Secure Access Link Features List and Release Updates

Introduction

This document provides information about Secure Access Link (SAL) features list from Release 1.5 through Release 2.5 and the enhancements implemented in each of these releases. This document supplements the Secure Access Link Gateway software and documentation. For latest documentation, product support notices, and service pack information, go to the Avaya Support website at http://support.avaya.com.

Contents

Features list and enhancements

Many of the SAL Gateway components and features were significantly enhanced from SAL Release 1.5 through SAL Release 2.5.

The following table lists the features and enhancements for all the releases of SAL Gateway, from Release 1.5 through Release 2.5.

Release	Enhancement	Description
SAL 1.5	Secure remote access	SAL facilitates secure remote access to support personnel and tools that need to access supported devices in customer network. SAL Gateway provides remote access to devices that are configured for remote access through SAL. Remote access though SAL Gateway provides: • Communication confidentiality • Customer-controlled authorization • TCP application-level (not a traditional VPN)
	Secure alarm delivery	SAL Gateway receives alarms, for example, SNMP INADS and syslog, from Avaya products in customer network, reformat them, and forward them to the Secure Access Core Concentrator Servers at Avaya support center and/or authorized partner's support center. SAL Gateway forwards alarms to customer-managed Network Management Systems (NMS) also.
	Easy to use GUI	SAL Gateway includes a Web-based graphical user interface (GUI) that provides an interface for administrative functions, configuration, and logging. The SAL Gateway UI provides a means to configure and monitor SAL Gateway as well as the associated devices for alarming and remote access.
	SAL Watchdog monitoring service	The SAL Watchdog service routinely monitors the operational state of all SAL Gateway services, restarts services in case of any abnormal shutdowns, and generates corresponding alarms.

Release	Enhancement	Description
SAL 1.5	Security	SAL 1.5 provides the following security features: • PKI support and Avaya VeriSign PKI certificates • Request/grant connectivity governed by customer policies • Avaya automated tools (Expert Systems) also authenticate with certificates
	SAL Gateway redundancy (manual)	SAL offers enhanced service availability by way of redundant gateways for remote access, alarming and inventory. Redundancy for SAL Gateways means that more than one SAL Gateway administers the same managed device. The configuration of the devices is such that they send SNMP traps to each of the gateways. Major advantages of redundancy are availability of access and geographic independence.
SAL 1.8	SAL Gateway diagnostics	The SAL Gateway diagnostics feature verifies the SAL Gateway communication with all other servers to provide easy ways for remote assistance. The diagnostics feature verifies the SAL Gateway communication with the following: • Secure Access Concentrator Core Server • Secure Access Concentrator Remote Server • Secure Access Policy Server • Managed devices • Components within the customer network such as LDAP servers
	Inventory collection	SAL Release 1.8 onwards, SAL Gateway provides the inventory collection functionality that collects inventory information about the supported managed devices and sends it to the Secure Access Concentrator Core Server for Avaya reference. The inventory data provides information such as the product type and version information for the reference of customers and Maintenance Service Providers (MSPs). Technicians can review inventory data for managed device configuration during ticket resolution. Inventory data also form the base for future software and firmware upgrade.
	SAL Gateway redundancy enhancement	SAL Gateway supports GUI for redundancy configuration.
	Security enhancement	In Release 1.8, SAL Gateway provides Role-Based Access Control (RBAC) support.

Release	Enhancement	Description
SAL 2.0	SAL Gateway IPv6 enablement	SAL Release 2.0 onwards, SAL Gateway is IPv6 enabled. You can deploy SAL Gateway on a: • Uni-mode IPv4 host • Uni-mode IPv6 host • Dual-mode, IPv6 and IPv4 host IPv6 enablement on the SAL Gateway necessitated the addition of the SAL Agent Watchdog, a new monitoring service that runs with the root privilege in SAL Gateway 2.0. Starting with SAL Gateway 2.1, SAL Agent Watchdog runs as normal saluser, where saluser is given certain pseudo permissions. The addition of the SAL Agent Watchdog service became necessary because: • The SAL Gateway supports RHEL 5.0, which operates with the limitation that it does not support port forwarding for IPv6. • With IPv6 enablement, the SAL Gateway component named SAL Agent service could not start without the root privilege. To run the service without the root privilege on an IPv6 host: 1. The SAL Agent service starts with the root privilege. 2. It binds the high privilege port, 162, to listen to alarms. 3. It then downgrades itself to the nonroot privilege. The SAL Agent Watchdog service monitors the SAL Agent service and restarts the agent service if the agent service abruptly shuts down.
	Device import and configure support	The SAL import and configure functionality allows the use of the SAL Gateway user interface (UI) to import registered devices from the systems of Avaya, and configure the assignment of the imported devices to SAL Gateways in a customer network. The SAL Gateway UI provides the Import and Configure Devices page to configure the assignment of registered devices to SAL Gateways.
	Device auto-onboarding support	The SAL auto-onboarding feature provides a mechanism whereby the device assignment or onboarding request list is serviced and the devices are automatically onboarded to the specified SAL Gateways. Auto-onboarding limits technician time related to setting up products for trap forwarding.
	Easy CA certificate refresh	SAL Gateway Release 2.0 can automatically download and install Certificate Authority (CA) certificates when fresh certificates are uploaded to the upstream Secure Access Concentrator Core Servers. You can also install the certificates manually.

Release	Enhancement	Description
SAL 2.0	Model distribution	The Model Distribution feature of SAL Gateway ensures that SAL-managed devices are associated with the latest model definitions. Upon a restart, a SAL Gateway checks the Secure Access Concentrator Core Server for new and updated models. If newer models are available, SAL Gateway automatically downloads and applies the latest models to the managed devices. SAL ensures that the SAL Gateway users always have access to the latest model versions. Models are applied in accordance with user preferences
	Gateway health monitoring	SAL Release 2.0 onwards, SAL Gateway supports status monitoring of the SAL Gateway components. Through the SAL Gateway UI, you can view Gateway diagnostics, configuration files, and health reports to determine the status of SAL Gateway. SAL Gateway consists of SAL Agent, Remote Access Agent, SAL Watchdog and SAL Gateway UI. The overall health of the SAL Gateway is a function of individual status of these components. You can generate reports that provide service status of various components supported by SAL Gateway. The reports also show the connectivity status of SAL Gateway with various server applications, such as Concentrator Core and Remote Servers, Policy Server, LDAP server, and proxy server.
	SNMP enhancement and v3 support	Release 2.0 onwards, SAL Gateway is a Simple Network Management Protocol (SNMP)-enabled product by having a SNMP Sub Agent and using the host computer's Net-SNMP agent as Master SNMP Agent. The OS SNMP Master Agent and SAL SNMP Sub Agent use the AgentX protocol for communication. SAL Gateway Release 1.8 and previous releases use SNMP v1 and v2c for alarming and inventory services of supported managed devices. The alarming service receives SNMP traps from managed devices and the inventory service sends SNMP get requests to managed devices to fetch inventory. With v3 support enablement, the alarming and inventory services now support SNMPv3 traps and get queries.
	Operating system support for SAL Gateway	SAL Gateway Release 2.0 is supported on the Red Hat Enterprise Linux (RHEL) 32-bit system versions 5.0 to 5.4. Supported VMware versions are: • VMware ESX 3.5 • VMware ESX 3.5i • VMware ESX 4.0 • VMware ESX 4.0i

Release	Enhancement	Description
SAL 2.1	Extended auto-onboarding support for managed devices	In Release 2.1, the SAL Gateway auto-onboarding feature is available for the following versions of products: • Avaya Aura® SIP Enablement Services (SES): Version 5.0, 5.1, and 5.2 • Avaya Modular Messaging Storage Server (MMSS): Version 4.0, 5.0, 5.1, and 5.2 • Avaya Aura® Application Enablement Services (AES): Version 4.2.2, 4.2.3, and 5.2 • Avaya Voice Portal (VP): Version 5.0 and 5.1 • Avaya Aura® Communication Manager (CM): Version 3.0, 5.2, and 6.0 When a device from any of the above product category is onboarded, SAL Gateway automatically configures itself as an SNMP V2c or V3 trap destination on the device, so that the device can send SNMP traps or alarms to SAL Gateway. The SAL Gateway forwards the SNMP traps to the Avaya Enterprise Server.
	Java 6 support	SAL Release 2.1 supports Java 6. You must install SAL Gateway Release 2.1 in Java 6 environment with all possible SAL deployment models.
	Installation enhancement	The SAL Gateway Release 2.1 installer supports an upgrade capability from all previously installed earlier releases of SAL Gateway. If the installer detects that SAL Gateway Release 1.5, 1.8, or 2.0 is already installed, including any patches and Service Packs applied to it, the installer proceeds with the upgrade process to Release 2.1.
	Data collection and upload support	SAL Gateway Release 2.1 supports data collection from managed devices that request for the data collection and upload feature. The new Data Collection and Upload (DCU) component of SAL Gateway facilitates data collection and upload from managed devices, such as SLA Mon Server, to Avaya Data Center. SAL Gateway collects data from managed devices depending on the configured preferences and uploads the data to the Concentrator Core Enterprise Server at Avaya Data Center.
	Security enhancements	SAL Gateway Release 2.1 provides the following security enhancements: • The new release limits the maximum number of sessions per user and per application on the SAL Gateway UI. The default setting for the SAL Gateway UI application is a maximum of 50 sessions per application and 25 sessions per user. You can configure both the limits. • Tomcat has been upgraded from version 6.0.20 to the latest version from Apache Foundation, 6.0.29. • SAL Gateway UI session time-out is changed from 15 minutes to 10 minutes. • Starting from Release 2.1, the SAL Agent Watchdog service runs as saluser instead of root. This service starts SAL Agent in case SAL Agent has shutdown ungracefully.

Release	Enhancement	Description
SAL 2.2	Operating system support for SAL Gateway	SAL Gateway Release 2.2 is supported on 32-bit and 64-bit systems with RHEL versions 5.x and 6.x. Supported VMware versions are: • VMware ESX 3.5 • VMware ESX 3.5i • VMware ESX 4.0 • VMware ESX 4.0i • VMware ESXi 5.0 **Note**: Avaya certifies ESXi 5.0 for SAL Gateway with 32-bit and 64-bit RHEL 5.x and 6.x operating systems.
	Auto generation of SAL Gateway IDs	In SAL Gateway Release 2.2, you can obtain the SAL Gateway identifying numbers, which include Solution Element ID (SEID) and Product ID, by two methods: • Before the SAL Gateway installation, obtain the IDs through the existing SAL Gateway registration process. • Auto-generate the IDs during the graphical user interface (GUI)-based installation of SAL Gateway. The silent installation of SAL Gateway does not support the auto generation of SEID. For silent installation, you must register SAL Gateway in advance.
	Log filtering and extracting capabilities	In SAL Gateway Release 2.2, you have the capability to filter log data in SAL Gateway using the SAL Gateway UI. You can select log files for various activities and then filter the data by defining filter criteria. You can also extract the filtered logs to your local system in the raw or CSV format to view and analyze the logs offline. The SAL Gateway UI displays the log files in logical categories for you to select, view, filter, and export. In Release 2.2, the SAL Gateway UI displays the log data as wrapped lines in a tabular format so that you can read the logs easily. You still have the option to view the logs in the raw format.
	Backup and restore capabilities	In Release 2.2, you can back up and restore Gateway configuration information easily through the SAL Gateway UI. You can now trigger a backup whenever required and schedule an automatic backup at specific intervals. SAL Gateway backs up and combines configuration files and folders into a backup archive. Whenever a requirement arises, you can restore previously backed up configuration information for SAL Gateway from the backup archives.
	Security enhancements	SAL Gateway Release 2.2 provides the following security enhancement: • Apache Tomcat version is upgraded to 6.0.33 to protect SAL Gateway against security vulnerabilities present in the earlier versions.

Release	Enhancement	Description
SAL 2.3	Automatic software update	In Avaya Diagnostic Server Release 2.0, the SAL Gateway component provides the automatic software update feature. Through this feature, Avaya Diagnostic Server automatically receives software updates, including major, minor, and service pack releases. Through the feature, Avaya ensures that you are using the latest version of Avaya Diagnostic Server and its components. When the feature is enabled, SAL Gateway automatically installs the downloaded software updates after a grace period. You receive email notifications related to software updates, including download status, installation status, and availability.
SAL 2.5	Automatic Solution Element ID generation through the SAL Gateway UI	With Avaya Diagnostic Server Release 2.5, the SAL Gateway automatic Solution Element ID generation capability is now available through the SAL Gateway UI. The facility was until now available only in the attended mode of installation of SAL Gateway. If you install SAL Gateway with the default ID, the automatic Solution Element ID generation facility becomes available on the SAL Gateway UI.
	Enhancement to automatic software update feature	In Release 2.5, the automatic software update feature is enhanced. You can now apply a downloaded software update immediately or in the next available time frame through the SAL Gateway UI.
	Ease of managed device administration on the SAL Gateway UI	The registration information of the products that are registered through Global Registration Tool (GRT) 4 now becomes available to the designated SAL Gateway. Therefore, the SAL Gateway UI now automatically populates the available registration information of such a product in the device administration pages of the UI. With this enhancement, you can save on the manual labor of entering the registration data on SAL Gateway, avoid typographic errors, and achieve better efficiency in the device onboarding process.

For more information about the enhancements in a particular release, see *Secure Access Link Gateway Implementation Guide* or *Administering Avaya Diagnostic Server SAL Gateway* for the respective release.

Fixes

For information on fixes for service packs on Secure Access Link releases, see the respective release notes for the service packs. Following are the release notes for SAL service packs available on the Avaya Support Center Web site at http://support.avaya.com.

Release Notes	Direct link on the Avaya Support Center Web site
Secure Access Link 1.8 Gateway Service Pack 3 Release Notes (Along with the SAL 1.8 SP3 fixes, this document includes the SP1 and SP2 fixes also)	https://downloads.avaya.com/css/P8/documents/100132875
Secure Access Link 2.0 Gateway Service Pack 1 Release Notes	https://downloads.avaya.com/css/P8/documents/100125412
Secure Access Link 2.0 Gateway Service Pack 2 Release Notes	https://downloads.avaya.com/css/P8/documents/100126370
Secure Access Link 2.0 Gateway Service Pack 3 Release Notes	https://downloads.avaya.com/css/P8/documents/100133981

Secure Access Link 2.0 Gateway Service Pack 4 Release Notes	https://downloads.avaya.com/css/P8/documents/100146447
Secure Access Link 2.0 Gateway Service Pack 5 Release Notes	https://downloads.avaya.com/css/P8/documents/100150306
Secure Access Link 2.0 Gateway Service Pack 6 Release Notes	https://downloads.avaya.com/css/P8/documents/100155200
Secure Access Link 2.1 Gateway Service Pack 1 Release Notes	https://downloads.avaya.com/css/P8/documents/100154043
Secure Access Link 2.1 Gateway Service Pack 2 Release Notes	https://downloads.avaya.com/css/P8/documents/100156478
Secure Access Link 2.1 Gateway Service Pack 3 Release Notes	https://downloads.avaya.com/css/P8/documents/100160982
Secure Access Link 2.1 Gateway Service Pack 4 Release Notes	https://downloads.avaya.com/css/P8/documents/100166351
Secure Access Link Gateway 2.2 Service Pack 1 Release Notes	http://support.avaya.com/css/P8/documents/100176517
Avaya Diagnostic Server 2.0 Service Pack 1 Release Notes	https://downloads.avaya.com/css/P8/documents/100182695
Avaya Diagnostic Server 2.0 Service Pack 2 Release Notes	https://downloads.avaya.com/css/P8/documents/101004577