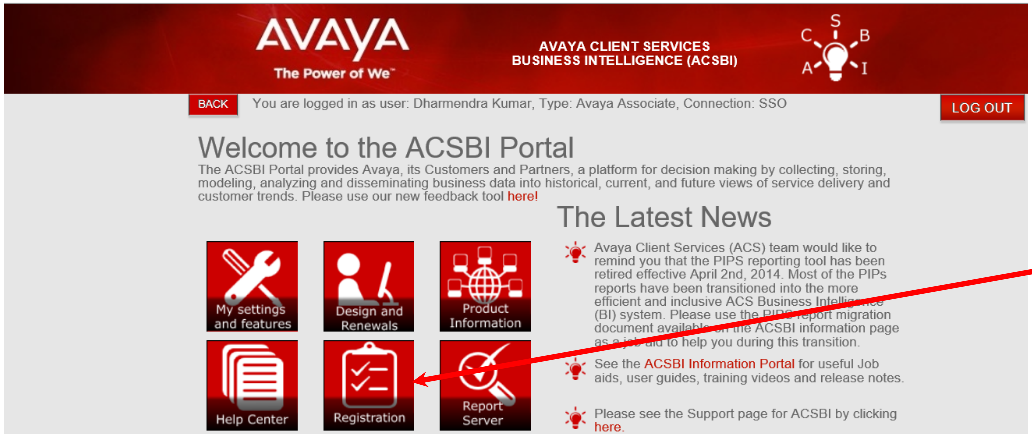
Device	Product ID	IP Address
(000)650-3118	7000098915	10.153.199.14
(628)364-0235	4000016476	10.154.73.148
(628)364-0247	4000016478	
(628)364-0247	4000016478	10.159.21.143
(628)431-6840	5000119778	

Reset Next

L. Looking up a Functional Location (FL) number (a.k.a. SoldTo number)

If you don't know your Avaya Functional Location (FL) number (a.k.a. SoldTo number), then you may find out using Avaya ACSBI reporting Tool.

1. **Visit https://acsbi.avaya.com using SSO login/password**
2. **From the home page Click on Registration**



You are logged in as user: Dharmendra Kumar, Type: Avaya Associate, Connection: SSO

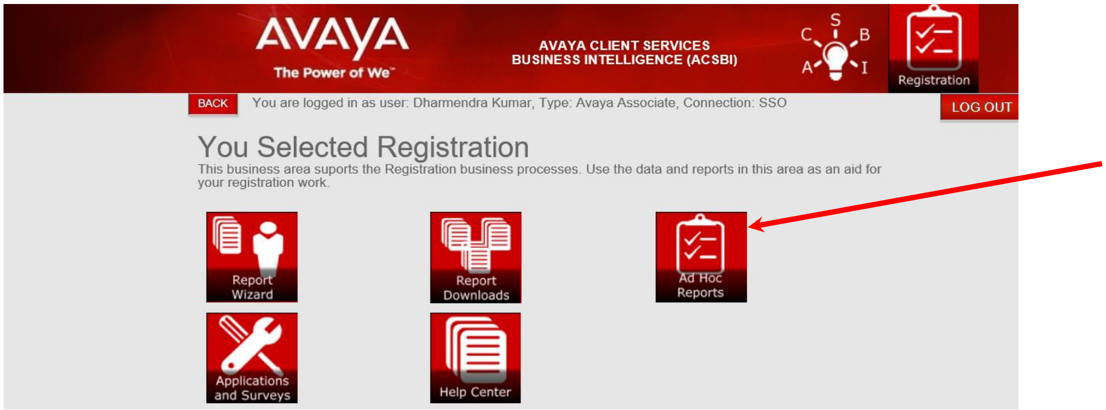
Welcome to the ACSBI Portal

The ACSBI Portal provides Avaya, its Customers and Partners, a platform for decision making by collecting, storing, modeling, analyzing and disseminating business data into historical, current, and future views of service delivery and customer trends. Please use our new feedback tool here!

The Latest News

- Avaya Client Services (ACS) team would like to remind you that the PIPS reporting tool has been retired effective April 2nd, 2014. Most of the PIPs reports have been transitioned into the more efficient and inclusive ACS Business Intelligence (BI) system. Please use the PIPS report migration document available on the ACSBI information page as a job aid to help you during this transition.
- See the ACSBI Information Portal for useful Job aids, user guides, training videos and release notes.
- Please see the Support page for ACSBI by clicking here.

3. Click on the Ad Hoc report and check SEID report box



You are logged in as user: Dharmendra Kumar, Type: Avaya Associate, Connection: SSO

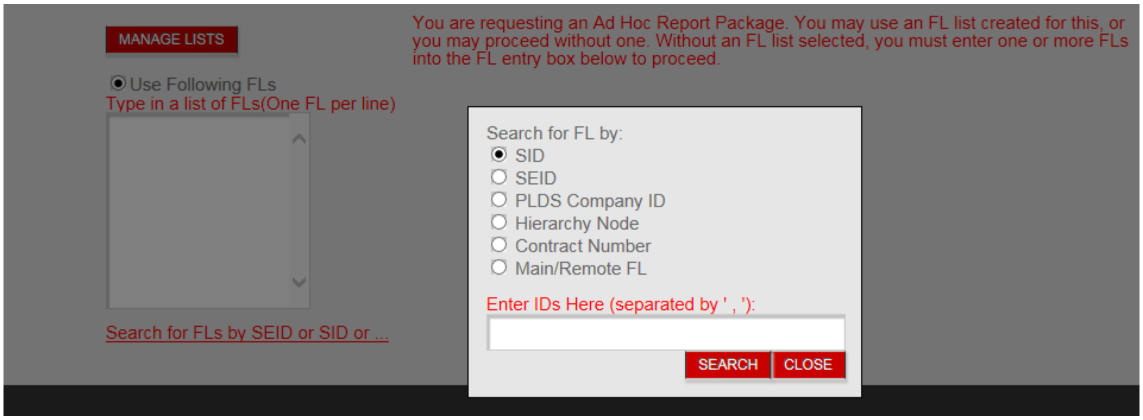
You Selected Registration

This business area suports the Registration business processes. Use the data and reports in this area as an aid for your registration work.

4. Click Next

5. Click on Search for FLs SEID or SID …

6. Search by SID, SEID, PLDS Company ID, Hierarchy Node, Contract Number or Main/Remote FL



You are requesting an Ad Hoc Report Package. You may use an FL list created for this, or you may proceed without one. Without an FL list selected, you must enter one or more FLs into the FL entry box below to proceed.

● Use Following FLs

Type in a list of FLs(One FL per line)

Search for FL by:

- ● SID
- ○ SEID
- ○ PLDS Company ID
- ○ Hierarchy Node
- ○ Contract Number
- ○ Main/Remote FL

Enter IDs Here (separated by ' , '):

M. Special considerations for ION appliance

API Tech, an Avaya DevConnect Partner, provides ION™ SA5610-SAL Avaya® SAL Edition Secure Appliance. This document treats ION™ SA5610-SAL as software-only. API Tech also has the following link for guidance, which includes the specific instructions for an ION upgrade (link).

N. Special considerations for an overloaded VSALGW

Please be advised that a VSALGW (SAL Gateway that is implemented on System Platform) is considered overloaded if the VSALGW contains more than 15 manage elements.

If more than 15 manage elements are connected to the VSALGW, the performance of that GW is adversely affected in the following ways:

- The # of alarms per second / per minute goes up, which increases the load on the gateway.
- The # of simultaneous connections has the potential to go up, which increases the load on the gateway.
- Every start/stop of the agent will require reading of XML files to load the manage element data, and the higher the number of managed elements the greater the load on the gateway.
- Onboarding, inventory, and other functions (some of which are initial, one-time functions) will put a greater load on the gateway with a larger number of managed elements.
- There will be a greater load on the gateway UI (longer web page load time) having to load the data for a larger number of managed elements.
- There are other internal processes that will be impacted by having a larger number of managed elements administered.
- Not only does the performance of the gateway suffer, but it is also possible that the VSALGW will lose full connectivity when the gateway is overloaded.

Recommended Action:

It is therefore highly recommended and encouraged that you migrate any VSALGW manage elements to an existing stand-alone SAL GW, or deploy a new SAL GW where you can consolidate all of your System Platform solution applications. The standalone SAL Gateway is specifically designed to handle a larger capacity of managed elements. See this link to learn more about the hardware specifications for a VMware or software standalone gateway.

The process of migrating VSALGWs to an existing stand-alone SALGW, or deploying a new SALGW where you can consolidate all of your System Platform solution applications is documented in this document in Sections 2.A – 2.D.

O. Remote Agent Push Details

The SAL Gateway upgrade process to support industry standard SHA-2 program has been advertised for a significant amount of time, and the PSN was released in July of 2015 (link). As of July 2016, the current trend of the progress being made for manual upgrades does not forecast the pre-established goal of 100% compliance by October 1, 2016 being met. As a result, Avaya has been exploring other avenues in order to ensure customers and partners don't experience a service disruption in January 2017.

What is the Remote Agent Push?

Avaya was able to develop a script that will remotely update the agent software inside version 2.x SAL Gateways, making the gateway SHA-2 compliant. Avaya will begin utilizing this remote agent push on October 3, 2016 with intention of meeting the 100% compliance mark sooner. This also off-loads work on many organizations and allows them to focus on the SAL GW version 1.x which will be End of Support Oct 1, 2016.

Special Considerations

If customers would like to be remotely upgraded via the remote agent push earlier than October 3, please fill out the "Early Adopters Form" and return it to earlyadopters@avaya.com by September 9, 2016.

If customers would like to avoid the remote agent push altogether, then they must submit the "Opt Out Form" and return it to optoutSHA2push@avaya.com by September 30, 2016. Otherwise beginning Oct 3, 2016 Avaya will begin the remote agent update program with no specific window management of the update. Avaya will perform the operation remotely between October 3 and Nov 18, 2016. Success or failures will be communicated to you the partner for manual upgrade follow-up as required.

For general questions regarding the remote agent push please contact SHA2Compliance@avaya.com

How is this different than the manual upgrade?

Please be aware this is not the preferred method of upgrade. Consult the PSN to learn more about the key differences.

Timeline

The Remote Agent Push will begin on Oct, 3 2016, and planned to last through November 18, 2016. Once the remote agent push has been tried, those remaining 2.x gateways that were not successfully updated will have the remaining time for a manual upgrade. Those failures for partner supported customers and gateways will be communicated as soon as they are known.

P. ACSBI SHA2 Readiness Report

The ACSBI *SHA-2 Readiness Report* allows those with an Avaya Single Sign-On (SSO) username and password to quickly view all of their account or customer gateways, and whether or not those gateways are SHA-2 compliant. By using this report, account managers, business partners, and customers can take proactive steps in upgrading the needed SAL Gateways to SHA-2 Compliant versions.

If you do not have a Single Sign –On, use Chapter 3 of the following document to obtain one (link)

Accessing the SHA2 Readiness Report

- Login to ACSBI at https://acsbi.avaya.com using your Avaya user SSO username and password.
- Click on the "Registration" icon on the ACSBI Landing Page.
- Click on "Ad Hoc Reports" icon on "You Selected Registration" page.
- Check the check box beside "SAL GW SHA-2 Readiness Report" to select it, and click "Next".

A full user guide is avaible (link)

Q. Index of Avaya Mentor YouTube video resources

Avaya has made many videos available on YouTube that walk through a variety of relevant implementation and configuration steps related to SAL Gateways. Below is an index of those videos.

Avaya Diagnostic Server videos:

- How to Retire an Avaya SAL Gateway on System Platform (VSALGW)
- How to Upgrade a SVM1 (VSALGW 2.1 on System Platform): Scenario M
- How to Upgrade a SVM2 (VSALGW 2.2 on System Platform): Scenario N
- How to Upgrade a SVM3 (VSALGW 2.2 on System Platform): Scenario O
- How to perform a SAL VE 1.0 Migration to Avaya Diagnostic Server 2.0
- How to Install the Avaya Diagnostic Server 2.0 using the Attended Mode
- How to Install the Avaya Diagnostic Server 2.0 Virtual Appliance
- How to Edit and Validate the ADS 2.0 unattended install ADS_Response.properties file
- How to perform an unattended upgrade or migration to Avaya Diagnostic Server 2.0
- Automatic Software Update Feature for Avaya Diagnostics Server 2.0
- How to Install the Avaya Diagnostic Server 2.0 using the Unattended Mode
- How to trigger an Avaya Diagnostic Server software update through command line in unattended mode
- Performing a Secure Access Link Gateway Silent Installation and Upgrade
- Disabling your Avaya System Platform Secure Access Link Gateway
- How to Add a Managed Element to a Secure Access Link Gateway

Secure Access Link ION videos

- How to Connect and Setup the ION SA5600-SAL - Avaya SAL Edition Secure Appliance
- How to Configure and Initialize the ION SA5600-SAL Avaya SAL Edition Secure Appliance
- How to Enable SSH for the ION SA5600-SAL - Avaya SAL Edition Secure Appliance
- How to Add a Managed Element to a Secure Access Link Gateway

3. Upgrade Scenarios

Use the simplified chart below to determine which set of following instructions to follow:

Upgrade Scenario	Current SAL Gateway	New SAL Gateway
A	Any SAL Gateway	An existing SAL Gateway 2.5.2
B	Any SAL Gateway	A new Software-only 2.5.2
C	Any SAL Gateway	A new OVA SAL Gateway 2.5.2
D	Any SAL Gateway	A new ION SAL Gateway 2.5.2
E	Software-only 1.x	Software-only 2.5.2
F	Software-only 2.0, 2.1, or 2.2	Software-only 2.5.2
G	Software-only 2.3.x, 2.5.0, or 2.5.1	Software-only 2.5.2
H	SAL Gateway 2.2 OVA	SAL Gateway OVA with SAL Gateway 2.5.2
I	SAL Gateway 2.2 OVA	ADS OVA with SAL Gateway 2.5.2
J	ADS 2.0 OVA	ADS OVA with SAL Gateway 2.5.2
K	OVA SAL Gateway 2.5 OVA for AVP	ADS OVA with SAL Gateway 2.5.2 for AVP
L	System Platform 1.x and 6.0.x VSALGW 1.x	A new or existing SAL Gateway 2.5.2
M	SVM1 (System Platform 6.2.x VSALGW 2.1)	SVM3: System Platform VSALGW 2.2.2
N	SVM2 (System Platform 6.3.0 VSALGW 2.2)	SVM3: System Platform VSALGW 2.2.2
O	SVM3 (System Platform 6.3.1+ VSALGW 2.2)	SVM3: System Platform VSALGW 2.2.2
P	Any ION SAL Gateway Appliance	ION SAL Gateway Appliance 2.5.2

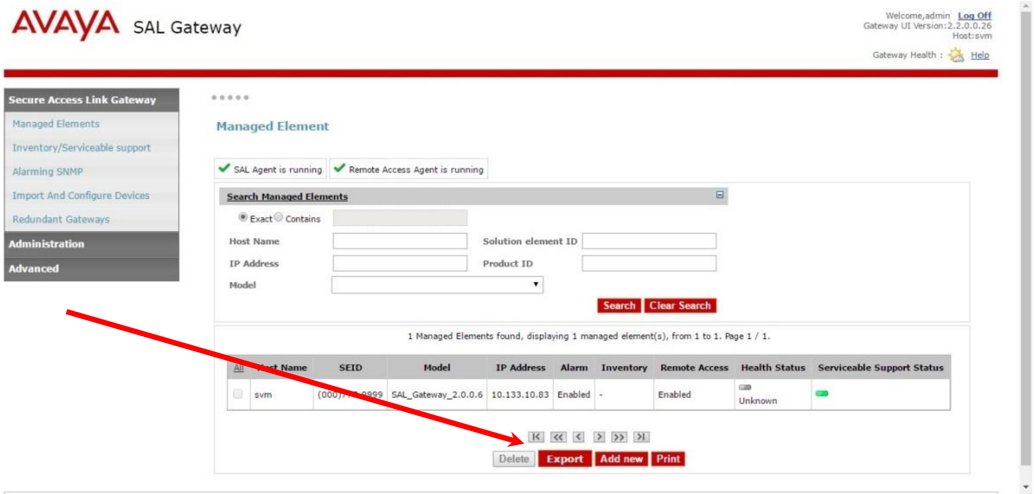
A. Retire existing SAL Gateway and migrate managed elements to an existing SAL Gateway

If you have an existing SHA2-compliant SAL Gateway, you may choose to simply migrate all your managed elements from an existing non-SHA2-compliant SAL Gateway to the SHA2-compliant one.

1. Export Managed Elements List

In addition to backing up your SAL Gateway, it is highly also advised that you export a copy of all of your Managed Elements from the SAL Gateway UI. This will provide you with a list of all of your Solution Element IDs and Alarm IDs needed in the event you need to re-administer any of your devices manually.

1.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
1.2. Authenticate with the admin or root user and password
1.3. On the bottom of the Managed Element page click on the ‘Export’ button

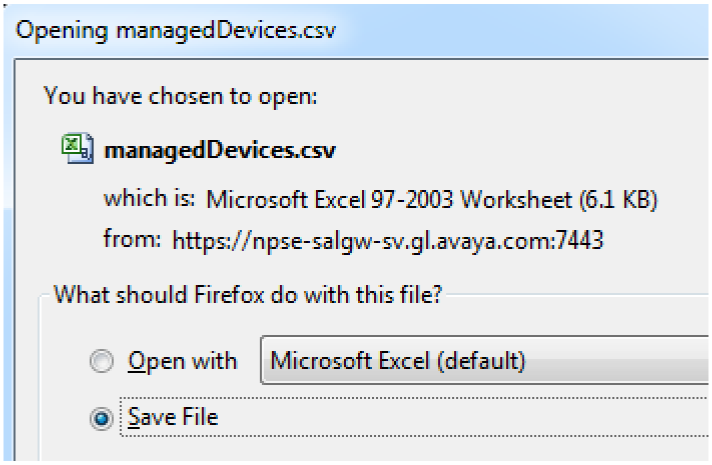


✓ SAL Agent is running ✓ Remote Access Agent is running

1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)7[illegible]9999	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

1.4. A dialogue window will appear where you can save the .CSV file.



Opening managedDevices.csv

You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

2. Access the going-forward SAL Gateway

Obtain credentials and access the target consolidation SAL Gateway to migrate your existing SAL Gateway managed elements.

3. Manually add the Managed Elements to the new SAL Gateway

Using the data within the CSV file you obtained from the original/source SAL Gateway (SAL Gateway from which the managed elements are being migrated), administer all of these elements, one by one, onto the target consolidation SAL Gateway by following this how-to video (link).

4. Technically Onboard the migrated managed elements in the Global Registration Tool (GRT)

Once the managed elements are added successfully into target consolidation SAL Gateway, then user would login into GRT and submit a connectivity & alarming request to check the managed elements on the SAL Gateway. These devices would have been previously technically onboarded, but will need to go through this process again to validate connectivity and alarming are working through the new SAL Gateway.

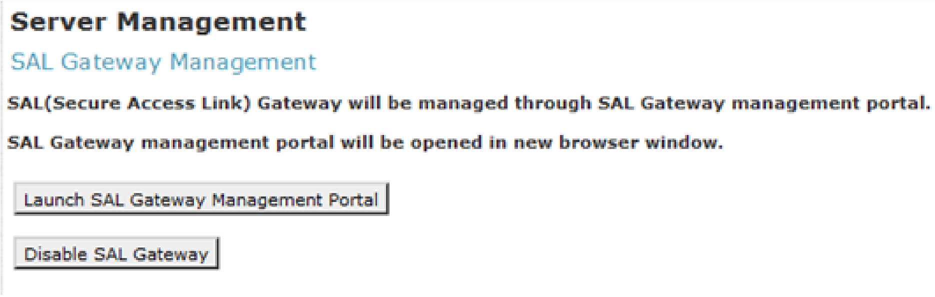
4.1. Log on to https://grt.avaya.com
  4.1.1. Create a new Technical On-Boarding connectivity & alarming retest request for all of the managed elements migrated to the new SAL Gateway. A video is available (link).
  4.1.2. Enter Sold To
  4.1.3. Click on existing registered assets list
  4.1.4. Find the SEID to be migrated
  4.1.5. Click on Re-Test
  4.1.6. Select the check box for “Test Remote Access” and “Test Alarming” (the latter is only available if the device is entitled and eligible for alarming)
  4.1.7. Then click on “Submit”
4.2. GRT will test connectivity & alarming, and if it fails due to any reason then a Service Request (SR) will be created for the SAL Technical Onboarding team. If required, the SAL Technical Onboarding team will address the SR.
4.3. Repeat for each SEID individually
4.4. Please Join Ava Chat at https://support.avaya.com, if you have any questions related to the GRT registration or the SAL Technical Onboarding process.

5. For a software-only or OVA SAL Gateway only – Decomission the old SAL Gateway

5.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
5.2. Authenticate with the admin or root user and password
5.3. Select all the Managed Elements by clicking the “all” selector
5.4. Click the Delete button to remove all the Managed Elements from this SAL Gateway
5.5. Restart the SAL Agent and Remote Access Agent within the SAL Gateway UI in order to apply these changes
5.6. Shutdown the SAL Gateway application
5.7. Login to the Global Registration Tool (https://grt.avaya.com)
5.8. Remove the SAL Gateway record using the “Record Validation” process. The following YouTube video shows this (link).

6. For a VSALGW (on System Platform) only - Decommission the old SAL Gateway

6.1. In addition to these written steps, a video exists showing how to do this (link)
6.2. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
6.3. Authenticate with the admin or root user and password
6.4. Select all the Managed Elements by clicking the “all” selector
6.5. Click the Delete button to remove all the Managed Elements from this SAL Gateway
6.6. Restart the SAL Agent and Remote Access Agent within the SAL Gateway UI in order to apply these changes
6.7. Skip steps 6.8, 6.9, and 6.10 if on System Platform 1.x
6.8. Login into the System Platform Console Domain with the ‘admin’ user.
6.9. On the left navigation pane under ‘Server Management” click on ‘SAL Gateway Management’.
6.10. Click on the ‘Disable SAL Gateway’ button.



Server Management

SAL Gateway Management

SAL(Secure Access Link) Gateway will be managed through SAL Gateway management portal.

SAL Gateway management portal will be opened in new browser window.

6.11. After disabling the SAL Gateway on System Platform, please deactivate the SEID associated with the original VSALGW by taking the following steps:

- **Customers:** Call Avaya IT. In the US 1-866-AVAYA IT, option 1, or 2. If you are not in the US, to obtain the number for other countries, visit https://support.avaya.com/contact and specify your country. During the phone call to AVAYA-IT ensure that you provide the SEID number for the SALGW to be deactivated.
- **Partners and Distributors:** submit an ITSS ticket www.avaya.com/partner-itss > Report an incident > Corporate Applications > support.avaya.com > In “Brief Description” enter VSALGW identified by SEID to be made Inactive
- **Avaya Associates:** Submit an ITSS ticket https://itss.avaya.com > request a service > applications supporting services > Siebel GCT > Data Assistance > Asset in Siebel Not in GRT. Ensure that you provide the SEID number for the SALGW to be deactivated.

B. Retire existing SAL Gateway and migrate managed elements to a new software-only SAL Gateway

The following steps explain how to get a new software-only SAL Gateway 2.5.2 installed and configured and then migrate an existing SAL Gateway to this new SAL Gateway.

1. Ensure proper network paths are open for the new software-only SAL Gateway

When deploying a new SAL Gateway into your environment, you’ll need to make sure that there are no firewall restrictions within your network for the new SAL Gateway, either restricting outbound access on HTTPS port 443 from the SAL Gateway (egress), or internally on UDP port 162 from your managed elements to the SAL Gateway (ingress).

The SAL Gateway uses port 443 outbound to communicate with the Avaya or Business Partner Secure Access Link Concentrator Servers for both alarm delivery and remote access connections. The specific ports and Avaya URLs are defined on page 11 of this linked Port Matrix document (link).

2. Register the new SAL Gateway with Avaya

When deploying a new SAL Gateway it will be necessary to register the SAL Gateway with Avaya which can be done either prior to the installation or automatically during an attended installation.

It is possible to use the Automatic Registration feature during SAL Gateway Installation during an attended UI installation to auto-generate the SEID & Alarm ID for the new SAL Gateway:

2.1. Use the *Deploying Avaya Diagnostic Server* section on Automatic Solution Element ID generation through the SAL Gateway UI (link)
2.2. Follow Pre-install task 16 from *Deploying Avaya Diagnostic Server* (link)

Otherwise, use the GRT Registration Process for the new SAL Gateway and it’s SEID & Alarm ID. See the following references:

2.3. Registering SAL Gateway generating the SIED & Alarm ID prior to installation (link)
2.4. Or use the KB article if an Avaya SSO Login available (link)
2.5. Once you received the SEID & Alarm ID of the newly registered SAL Gateway then save these numbers as they will be administered into the SAL GW during the SAL Gateway installation

3. Download the SAL Gateway software

- Avaya Diagnostic Server / SAL Gateway 2.5 (link)
- Avaya Diagnostic Server / SAL Gateway 2.5 Service Pack 3 (link)
- The software file should be already be downloaded on the SAL Gateway due to the Avaya Diagnostic Server software automatic update feature (link) or download the software again if needed

4. Deploy the new Software-only SAL Gateway

Deploy your new software-only SAL Gateway in the either the ***unattended*** mode or ***attended*** mode.

Unattended mode:

4.1. Edit and Validate the Avaya Diagnostic Server 2.0 unattended install ADS_Response.properties file (link)
4.2. Install the server in unattended mode (link)

Attended mode:

4.3. Install the server in attended mode (link)

For both modes:

4.4. Be sure to set up proper credentials. The Linux server administrator must have root credentials, and the SAL Gateway administrator must have a Linux account with SAL administrative privileges.

5. Apply Avaya Diagnostic Server 2.5 Service Pack 3

Instructions (link)

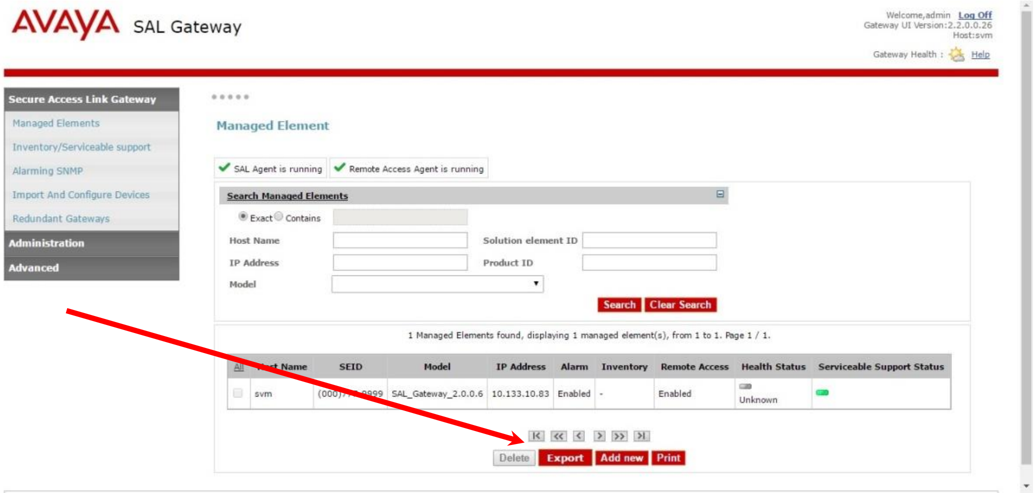
6. Additional Security Configuration

If required per the customer's specific installation, perform any OS-related configuration or hardening according to the instructions provided here (link).

7. Export Managed Elements List from old SAL Gateway

On the existing SAL Gateway use the following steps to obtain the CSV file of the existing managed elements to be migrated to the new software-only SAL Gateway

7.1. Login into the old SAL Gateway UI using https://sal-gateway-ipaddress:7443
7.2. Authenticate with the admin or root user and password
7.3. On the bottom of the Managed Element page click on the 'Export' button

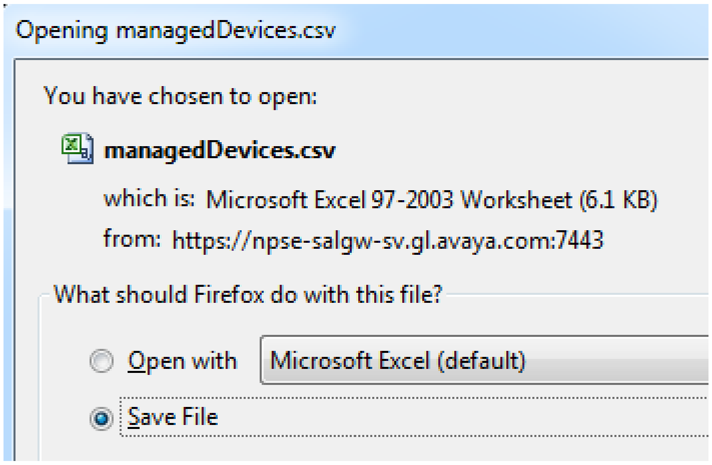


✓ SAL Agent is running ✓ Remote Access Agent is running

1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)7[illegible]9999	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

7.4. A dialogue window will appear where you can save the .CSV file.



Opening managedDevices.csv

You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

8. Access the new SAL Gateway

Obtain credentials and access the target consolidation SAL Gateway to migrate your existing SAL Gateway managed elements.

9. Manually add the Managed Elements to the new SAL Gateway

Using the data within the CSV file you obtained from the original/source SAL Gateway (SAL Gateway from which the managed elements are being migrated), administer all of these elements, one by one, onto the target consolidation SAL Gateway by following this how-to video (link).

10. Technically Onboard the migrated managed elements in the Global Registration Tool (GRT)

Once the managed elements are added successfully into target consolidation SAL Gateway, then user would login into GRT and submit a connectivity & alarming request to check the managed elements on the SAL Gateway.

10.1. Create a new Technical On-Boarding connectivity & alarming retest request for all of the managed elements migrated to the new SAL Gateway. A video is available (link).
  10.1.1. Enter Sold To
  10.1.2. Click on existing registered assets list
  10.1.3. Find the SEID to be migrated
  10.1.4. Click on Re-Test
  10.1.5. Select the check box for “Test Remote Access” and “Test Alarming” (the latter is only available if the device is entitled and eligible for alarming)
  10.1.6. Then click on “Submit”
10.2. GRT will test connectivity & alarming, and if it fails due to any reason then a Service Request (SR) will be created for the SAL Technical Onboarding team. If required, the SAL Technical Onboarding team will address the SR.
10.3. Repeat for each SEID individually
10.4. Please Join Ava Chat at https://support.avaya.com, if you have any questions related to the GRT registration or the SAL Technical Onboarding process.

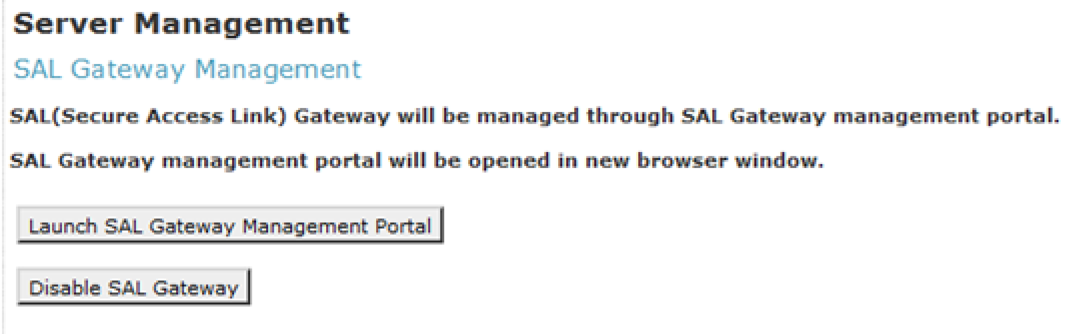
11. For a software-only or OVA SAL Gateway only – Decomission the old SAL Gateway

11.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
11.2. Authenticate with the admin or root user and password
11.3. Select all the Managed Elements by clicking the “all” selector
11.4. Click the Delete button to remove all the Managed Elements from this SAL Gateway
11.5. Restart the SAL Agent and Remote Access Agent within the SAL Gateway UI in order to apply these changes
11.6. Shutdown the SAL Gateway application
11.7. Login to the Global Registration Tool (https://grt.avaya.com)

11.8. Remove the SAL Gateway record using the “Record Validation” process. The following YouTube video shows this (link).

12. For a VSALGW (on System Platform) only - Decommission the old SAL Gateway

12.1. In addition to these written steps, a video exists showing how to do this (link)
12.2. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
12.3. Authenticate with the admin or root user and password
12.4. Select all the Managed Elements by clicking the “all” selector
12.5. Click the Delete button to remove all the Managed Elements from this SAL Gateway
12.6. Restart the SAL Agent and Remote Access Agent within the SAL Gateway UI in order to apply these changes
12.7. Skip steps 13..8, 13.9, and 13.10 if on System Platform 1.x
12.8. Login into the System Platform Console Domain with the ‘admin’ user.
12.9. On the left navigation pane under ‘Server Management” click on ‘SAL Gateway Management’.
12.10. Click on the ‘Disable SAL Gateway’ button.



Server Management

SAL Gateway Management

SAL(Secure Access Link) Gateway will be managed through SAL Gateway management portal.

SAL Gateway management portal will be opened in new browser window.

12.11. After disabling the SAL Gateway on System Platform, please deactivate the SEID associated with the original VSALGW by taking the following steps:

- **Customers:** Call Avaya IT. In the US 1-866-AVAYA IT, option 1, or 2. If you are not in the US, to obtain the number for other countries, visit https://support.avaya.com/contact and specify your country. During the phone call to AVAYA-IT ensure that you provide the SEID number for the SALGW to be deactivated.
- **Partners and Distributors:** submit an ITSS ticket www.avaya.com/partner-itss > Report an incident > Corporate Applications > support.avaya.com > In “Brief Description” enter VSALGW identified by SEID to be made Inactive
- **Avaya Associates:** Submit an ITSS ticket https://itss.avaya.com > request a service > applications supporting services > Siebel GCT > Data Assistance > Asset in Siebel Not in GRT. Ensure that you provide the SEID number for the SALGW to be deactivated.

C. Retire existing SAL Gateway and migrate managed elements to a new OVA SAL Gateway

The following steps explain how to get a new OVA SAL Gateway 2.5.2 installed and configured and then migrate an existing SAL Gateway to this new SAL Gateway.

1. Ensure proper network paths are open for the new OVA SAL Gateway

When deploying a new SAL Gateway into your environment, you’ll need to make sure that there are no firewall restrictions within your network for the new SAL Gateway, either restricting outbound access on HTTPS port 443 from the SAL Gateway (egress), or internally on UDP port 162 from your managed elements to the SAL Gateway (ingress).

The SAL Gateway uses port 443 outbound to communicate with the Avaya or Business Partner Secure Access Link Concentrator Servers for both alarm delivery and remote access connections. The specific ports and Avaya URLs are defined on page 11 of this linked Port Matrix document (link).

2. Register the new SAL Gateway with Avaya

When deploying a new SAL Gateway it will be necessary to register the SAL Gateway with Avaya which can be done either prior to the installation or automatically during an attended installation.

It is possible to use the Automatic Registration feature during SAL Gateway Installation during an attended UI installation to auto-generate the SEID & Alarm ID for the new SAL Gateway:

2.1. Use the *Deploying Avaya Diagnostic Server* section on Automatic Solution Element ID generation through the SAL Gateway UI (link)
2.2. Follow Pre-install task 16 from *Deploying Avaya Diagnostic Server* (link)

Otherwise, use the GRT Registration Process for the new SAL Gateway and it's SEID & Alarm ID. See the following references:

2.3. Registering SAL Gateway generating the SIED & Alarm ID prior to installation (link)
2.4. Or use the KB article if an Avaya SSO Login available (link)
2.5. Once you received the SEID & Alarm ID of the newly registered SAL Gateway then save these numbers as they will be administered into the SAL GW during the SAL Gateway installation

3. Download the SAL Gateway software

- Avaya Diagnostic Server 2.0 / SAL Gateway 2.0 OVA (link)
- Avaya Diagnostic Server 2.5 (link)
- Avaya Diagnostic Server / SAL Gateway 2.5 Service Pack 3 (link)

4. Deploy the new OVA SAL Gateway

Instructional video (link)

5. If on SAL Gateway 2.3, Upgrade to Avaya Diagnostic Server 2.5 (SAL Gateway 2.5)

- Upgrade checklist (link)
  - Note here that this checklist includes a required Java update
- Upgrade instructions (link)

6. Apply Avaya Diagnostic Server 2.5 Service Pack 3

- Instructions (link)

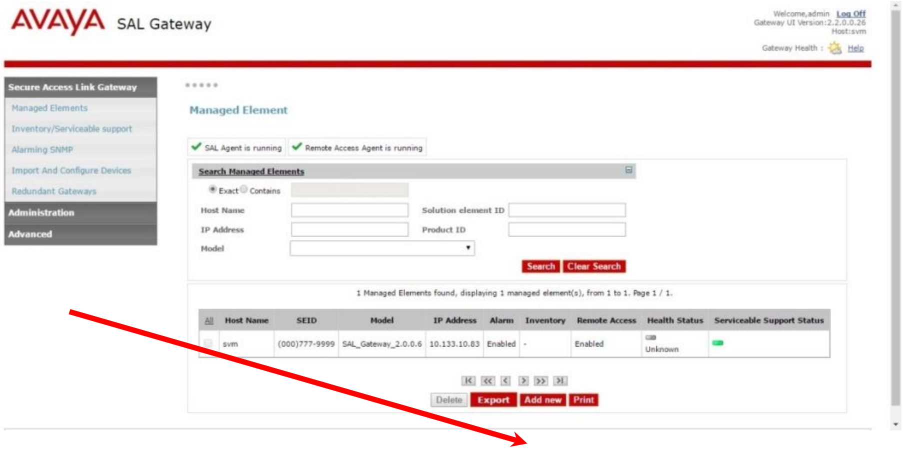
7. Additional Security Configuration

If required per the customer's specific installation, perform any OS-related configuration or hardening according to the instructions provided here (link).

8. Export Managed Elements List from old SAL Gateway

On the existing SAL Gateway use the following steps to obtain the CSV file of the existing managed elements to be migrated to the new software-only SAL Gateway

8.1. Login into the old SAL Gateway UI using https://sal-gateway-ipaddress:7443
8.2. Authenticate with the admin or root user and password
8.3. On the bottom of the Managed Element page click on the 'Export' button

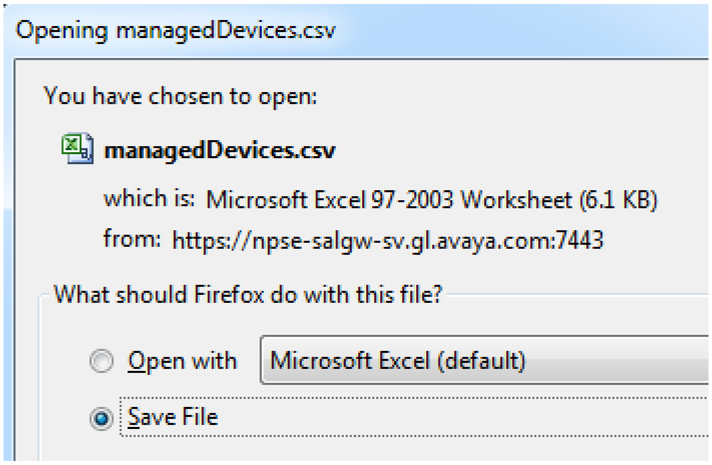


✓ SAL Agent is running ✓ Remote Access Agent is running

1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)777-9999	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

8.4. A dialogue window will appear where you can save the .CSV file.



Opening managedDevices.csv

You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

9. Access the new SAL Gateway

Obtain credentials and access the target consolidation SAL Gateway to migrate your existing SAL Gateway managed elements.

10. Manually add the Managed Elements to the new SAL Gateway

Using the data within the CSV file you obtained from the original/source SAL Gateway (SAL Gateway from which the managed elements are being migrated), administer all of these elements, one by one, onto the target consolidation SAL Gateway by following this how-to video (link).

11. Technically Onboard the migrated managed elements in the Global Registration Tool (GRT)

Once the managed elements are added successfully into target consolidation SAL Gateway, then user would login into GRT and submit a connectivity & alarming request to check the managed elements on the SAL Gateway.

11.1. Create a new Technical On-Boarding connectivity & alarming retest request for all of the managed elements migrated to the new SAL Gateway. A video is available (link).
  11.1.1. Enter Sold To
  11.1.2. Click on existing registered assets list
  11.1.3. Find the SEID to be migrated
  11.1.4. Click on Re-Test
  11.1.5. Select the check box for “Test Remote Access” and “Test Alarming” (the latter is only available if the device is entitled and eligible for alarming)
  11.1.6. Then click on “Submit”
11.2. GRT will test connectivity & alarming, and if it fails due to any reason then a Service Request (SR) will be created for the SAL Technical Onboarding team. If required, the SAL Technical Onboarding team will address the SR.
11.3. Repeat for each SEID individually
11.4. Please Join Ava Chat at https://support.avaya.com, if you have any questions related to the GRT registration or the SAL Technical Onboarding process.

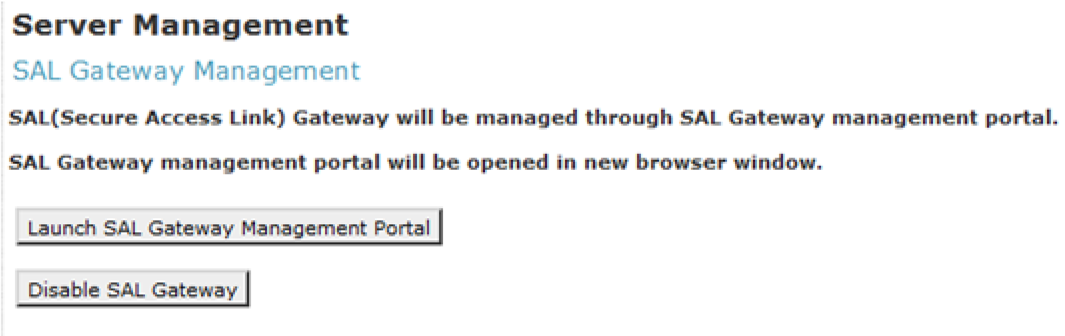
12. For a software-only or OVA SAL Gateway only – Decomission the old SAL Gateway

12.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
12.2. Authenticate with the admin or root user and password
12.3. Select all the Managed Elements by clicking the “all” selector
12.4. Click the Delete button to remove all the Managed Elements from this SAL Gateway
12.5. Restart the SAL Agent and Remote Access Agent within the SAL Gateway UI in order to apply these changes
12.6. Shutdown the SAL Gateway application
12.7. Login to the Global Registration Tool (https://grt.avaya.com)

12.8. Remove the SAL Gateway record using the “Record Validation” process. The following YouTube video shows this (link).

13. For a VSALGW (on System Platform) only - Decommission the old SAL Gateway

13.1. In addition to these written steps, a video exists showing how to do this (link)
13.2. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
13.3. Authenticate with the admin or root user and password
13.4. Select all the Managed Elements by clicking the “all” selector
13.5. Click the Delete button to remove all the Managed Elements from this SAL Gateway
13.6. Restart the SAL Agent and Remote Access Agent within the SAL Gateway UI in order to apply these changes
13.7. Skip steps 13.8, 13.9, and 13.10 if on System Platform 1.x
13.8. Login into the System Platform Console Domain with the ‘admin’ user.
13.9. On the left navigation pane under ‘Server Management” click on ‘SAL Gateway Management’.
13.10. Click on the ‘Disable SAL Gateway’ button.



Server Management

SAL Gateway Management

SAL(Secure Access Link) Gateway will be managed through SAL Gateway management portal.

SAL Gateway management portal will be opened in new browser window.

13.11. After disabling the SAL Gateway on System Platform, please deactivate the SEID associated with the original VSALGW by taking the following steps:

- **Customers:** Call Avaya IT. In the US 1-866-AVAYA IT, option 1, or 2. If you are not in the US, to obtain the number for other countries, visit https://support.avaya.com/contact and specify your country. During the phone call to AVAYA-IT ensure that you provide the SEID number for the SALGW to be deactivated.
- **Partners and Distributors:** submit an ITSS ticket www.avaya.com/partner-itss > Report an incident > Corporate Applications > support.avaya.com > In “Brief Description” enter VSALGW identified by SEID to be made Inactive
- **Avaya Associates:** Submit an ITSS ticket https://itss.avaya.com > request a service > applications supporting services > Siebel GCT > Data Assistance > Asset in Siebel Not in GRT. Ensure that you provide the SEID number for the SALGW to be deactivated.

D. Retire existing SAL Gateway and migrate managed elements to a new ION appliance SAL Gateway

The following steps explain how to get a new ION Appliance SAL Gateway 2.5.2 installed and configured and then migrate an existing SAL Gateway to this new SAL Gateway.

1. Ensure proper network paths are open for the new ION appliance SAL Gateway

When deploying a new SAL Gateway into your environment, you’ll need to make sure that there are no firewall restrictions within your network for the new SAL Gateway, either restricting outbound access on HTTPS port 443 from the SAL Gateway (egress), or internally on UDP port 162 from your managed elements to the SAL Gateway (ingress).

The SAL Gateway uses port 443 outbound to communicate with the Avaya or Business Partner Secure Access Link Concentrator Servers for both alarm delivery and remote access connections. The specific ports and Avaya URLs are defined on page 11 of this linked Port Matrix document (link).

2. Register the new SAL Gateway with Avaya

When deploying a new SAL Gateway it will be necessary to register the SAL Gateway with Avaya which can be done either prior to the installation or automatically during an attended installation.

It is possible to use the Automatic Registration feature during SAL Gateway Installation during an attended UI installation to auto-generate the SEID & Alarm ID for the new SAL Gateway:

2.1. Use the *Deploying Avaya Diagnostic Server* section on Automatic Solution Element ID generation through the SAL Gateway UI (link)
2.2. Follow Pre-install task 16 from *Deploying Avaya Diagnostic Server* (link)

Otherwise, use the GRT Registration Process for the new SAL Gateway and it's SEID & Alarm ID. See the following references:

2.3. Registering SAL Gateway generating the SIED & Alarm ID prior to installation (link)
2.4. Or use the KB article if an Avaya SSO Login available (link)
2.5. Once you received the SEID & Alarm ID of the newly registered SAL Gateway then save these numbers as they will be administered into the SAL GW during the SAL Gateway installation

3. Deploy the new ION Appliance SAL Gateway

- Connect and setup (link)
- Configure and initialize (link)
- Enable SSH (link)

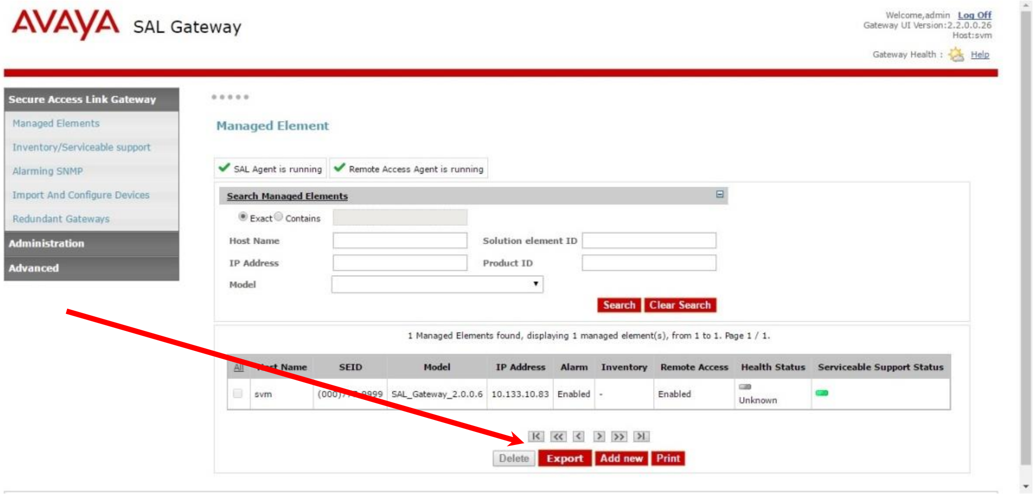
4. Apply Avaya Diagnostic Server 2.5 Service Pack 3

Newly acquired ION Appliances should already have 2.5.3 installed and thus be SHA2 compliant. To validate, please use the instructions in Section 3 to determine the SAL Gateway version and if not at 2.5.3 or later, please follow the instructions from ION to upgrade (link)

5. Export Managed Elements List from old SAL Gateway

On the existing SAL Gateway use the following steps to obtain the CSV file of the existing managed elements to be migrated to the new software-only SAL Gateway

5.1. Login into the old SAL Gateway UI using https://sal-gateway-ipaddress:7443
5.2. Authenticate with the admin or root user and password
5.3. On the bottom of the Managed Element page click on the 'Export' button



Gateway UI Version:2.2.0.0.26
Host:svm

✓ SAL Agent is running ✓ Remote Access Agent is running

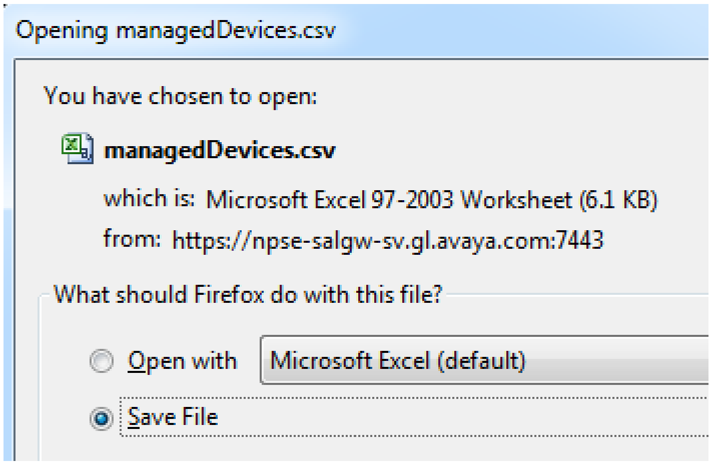
● Exact ○ Contains

Host Name:
Solution element ID:
IP Address:
Product ID:
Model:

1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)[illegible]9999	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

5.4. A dialogue window will appear where you can save the .CSV file.



Opening managedDevices.csv

You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

6. Access the new SAL Gateway

Obtain credentials and access the target consolidation SAL Gateway to migrate your existing SAL Gateway managed elements.

7. Manually add the Managed Elements to the new SAL Gateway

Using the data within the CSV file you obtained from the original/source SAL Gateway (SAL Gateway from which the managed elements are being migrated), administer all of these elements, one by one, onto the target consolidation SAL Gateway by following this how-to video (link).

8. Technically Onboard the migrated managed elements in the Global Registration Tool (GRT)

Once the managed elements are added successfully into target consolidation SAL Gateway, then user would login into GRT and submit a connectivity & alarming request to check the managed elements on the SAL Gateway.

8.1. Create a new Technical On-Boarding connectivity & alarming retest request for all of the managed elements migrated to the new SAL Gateway. A video is available (link).
  8.1.1. Enter Sold To
  8.1.2. Click on existing registered assets list
  8.1.3. Find the SEID to be migrated
  8.1.4. Click on Re-Test
  8.1.5. Select the check box for “Test Remote Access” and “Test Alarming” (the latter is only available if the device is entitled and eligible for alarming)
  8.1.6. Then click on “Submit”
8.2. GRT will test connectivity & alarming, and if it fails due to any reason then a Service Request (SR) will be created for the SAL Technical Onboarding team. If required, the SAL Technical Onboarding team will address the SR.
8.3. Repeat for each SEID individually
8.4. Please Join Ava Chat at https://support.avaya.com, if you have any questions related to the GRT registration or the SAL Technical Onboarding process.

9. Remove the Managed Elements from the old SAL Gateway

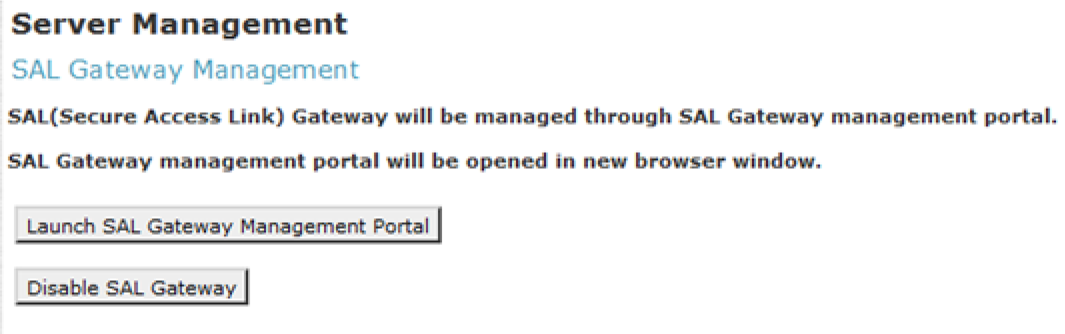
9.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
9.2. Authenticate with the admin or root user and password
9.3. Select all the Managed Elements by clicking the “all” selector
9.4. Click the Delete button to remove all the Managed Elements from this SAL Gateway
9.5. Restart the SAL Agent and Remote Access Agent within the SAL Gateway UI in order to apply these changes

10. For a software-only or OVA SAL Gateway only - Properly remove the old SAL Gateway from GRT

10.1. Shutdown the SAL Gateway application
10.2. Login to the Global Registration Tool (https://grt.avaya.com)
10.3. Remove the SAL Gateway record using the “Record Validation” process. The following YouTube video shows this (link).

11. Decommission the old SAL Gateway (VSALGW on System Platform)

11.1. Skip this step if on System Platform 1.x
11.2. Login into the System Platform Console Domain with the ‘admin’ user.
11.3. On the left navigation pane under ‘Server Management” click on ‘SAL Gateway Management’.
11.4. Click on the ‘Disable SAL Gateway’ button.



Server Management

SAL Gateway Management

SAL(Secure Access Link) Gateway will be managed through SAL Gateway management portal.

SAL Gateway management portal will be opened in new browser window.

11.5. After disabling the SAL Gateway on System Platform, please deactivate the SEID associated with the original VSALGW by taking the following steps:

- **Customers:** Call Avaya IT. In the US 1-866-AVAYA IT, option 1, or 2. If you are not in the US, to obtain the number for other countries, visit https://support.avaya.com/contact and specify your country. During the phone call to AVAYA-IT ensure that you provide the SEID number for the SALGW to be deactivated.
- **Partners and Distributors:** submit an ITSS ticket www.avaya.com/partner-itss > Report an incident > Corporate Applications > support.avaya.com > In “Brief Description” enter VSALGW identified by SEID to be made Inactive
- **Avaya Associates:** Submit an ITSS ticket https://itss.avaya.com > request a service > applications supporting services > Siebel GCT > Data Assistance > Asset in Siebel Not in GRT. Ensure that you provide the SEID number for the SALGW to be deactivated.

E. Upgrade a Software-only SAL Gateway 1.x

1. Recommend upgrading the operating system to RHEL 6.x

SAL Gateway 1.x uses RHEL 5.x. SAL Gateway 2.x supports both RHEL 5.x and 6.x, As such, upgrading from 1.x to 2.x does not require an OS upgrade. However, clients running RHEL 5.x should strongly consider upgrading the OS to RHEL 6.x 64-bit as part of this project. The next major release of SAL Gateway will run on RHEL 6.x and later, so an OS upgrade will be required from 2.5 to 3.x if not done now.

Also know this planning allows the customer to employ the sw-auto-update feature to upgrade/update to the future Avaya Diagnostic Server 3.0.

RHEL 5.x is also 3.5 years behind RHEL 6.x in Red Hat’s lifecycle process. You can read more about the current lifecycle status and dates for RHEL 5.x at (link).

If you choose to upgrade the OS to RHEL 6.x, please use the Upgrade Scenario B instructions instead. You will be able to re-use your existing SALGW SEID.

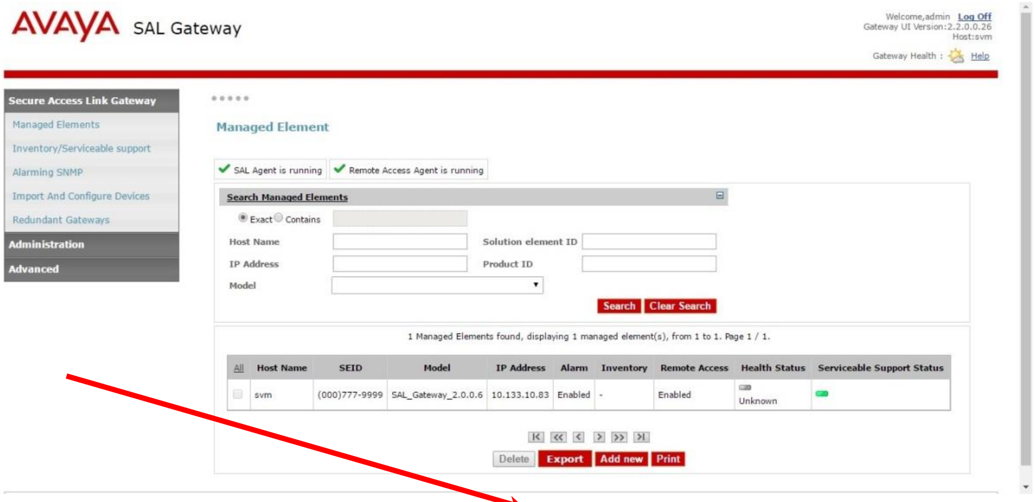
2. Backup the SAL Gateway

This 1.x SAL Gateway software does not natively provide backup capability. For the names of the files that you want to back up, use this (link).

3. Export Managed Elements List

In addition to backing up your SAL Gateway, it is highly also advised that you export a copy of all of your Managed Elements from the SAL Gateway UI. This will provide you with a list of all of your Solution Element IDs and Alarm IDs needed in the event you need to re-administer any of your devices manually.

3.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
3.2. Authenticate with the admin or root user and password
3.3. On the bottom of the Managed Element page click on the ‘Export’ button

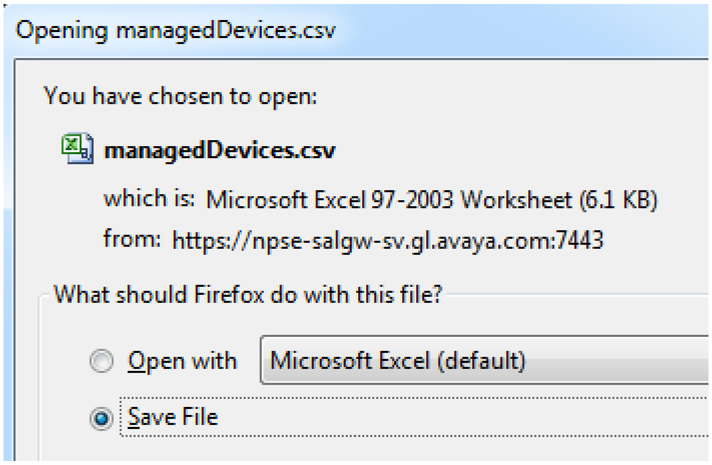


✓ SAL Agent is running ✓ Remote Access Agent is running

1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)777-9999	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	

3.4. A dialogue window will appear where you can save the .CSV file.



Opening managedDevices.csv

You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)
from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)
● Save File

4. Download the SAL Gateway software

- SAL Gateway 2.1 (link)
- Avaya Diagnostic Server / SAL Gateway 2.5 (link)
- Avaya Diagnostic Server / SAL Gateway 2.5 Service Pack 3 (link)

5. Upgrade the SAL Gateway from 1.x to 2.1

- Upgrade checklist (link)
    - Note here that this checklist includes a required Java update
- Upgrade instructions (link)

6. Upgrade the SAL Gateway from 2.1 to Avaya Diagnostic Server 2.5 (SAL Gateway 2.5)

- Upgrade checklist (link)
- Upgrade instructions (link)

7. Apply Avaya Diagnostic Server 2.5 Service Pack 3

- Instructions (link)

8. No changes are needed in the Global Registration Tool (GRT)

F. Upgrade a Software-only SAL Gateway 2.0, 2.1, or 2.2

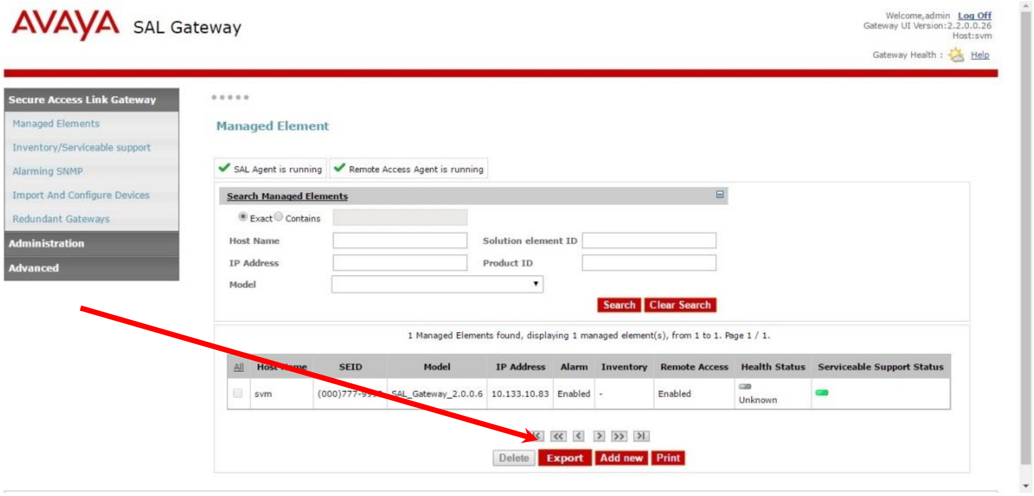
1. Backup the SAL Gateway

- Instructions (link)

2. Export Managed Elements List

In addition to backing up your SAL Gateway, it is highly also advised that you export a copy of all of your Managed Elements from the SAL Gateway UI. This will provide you with a list of all of your Solution Element IDs and Alarm IDs needed in the event you need to re-administer any of your devices manually.

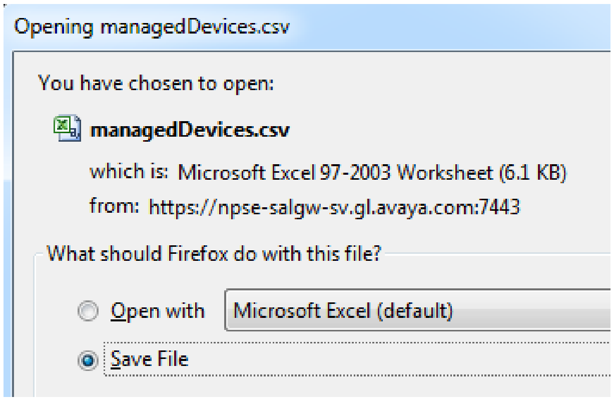
2.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
2.2. Authenticate with the admin or root user and password
2.3. On the bottom of the Managed Element page click on the 'Export' button



1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)777-99	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

2.4. A dialogue window will appear where you can save the .CSV file.



You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

3. Download the SAL Gateway software

- Avaya Diagnostic Server / SAL Gateway 2.5 (link)
- Avaya Diagnostic Server / SAL Gateway 2.5 Service Pack 3 (link)

4. Upgrade the SAL Gateway from 2.x to Avaya Diagnostic Server 2.5 (SAL Gateway 2.5)

- Upgrade checklist (link)
    - Note here that this checklist includes a required Java update
- Upgrade instructions (link)

5. Apply Avaya Diagnostic Server 2.5 Service Pack 3

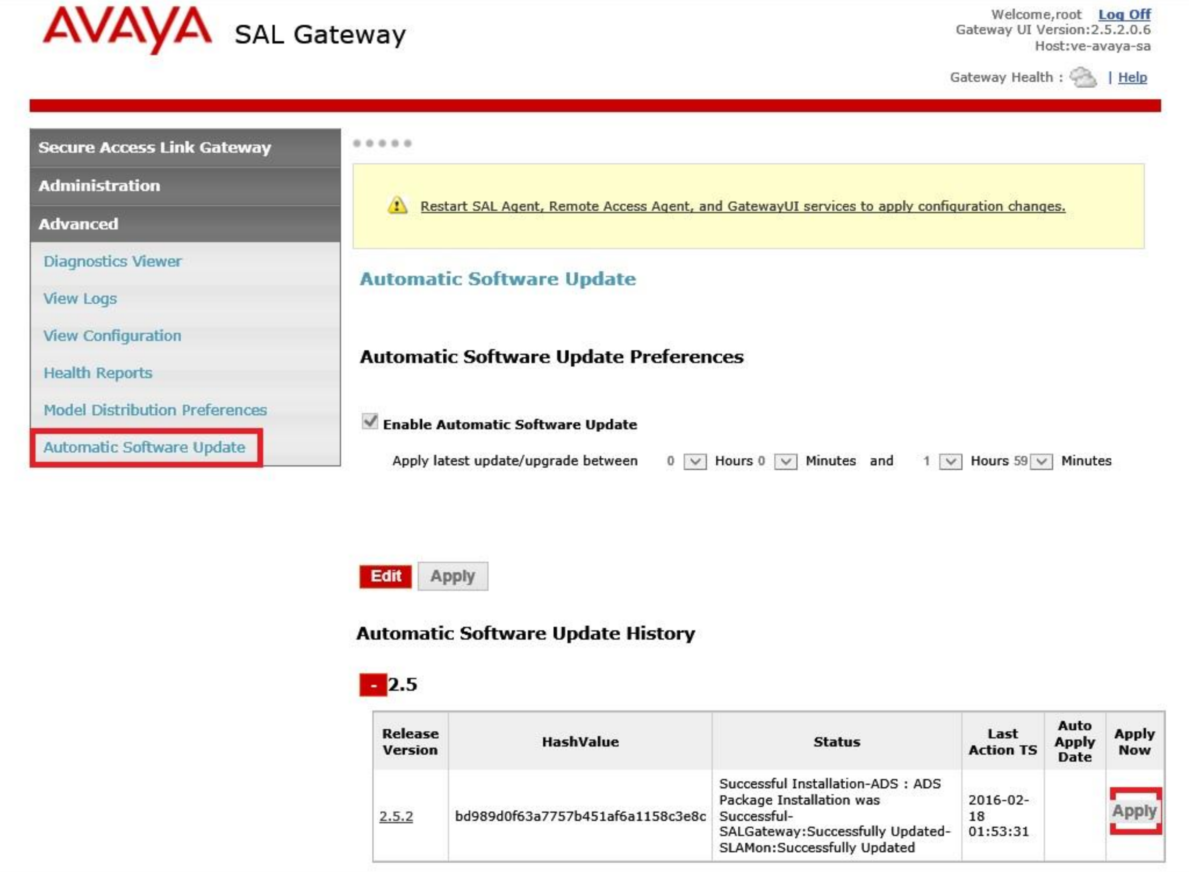
- Instructions (link)

6. No changes are needed in the Global Registration Tool (GRT)

G. Upgrade a Software-only SAL Gateway 2.3.x, 2.5.0, or 2.5.1

It is recommended that the customer enable software-auto-update feature available on the SAL Gateway 2.3 and greater. This allows the customer to automatically receive downloads, notifications and automatically schedule, at their predetermined time, a software update/upgrade. Instructions on enabling this feature are available here (link).

On SAL Gateway 2.5, the customer also has the option to apply the new software manually by clicking on the “Apply” button, as opposed to having the SAL Gateway apply the software on the “Auto Apply Date” at the specified time window. SAL Gateway 2.3 does not have the "Apply" button.



Gateway UI Version:2.5.2.0.6
Host:ve-avaya-sa

Restart SAL Agent, Remote Access Agent, and GatewayUI services to apply configuration changes.

Automatic Software Update

Automatic Software Update Preferences

☑ Enable Automatic Software Update

Apply latest update/upgrade between 0 Hours 0 Minutes and 1 Hours 59 Minutes

Automatic Software Update History

2.5

Release Version	HashValue	Status	Last Action TS	Auto Apply Date	Apply Now
2.5.2	bd989d0f63a7757b451af6a1158c3e8c	Successful Installation-ADS : ADS Package Installation was Successful-SALGateway:Successfully Updated-SLAMon:Successfully Updated	2016-02-18 01:53:31		Apply

If the customer has chosen to utilize the software-auto-update feature, the SAL Gateway will automatically update itself to the latest version of the SAL Gateway application. No further work is needed.

The following steps are for a SAL Gateway 2.3 when the customer has chosen not to use the automatic software update feature.

1. Backup the SAL Gateway

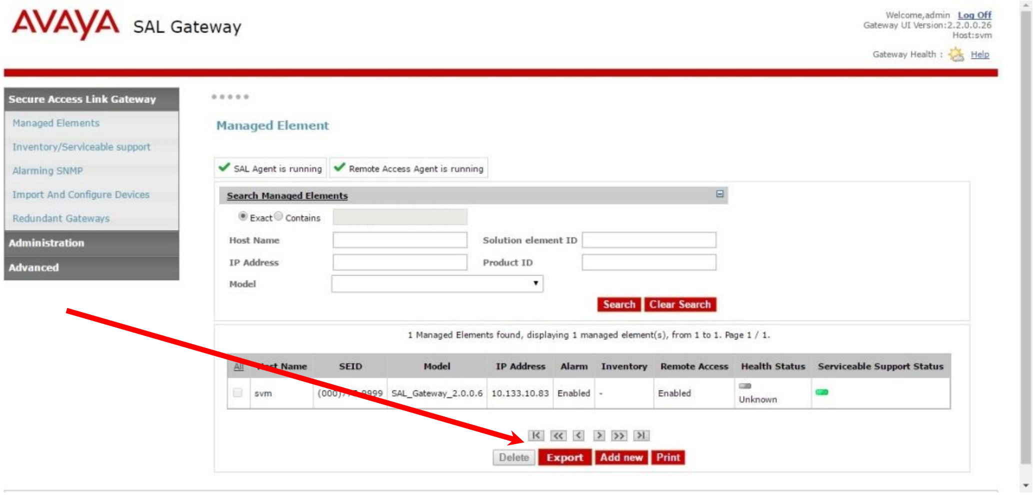
Use the following relevant upgrade steps for this manual install case.

1.1. Instructions (link)
1.2. Pull copy off the backup archive form the SAL Gateway server using an SFTP client such as WinSCP
1.3. Or you can backup directly to a remote server via the SAL Gateway user interface (link)

2. Export Managed Elements List

In addition to backing up your SAL Gateway, it is highly also advised that you export a copy of all of your Managed Elements from the SAL Gateway UI. This will provide you with a list of all of your Solution Element IDs and Alarm IDs needed in the event you need to re-administer any of your devices manually.

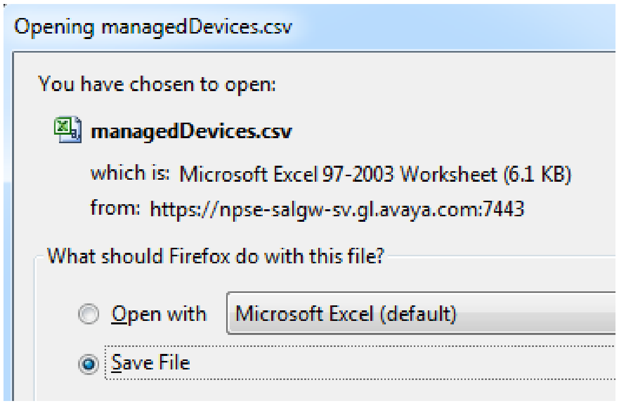
2.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
2.2. Authenticate with the admin or root user and password
2.3. On the bottom of the Managed Element page click on the ‘Export’ button



1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)[illegible]9999	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

2.4. A dialogue window will appear where you can save the .CSV file.



You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

3. Download the SAL Gateway software

These software files should be already be downloaded on the SAL Gateway due to the Avaya Diagnostic Server software automatic update feature (link) or download the software again if needed

- Avaya Diagnostic Server / SAL Gateway 2.5 (link) (Only needed if customer is currently on 2.3)
- Avaya Diagnostic Server / SAL Gateway 2.5 Service Pack 3 (link)

4. If on SAL Gateway 2.3, Upgrade to Avaya Diagnostic Server 2.5 (SAL Gateway 2.5)

- Upgrade checklist (link)
    - Note here that this checklist includes a required Java update
- Upgrade instructions (link)

5. Apply Avaya Diagnostic Server 2.5 Service Pack 3

- Instructions (link)

6. No changes are needed in the Global Registration Tool (GRT)

H. Upgrade the SAL Gateway software on a SAL Gateway 2.2 OVA

The SAL 2.2 OVA is a VMware virtual machine with SAL Gateway 2.2. It is the only SAL Gateway OVA that Avaya released prior to the Avaya Diagnostic Server 2.0 OVA.

There are two methods to upgrade the SAL 2.2 OVA. One method is to upgrade the SAL Gateway software on this virtual machine (steps below). The second method is to upgrade the OVA itself (Scenario I).

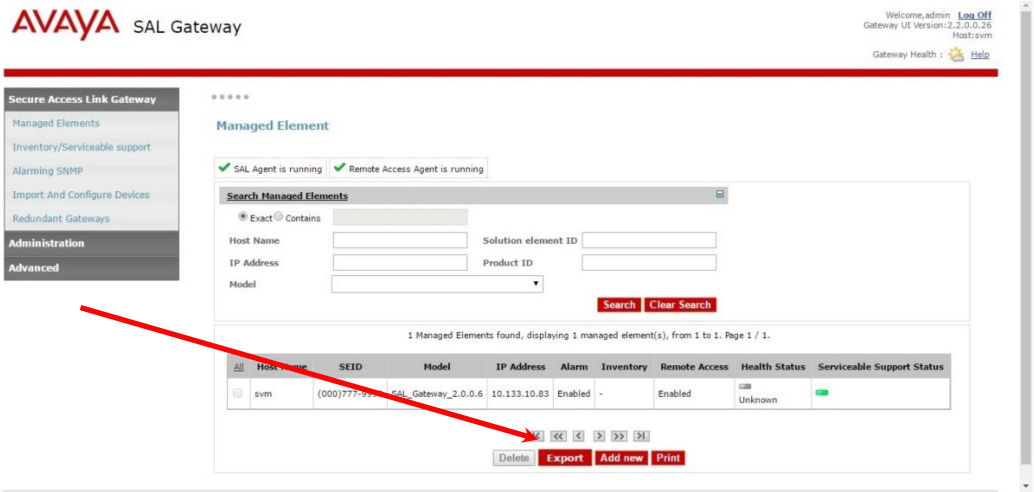
1. Backup the SAL Gateway

1.1. Instructions (link)
1.2. Pull copy off the backup archive form the SAL Gateway server using an SFTP client such as WinSCP
1.3. Or you can backup directly to a remote server via the SAL Gateway user interface (link)

2. Export Managed Elements List

In addition to backing up your SAL Gateway, it is highly also advised that you export a copy of all of your Managed Elements from the SAL Gateway UI. This will provide you with a list of all of your Solution Element IDs and Alarm IDs needed in the event you need to re-administer any of your devices manually.

2.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
2.2. Authenticate with the admin or root user and password
2.3. On the bottom of the Managed Element page click on the 'Export' button

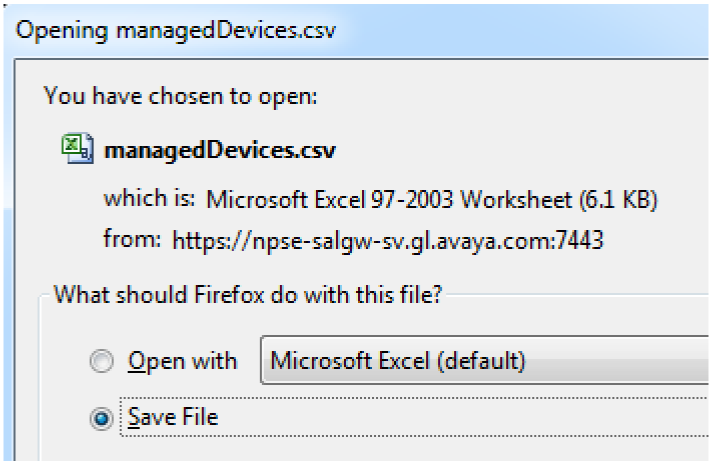


✓ SAL Agent is running ✓ Remote Access Agent is running

1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)777-99	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

2.4. A dialogue window will appear where you can save the .CSV file.



Opening managedDevices.csv

You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

3. Download the SAL Gateway software

- Avaya Diagnostic Server / SAL Gateway 2.5 (link)
- Avaya Diagnostic Server / SAL Gateway 2.5 Service Pack 3 (link)

4. Upgrade the SAL Gateway from 2.x to Avaya Diagnostic Server 2.5 (SAL Gateway 2.5)

- Upgrade checklist (link)
  - Note here that this checklist includes a required Java update
- Upgrade instructions (link)
  - The instructions in this section so far are almost identical to scenario F. However, there are critical additional steps for the SAL 2.2 OVA. Prior to upgrading the SAL Gateway, you must
  - `stop iptables – service iptables stop`
  - Then after the upgrade is complete, you must
  - `start iptables – service iptables start`

5. Apply Avaya Diagnostic Server 2.5 Service Pack 3

- Instructions (link)

6. No changes are needed in the Global Registration Tool (GRT)

I. Upgrade a SAL Gateway 2.2 OVA to ADS 2.0 OVA with SAL Gateway 2.5.2

The SAL 2.2 OVA is a VMware virtual machine with SAL Gateway 2.2. It is the only SAL Gateway OVA that Avaya released prior to the Avaya Diagnostic Server 2.0 OVA.

There are two methods to upgrade the SAL 2.2 OVA. One method is to upgrade the SAL Gateway software on this virtual machine (Scenario H). The second method is to upgrade the OVA itself (steps below).

1. Backup the SAL Gateway

1.1. Instructions (link)

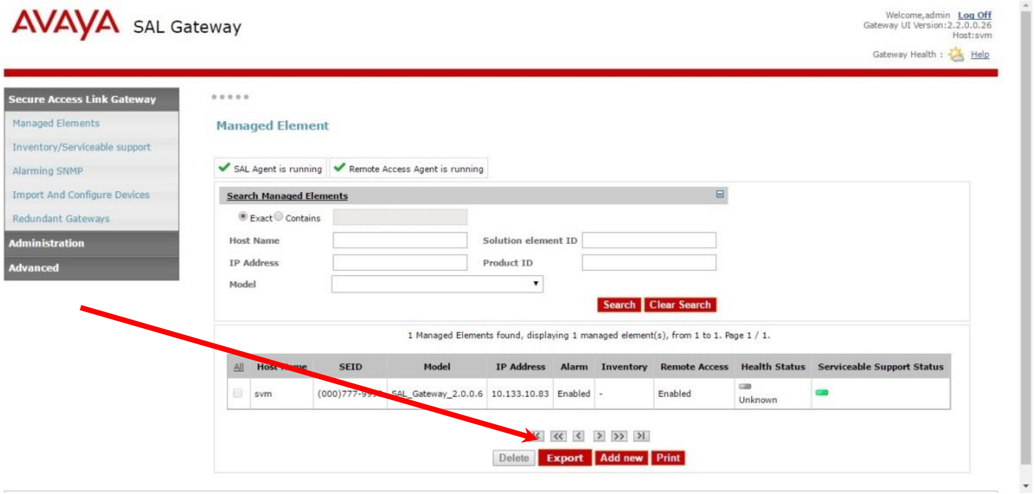
1.2. Pull copy off the backup archive form the SAL Gateway server using an SFTP client such as WinSCP

1.3. Or you can backup directly to a remote server via the SAL Gateway user interface (link)

2. Export Managed Elements List

In addition to backing up your SAL Gateway, it is highly also advised that you export a copy of all of your Managed Elements from the SAL Gateway UI. This will provide you with a list of all of your Solution Element IDs and Alarm IDs needed in the event you need to re-administer any of your devices manually.

2.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
2.2. Authenticate with the admin or root user and password
2.3. On the bottom of the Managed Element page click on the 'Export' button

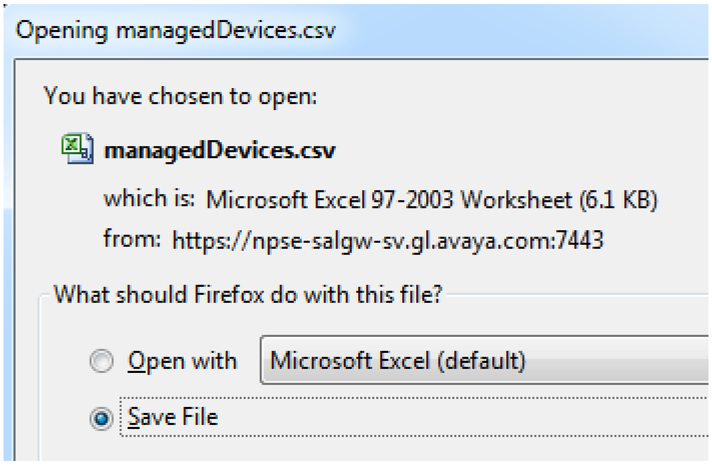


✓ SAL Agent is running ✓ Remote Access Agent is running

1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)777-99	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

2.4. A dialogue window will appear where you can save the .CSV file.



You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

3. Download the SAL Gateway software

- Avaya Diagnostic Server 2.0 OVA (link)
- Avaya Diagnostic Server / SAL Gateway 2.5 (link)
- Avaya Diagnostic Server / SAL Gateway 2.5 Service Pack 3 (link)

4. Upgrade the SAL 2.2 OVA to the Avaya Diagonstic Server 2.0 OVA

- The ADS 2.0 OVA has a larger virtual machine footprint than the SAL 2.2 OVA, so you must plan accordingly.
- Instructions (link)

5. Upgrade the software on the ADS 2.0 OVA to ADS 2.5

- The ADS 2.0 OVA contains SAL Gateway 2.3 (Avaya had not aligned the release numbering by the time ADS 2.0 was released).
- Avaya did not create a new OVA for ADS 2.5. Instead, the upgrade path is to simply upgrade the software on the ADS 2.0 virtual machine from SAL Gateway 2.3 to SAL Gateway 2.5.
- Upgrade checklist (link)
  - Note here that this checklist includes a required Java update
- Upgrade instructions (link)
  - The instructions in this section so far are almost identical to scenario F. However, there are critical additional steps for the SAL 2.2 OVA. Prior to upgrading the SAL Gateway, you must
  - `stop iptables – service iptables stop`
  - Then after the upgrade is complete, you must
  - `start iptables – service iptables start`

6. Apply Avaya Diagnostic Server 2.5 Service Pack 3

- Instructions (link)

7. No changes are needed in the Global Registration Tool (GRT)

J. Upgrade ADS 2.0 OVA

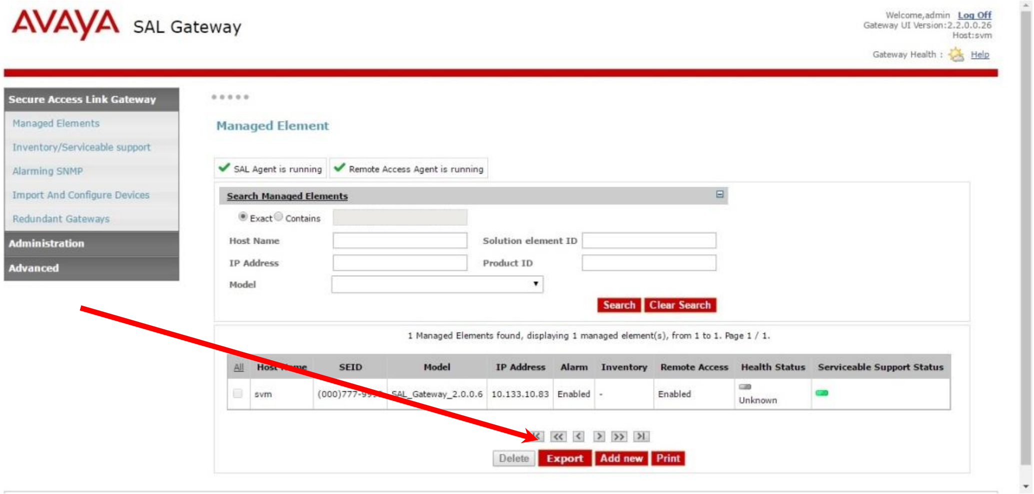
1. Backup the SAL Gateway

1.1. Instructions (link)
1.2. Pull copy off the backup archive form the SAL Gateway server using an SFTP client such as WinSCP
1.3. Or you can backup directly to a remote server via the SAL Gateway user interface (link)

2. Export Managed Elements List

In addition to backing up your SAL Gateway, it is highly also advised that you export a copy of all of your Managed Elements from the SAL Gateway UI. This will provide you with a list of all of your Solution Element IDs and Alarm IDs needed in the event you need to re-administer any of your devices manually.

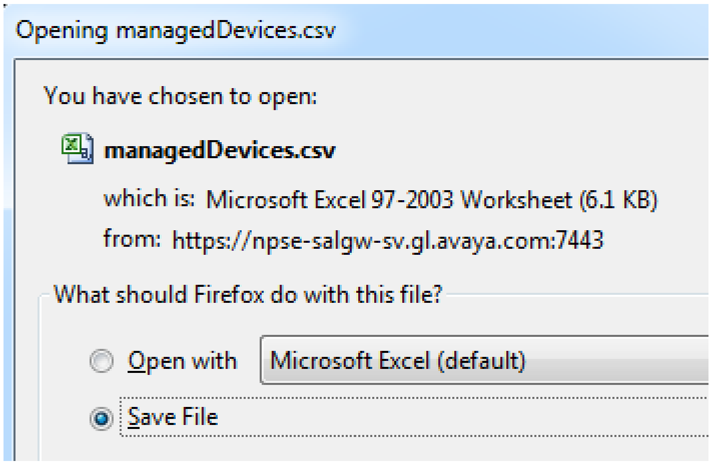
2.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
2.2. Authenticate with the admin or root user and password
2.3. On the bottom of the Managed Element page click on the ‘Export’ button



1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)777-99	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

2.4. A dialogue window will appear where you can save the .CSV file.



Opening managedDevices.csv

You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

3. Download the SAL Gateway software

- Avaya Diagnostic Server / SAL Gateway 2.5 (link)
- Avaya Diagnostic Server / SAL Gateway 2.5 Service Pack 3 (link)

4. Upgrade the software on the ADS 2.0 OVA to ADS 2.5

- The ADS 2.0 OVA contains SAL Gateway 2.3 (Avaya had not aligned the release numbering by the time ADS 2.0 was released).
- Avaya did not create a new OVA for ADS 2.5. Instead, the upgrade path is to simply upgrade the software on the ADS 2.0 virtual machine from SAL Gateway 2.3 to SAL Gateway 2.5.
- Upgrade checklist (link)
    - Note here that this checklist includes a required Java update
- Upgrade instructions (link)
    - The instructions in this section so far are almost identical to scenario F. However, there are critical additional steps for the SAL 2.2 OVA. Prior to upgrading the SAL Gateway, you must
    - `stop iptables – service iptables stop`
    - Then after the upgrade is complete, you must
    - `start iptables – service iptables start`

5. Apply Avaya Diagnostic Server 2.5 Service Pack 3

- Instructions (link)

6. No changes are needed in the Global Registration Tool (GRT)

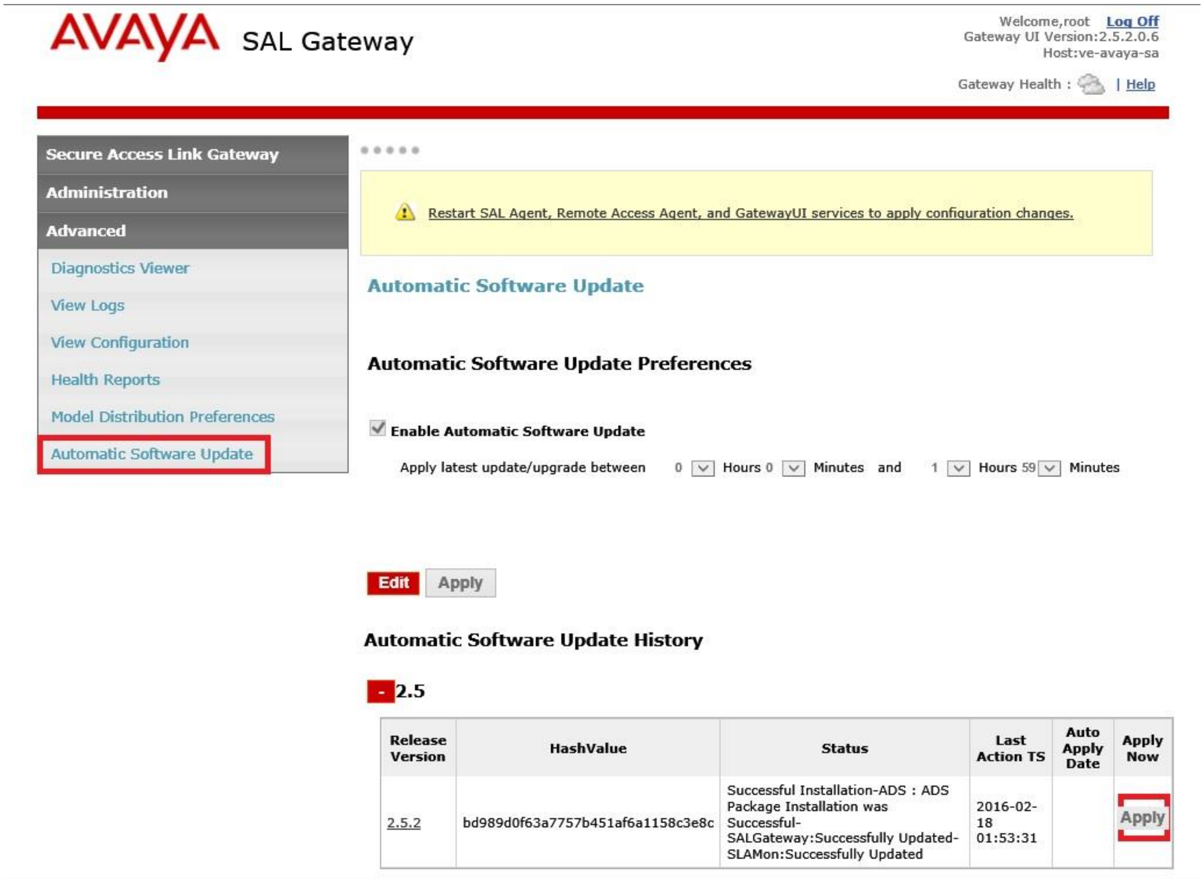
K. Upgrade an SAL Gateway 2.5 OVA for Appliance Virtualization Platform (AVP)

As mentioned in Section 2.C, the SAL 2.5 OVA for AVP is a small-footprint OVA designed to fit on the Avaya Aura 7 Appliance Virtualization Platform (AVP), along with other Avaya Aura products. It is the AVP equivalent to the Services Virtual Machine (SVM) on Avaya Aura 6 System Platform. This OVA has a very low capacity SAL Gateway 2.5 capable of supporting only 15 managed elements.

An overview of the Small SAL 2.5 OVA being used on the Avaya Aura Appliance Virtualization can be found here for reference. The upgrade steps for this case are as follows:

It is recommended that the customer enable the software-auto-update feature available on the SAL Gateway. This allows the customer to automatically receive downloads, notifications and automatically schedule, at their predetermined time, a software update/upgrade. Instructions on enabling this feature are available here (link).

On the SAL Gateway, the customer also has the option to apply the new software manually by clicking on the “Apply” button, as opposed to having the SAL Gateway apply the software on the “Auto Apply Date” at the specified time window.



Restart SAL Agent, Remote Access Agent, and GatewayUI services to apply configuration changes.

Automatic Software Update

Automatic Software Update Preferences

☑ **Enable Automatic Software Update**

Apply latest update/upgrade between 0 Hours 0 Minutes and 1 Hours 59 Minutes

Automatic Software Update History

2.5

Release Version	HashValue	Status	Last Action TS	Auto Apply Date	Apply Now
2.5.2	bd989d0f63a7757b451af6a1158c3e8c	Successful Installation-ADS : ADS Package Installation was Successful-SALGateway:Successfully Updated-SLAMon:Successfully Updated	2016-02-18 01:53:31		Apply

If the customer has chosen to utilize the software-auto-update feature, the SAL Gateway will automatically update itself to the latest version of the SAL Gateway application. No further work is needed.

The following steps are for completing this upgrade when the customer has chosen not to use the automatic software update feature.

1. Backup the SAL Gateway

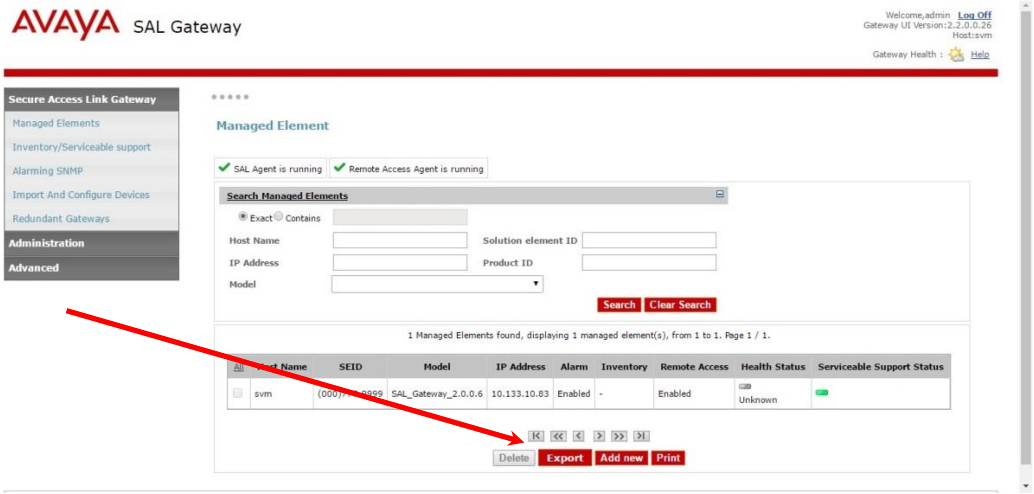
Use the following relevant upgrade steps for this manual install case.

1.1. Instructions (link)
1.2. Pull copy off the backup archive form the SAL Gateway server using an SFTP client such as WinSCP
1.3. Or you can backup directly to a remote server via the SAL Gateway user interface (link)

2. Export Managed Elements List

In addition to backing up your SAL Gateway, it is highly also advised that you export a copy of all of your Managed Elements from the SAL Gateway UI. This will provide you with a list of all of your Solution Element IDs and Alarm IDs needed in the event you need to re-administer any of your devices manually.

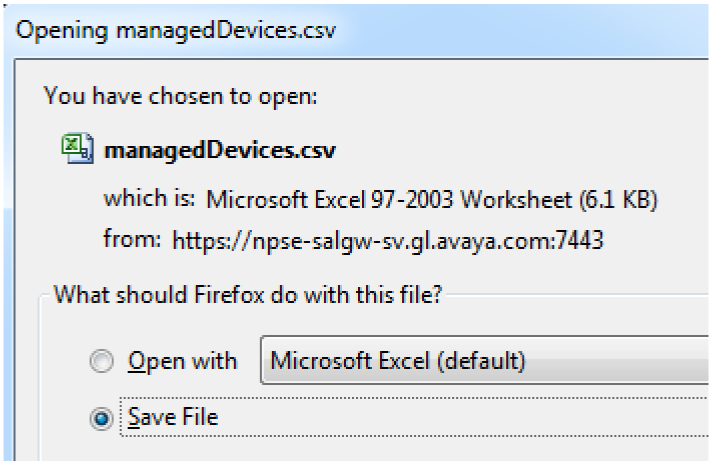
2.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
2.2. Authenticate with the admin or root user and password
2.3. On the bottom of the Managed Element page click on the ‘Export’ button



1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)[illegible]9999	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

2.4. A dialogue window will appear where you can save the .CSV file.


Opening managedDevices.csv

You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)
from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)
● Save File

3. Download the SAL Gateway software

These software files should be already be downloaded on the SAL Gateway due to the Avaya Diagnostic Server software automatic update feature (link) or download the software again if needed

- Avaya Diagnostic Server / SAL Gateway 2.5 (link) (Only needed if customer is currently on 2.3)
- Avaya Diagnostic Server / SAL Gateway 2.5 Service Pack 3 (link)

4. If on SAL Gateway 2.3, Upgrade to Avaya Diagnostic Server 2.5 (SAL Gateway 2.5)

- Upgrade checklist (link)
    - Note here that this checklist includes a required Java update
- Upgrade instructions (link)

5. Apply Avaya Diagnostic Server 2.5 Service Pack 3

- Instructions (link)

6. No changes are needed in the Global Registration Tool (GRT)

L. Upgrade a VSALGW 1.x on System Platform 1.x or 6.0.x

While possible to upgrade a VSALGW on a System Platform 1.x or 6.0.x, this scenario includes a significant amount of time, complexity and service affecting downtime involved in this task, since not only would you need to upgrade your System Platform version, but also all of your Avaya virtual machines for your given template.

It is therefore ***highly recommended and encouraged*** that you migrate any VSALGW managed elements to an existing stand-alone SAL Gateway (Scenario A), or deploy a new SAL Gateway (Scenarios B, C, and D) where you can consolidate all of your System Platform solution applications which are currently managed by this non-compliant version. Else, follow the steps below

M. Upgrade a SVM1 (System Platform 6.2.x VSALGW 2.1)

A full video showing all the following steps for Scenario M can be found at this (link).

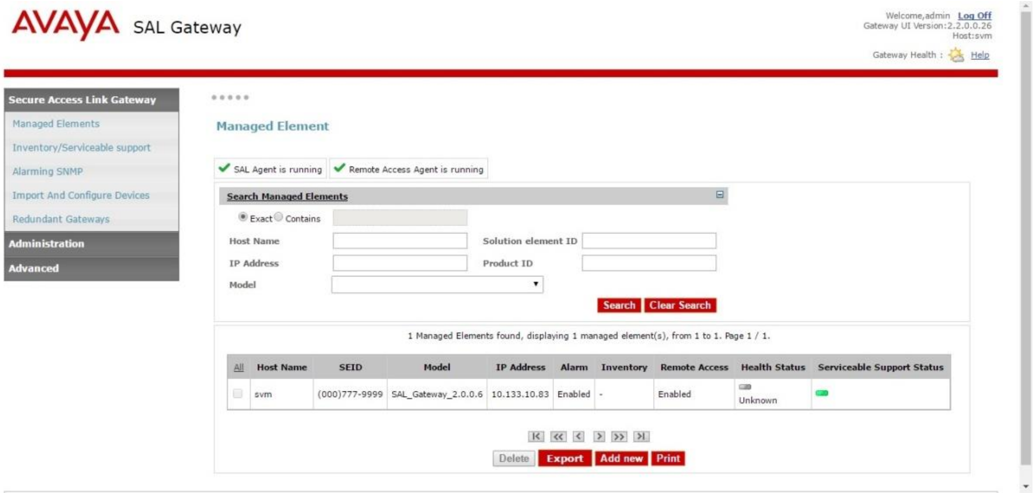
1. Backup the SAL Gateway

1.1. Instructions (link)
1.2. If the user encounters browser issues with the SAL Gateway user more recent browsers (ex. IE11 and greater), please consult PSN004538u.
1.3. Pull copy off the backup archive form the System Platform server using an SFTP client such as WinSCP

2. Download the SAL Gateway software

In addition to backing up your SAL Gateway, it is highly also advised that you export a copy of all of your Managed Elements from the SAL Gateway UI. This will provide you with a list of all of your Solution Element IDs and Alarm IDs needed in the event you need to re-administer any of your devices manually.

2.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
2.2. Authenticate with the admin or root user and password
2.3. On the bottom of the Managed Element page click on the ‘Export’ button



✓ SAL Agent is running ✓ Remote Access Agent is running

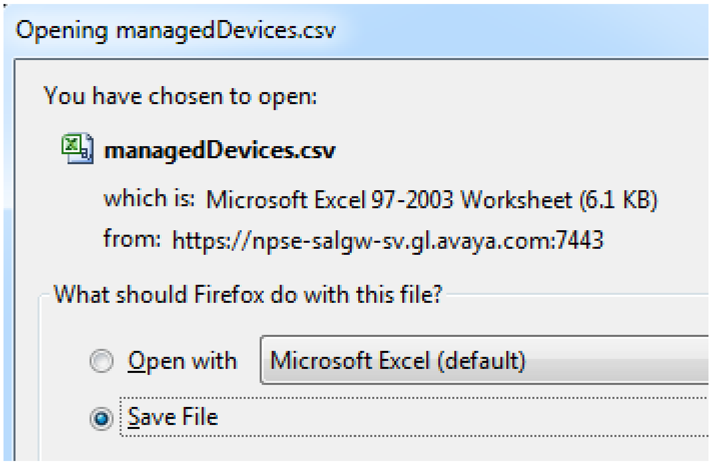
● Exact ○ Contains

Host Name:
Solution element ID:
IP Address:
Product ID:
Model:

1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)777-9999	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

2.4. A dialogue window will appear where you can save the .CSV file.



Opening managedDevices.csv

You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

3. Download the SAL Gateway software

- Services-VM 3.0 (link)
- Services-VM Sanity Plug-in Patch (link)
- Services-VM Service Pack #1 (link)

4. Upgrade to Services-VM 3.0

Instructions (link)

5. Apply Services-VM Sanity Plug-in Patch

Instructions (link)

6. Apply Service-VM3 Service Pack #1

6.1. Stop the watchdog process per the release notes (link)
6.2. Follow the instructions in Administering Avaya Aura® System Platform for downloading and installing patches (link)

7. No changes are needed in the Global Registration Tool (GRT)

N. Upgrade a SVM2 (System Platform 6.3.0 VSALGW 2.2)

A full video showing all the following steps for Scenario N can be found at this (link).

1. Backup the SAL Gateway

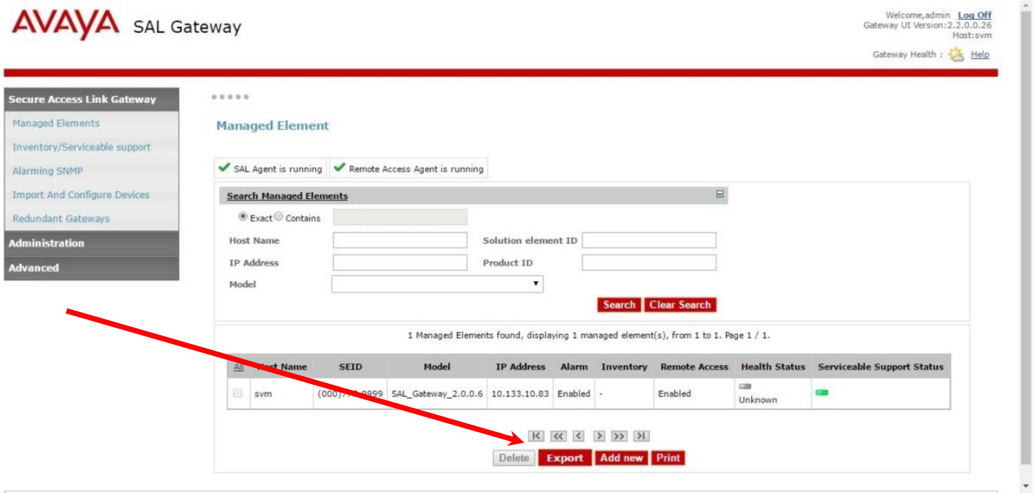
1.1. Instructions (link)
1.2. If the user encounters browser issues with the SAL Gateway user more recent browsers (ex. IE11 and greater), please consult PSN004538u.
1.3. Pull copy off the backup archive form the SAL Gateway server using an SFTP client such as WinSCP
1.4. Or you can backup directly to a remote server via the SAL Gateway user interface (link)

2. Export Managed Elements List

In addition to backing up your SAL Gateway, it is highly also advised that you export a copy of all of your Managed Elements from the SAL Gateway UI. This will provide you with a list of all of your Solution Element IDs and Alarm IDs needed in the event you need to re-administer any of your devices manually.

2.1. Login into the SAL Gateway UI using https://sal-gateway-ipaddress:7443
2.2. Authenticate with the admin or root user and password

2.3. On the bottom of the Managed Element page click on the ‘Export’ button

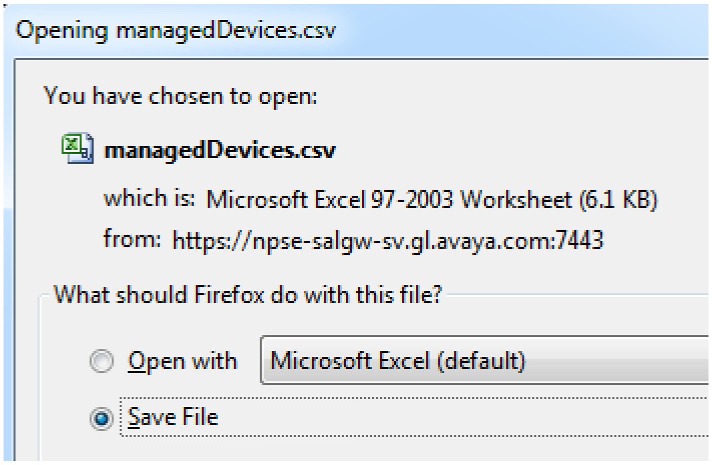


✓ SAL Agent is running ✓ Remote Access Agent is running

1 Managed Elements found, displaying 1 managed element(s), from 1 to 1. Page 1 / 1.

All	Host Name	SEID	Model	IP Address	Alarm	Inventory	Remote Access	Health Status	Serviceable Support Status
☐	svm	(000)[illegible]9999	SAL_Gateway_2.0.0.6	10.133.10.83	Enabled	-	Enabled	Unknown	🟩

2.4. A dialogue window will appear where you can save the .CSV file.


Opening managedDevices.csv

You have chosen to open:

managedDevices.csv

which is: Microsoft Excel 97-2003 Worksheet (6.1 KB)

from: https://npse-salgw-sv.gl.avaya.com:7443

What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

3. Download the SAL Gateway software

- Services-VM 3.0 (link)
- Services-VM Sanity Plug-in Patch (link)
- Services-VM Service Pack #1 (link)

4. Upgrade to Services-VM 3.0

Instructions (link)

5. Apply Services-VM Sanity Plug-in Patch

Instructions (link)

6. Apply Service-VM3 Service Pack #1

6.1. Stop the watchdog process per the release notes (link)

6.2. Follow the instructions in Administering Avaya Aura® System Platform for downloading and installing patches (link)

7. No changes needed in the Global Registration Tool (GRT)

O. Upgrade a SVM3 (System Platform 6.3.1+ VSALGW 2.2)

A full video showing all the following steps for Scenario O can be found at this (link).

While all System Platform systems at 6.3.1 or greater should have already had their VSALGW upgraded to SVM3, please confirm that to be the case using Section 2.I. If instead you find this server to still be running SVM2, please use Scenario N above.

1. Backup the SAL Gateway

Instructions (link)

2. Download the SAL Gateway software

Services-VM Service Pack #1 (link)

3. Apply Service-VM3 Service Pack #1

3.1. Stop the watchdog process per the release notes (link)
3.2. Follow the instructions in Administering Avaya Aura® System Platform for downloading and installing patches (link)

4. No changes are needed in the Global Registration Tool (GRT)

P. In-place Upgrade of an ION SAL Gateway Appliance

API Tech has published a comprehensive set of instructions on how to upgrade an existing ION SAL Gateway appliance to be SHA2 compliant. These instructions are available at this (link).

No changes are needed in the Global Registration Tool (GRT)

Appendix A: Glossary

ADS: Avaya Diagnostic Server. Overall umbrella for two elements: SAL and SLA Mon™

a.k.a. also known as

CA: Certificate Authority

CDom: Console Domain a virtualize machine on the Avaya Aura System Platform product that contains System Platform console (administrative console). And in addition in the System Platform versions 1.x and 6.0.x release had the Secure Access Link embedded into the CDom virtual machine.

EXPERT: Avaya EXPERT Systems(SM) Diagnostic Tools are powerful problem finders, delivering continuous monitoring, a patented resolution process, and much more. These automated tools proactively and autonomously resolve communications problems.

FL: Functional Location, a number assigned by Avaya to indicate a unique customer location. Also known as the SoldTo number,

GRT: Global Registration Tool - https://grt.avaya.com/grt/

GW: Gateway as is SAL GW

GUI: Graphical User Interface

ID: Identifier

ION: ION™ SA5610-SAL Avaya® SAL Edition Secure Appliance provided by API Tech, an Avaya DevConnect Partner.

NA: Not Applicable

OVA: VMware based Open Virtualized Appliance

OS: Operating System

RHEL: Red Hat Enterprise Linux

SAL: Secure Access Link

SALGW: The SE Code for a standalone SAL Gateway

SEID: Solution Element Identifier – A unique 10-digit number assigned to an Avaya application/product upon registration within the GRT tool. SEIDs are typically formatted like a US phone number: (123) 456-7890

SE Code: Solution Element Code, a short abbreviation indicating the type of Avaya product. A few examples are SALGW = SAL Gateway, VCM = Virtual Communication Manager, ASM = Avaya Session Manager, SM = System Manager, AES = Application Enablement Services

SHA: Secure Hash Algorithm

SHA-1: Secure Hash Algorithm 1. All Certificate Authorities stopped issuing SHA-1 certificates in Dec 2015 and existing SHA-1 certificates in the field are expected to expire by Dec 2016.

SHA-2: Secure Hash Algorithm 2 is a set of cryptographic hash functions designed by the National Security Agency (NSA). This is newer & more secure than SHA-1 algorithm using a 256-bit (32-byte) hash.

SLA Mon™: Service Level Agreement Monitor, an element of Avaya Diagnostic Server. Provides network monitoring for key Avaya system parameters.

SR: Service Request

SSH: Secure Shell Linux command

SSO Login: Single Sign On – and Avaya login that gains access to many Avaya resources / systems

SVM: Services Virtual Machine

Services-VM: Same as SVM or Services Virtual Machine

UI: User Interface

VSALGW: This nomenclature, VSALGW is the SE Code for a SAL Gateway that is part of Avaya Aura System Platform.

Appendix B: Change History

Date	Version	Updates
May 16, 2016	1.0	
May 27, 2016	1.1	• Section 8.B. streamlining the SAL Gateway 2.1, Services-VM1, upgrade directly to Services-VM3 & appropriate tables in section 1 & 8 • Appendix B & C detailing GRT migration process folded into section 8 • Section 6,7,8 added larger screenshot for managed elements export • Appendix I specific ION hyperlinks • Minor number of format and clarifying word corrections (e.g. expanding full product names out versus acronyms) • Minor hyperlink updates • Added direct links to pages into hyperlinks as possible to aid user directly into the page/section of the hyperlinked document • Used Appendix H (was futures) for addressing FL search
June 22, 2016	1.2	• Reformatting and structuring of the document • Using “SAL Gateway” instead of SALGW to refer to SAL Gateways in general, removing confusion with the SECode SALGW • Added clarity around when GRT work is and isn’t needed • Updated instrcutions to care for SAL Gateway 2.3.x
July 8, 2016	1.3	• Clarified instructions for properly decommissioning old SAL Gateways • Added instructional videos for Scenarios M, N, O • Added instructional videos for properly decommissioning a VSAL GW • Replaced references to ADS Service Pack 2, with Service Pack 3
July 27, 2016	1.4	• Added details regarding the Remote Agent Push • Added details regarding the ACSBI SHA2 Readiness Report
August 31, 2016	1.5	• Clarified GRT steps for migrating SEIDs to a new SAL Gateway
September 27, 2016	1.6	• Corrected steps for retesting migrated devices in Scenario A
September 30, 2016	1.7	• Corrected steps for retesting migrated devices in Scenarios B, C, & D